



Report VA/PT DEMO

Contesto

Rapporto di audit eseguito con Fred for security installato su una rete aziendale con 30 IP.

Fred for security ha inviato al cliente un rapporto di 799 pagine, in questa demo sono state estratte solo le prime 220 pagine.

Indice

Introduzione	3
Livelli di gravità	4
Executive Summary	5
Traceroute	10
Sistemi operativi	15
Porte e servizi individuati	18
Segnalatori di Versione individuati	27
Elenco delle Vulnerabilità	40
Vulnerabilità	82
Sistema Target: 192.168.0.1	82
Sistema Target: 192.168.0.2	100
Sistema Target: 192.168.0.3	123
Sistema Target: 192.168.0.4	135
Sistema Target: 192.168.0.13	142
Sistema Target: 192.168.0.17	143
Sistema Target: 192.168.0.25	148
Sistema Target: 192.168.0.27	153
Sistema Target: 192.168.0.29	167
Sistema Target: 192.168.0.30	195
Sistema Target: 192.168.0.34	198
Sistema Target: 192.168.0.37	203
Sistema Target: 192.168.0.40	224
Sistema Target: 192.168.0.46	245
Sistema Target: 192.168.0.54	253
Sistema Target: 192.168.0.62	262
Sistema Target: 192.168.0.100	290
Sistema Target: 192.168.0.101	305
Sistema Target: 192.168.0.120	316
Sistema Target: 192.168.0.121	323
Sistema Target: 192.168.0.201	330
Sistema Target: 192.168.0.205	334
Sistema Target: 192.168.0.222	338
Sistema Target: 192.168.0.225	352
Sistema Target: 192.168.0.235	360
Sistema Target: 192.168.0.248	362
Sistema Target: 192.168.0.249	393
Sistema Target: 192.168.0.251	425
Sistema Target: 192.168.0.253	609

Sistema Target: 192.168.0.254	703
Sistemi Offline	797

FRED FOR SECURITY DEMO

Introduzione

Questo report è il risultato di un "online vulnerability assessment", eseguito da **admin**.

Questo documento è stato redatto e predisposto per fornire un report rapido e di immediata comprensione per semplificare il compito di mettere in sicurezza sistemi di computer e apparecchiature informatiche collegate a Internet.

Le vulnerabilità di sistema sono classificate in quattro categorie: **rischio Alto, Medio, Basso o Informazione**. Una spiegazione dettagliata per ciascuna categoria di vulnerabilità si trova al capitolo **Livelli di gravità**.

Un **Executive Summary** è stato redatto appositamente per una consultazione a livello di management. Questo contiene sia informazioni scritte sia grafici, sulla base dei risultati del vulnerability assessment. Tali risultati includono informazioni su "quando è stata eseguita la scansione", "chi ha eseguito la scansione", e la quantità di vulnerabilità rilevate per ciascuna categoria.

L'**Executive Summary** include anche una conclusione che riporta il "livello complessivo di sicurezza" del sistema sotto esame.

I dettagli e nomi delle vulnerabilità trovate si trovano al capitolo **Sintesi delle vulnerabilità**. A seguire, sono elencati i dettagli di ciascuna vulnerabilità e le indicazioni per rimuoverle.

Where possible, a **CVSS score(*)**, a **CVE(**)** and/or a **USN(***)** are present, for further details.

Ogni vulnerabilità individuata viene corredata con un possibile rimedio.



(*) CVSS is the NIST (National Institute of Standards and Technology) severity scoring system.

(**) CVE è l'elenco ufficiale CVE Mitre.

(***) USN è la lista ufficiale di Ubuntu Security Notice.

Livelli di gravità

Vulnerabilità di livello Alto

Quando viene individuata una vulnerabilità di livello Alto, significa che è possibile per un intruso penetrare e compromettere completamente il sistema e/o accedere ad informazioni altamente sensibili. Esiste un elevato rischio di furto o perdita di dati privati e sensibili.

Vulnerabilità di livello Medio

Quando viene individuata una vulnerabilità di livello Medio, significa che un intruso può ottenere l'accesso a informazioni di sistema che potrebbero portare ad attacchi più specifici ed eventualmente alla compromissione del sistema. Ciò a sua volta potrebbe portare al furto o alla perdita di dati privati e sensibili.

Vulnerabilità di livello Basso

Quando viene individuata una vulnerabilità di livello Basso, significa generalmente che un intruso può ottenere l'accesso a informazioni di sistema che possono aiutare a condurre attacchi più specifici, con conseguente furto o perdita di dati privati e sensibili.

Informazione

Tutte le voci di livello Informazione forniscono semplicemente informazioni aggiuntive a quelle già disponibili sul sistema in esame. Non costituiscono un'indicazione sulla vulnerabilità o meno del sistema.

Executive Summary

Questo report illustra il risultato di una scansione di sicurezza effettuata da **admin**. Contiene informazioni riservate sullo stato della rete. L'accesso a queste informazioni da parte di personale non autorizzato può consentire loro di compromettere la sicurezza della rete.

Nome dello Scan	NetworkScan_internal	Profilo di scansione	Best Scan
Data/ora Inizio	14-09-2023 15:06:53	Data/ora fine	21-09-2023 09:43:57
Durata	162:37:04 (6 days, 18 hours, 37 minutes, 4 seconds)		
Versione Scanner	9.9.33.1357	Versione Firmware	57.0.4
Elenco dei sistemi controllati	192.168.0.0, 192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.13, 192.168.0.14, 192.168.0.15, 192.168.0.16, 192.168.0.17, ... ,192.168.0.255		

Questa scansione è stata eseguita dall'utente **admin**.

La scansione di 1 IP ha prodotto falsi positivi ed è stata interrotta

Livello di Sicurezza Complessivo

Cat. 1 (livello Critico)


La scansione eseguita da **admin** ha determinato che la sicurezza del sistema è ad un livello basso. E' possibile che intrusi penetrino completamente il sistema con una conseguente perdita di dati privati e sensibili. Si raccomanda di prendere provvedimenti immediati per aumentare il livello di sicurezza.

Sistemi Online

I seguenti sistemi erano in linea al momento della scansione:

192.168.0.1, 192.168.0.2, 192.168.0.3, 192.168.0.4, 192.168.0.13, 192.168.0.17, 192.168.0.25, 192.168.0.27, 192.168.0.29, 192.168.0.30, 192.168.0.34, 192.168.0.37, 192.168.0.40, 192.168.0.46, 192.168.0.54, 192.168.0.62, 192.168.0.100, ... ,192.168.0.254

Sistemi Offline

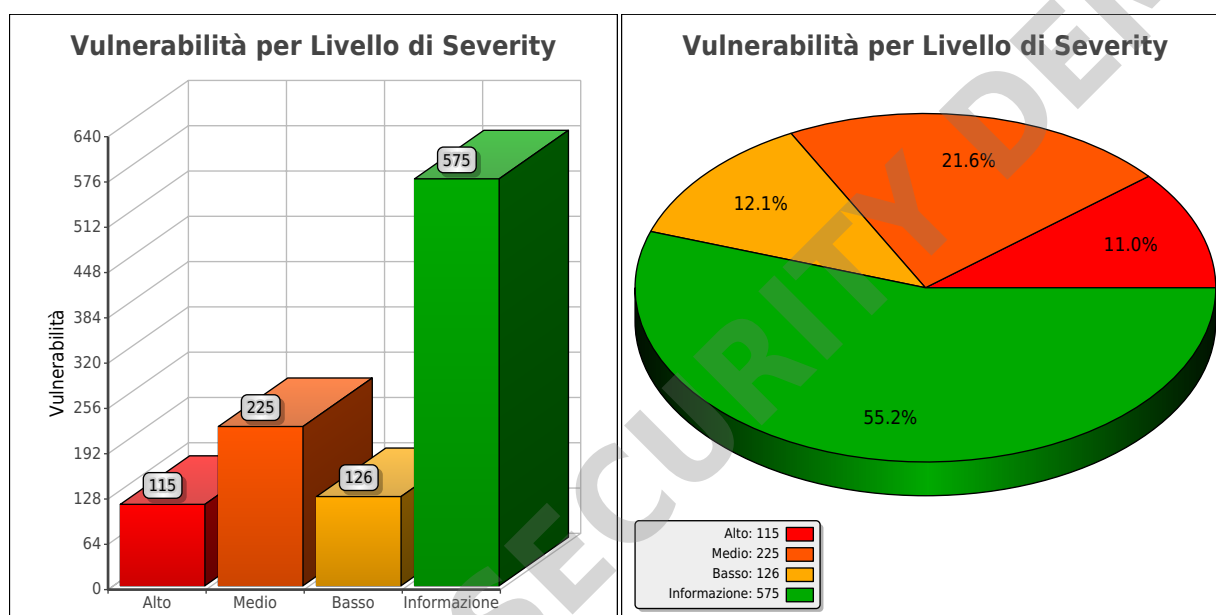
Alcuni sistemi non erano in linea al momento della scansione, quindi sono stati esclusi dai risultati sopra.

Sistemi Offline: 192.168.0.0, 192.168.0.5, 192.168.0.6, 192.168.0.7, 192.168.0.8, 192.168.0.9, 192.168.0.10, 192.168.0.11, 192.168.0.12, 192.168.0.14, 192.168.0.15, 192.168.0.16, 192.168.0.18, 192.168.0.19, 192.168.0.20, 192.168.0.21, 192.168.0.22

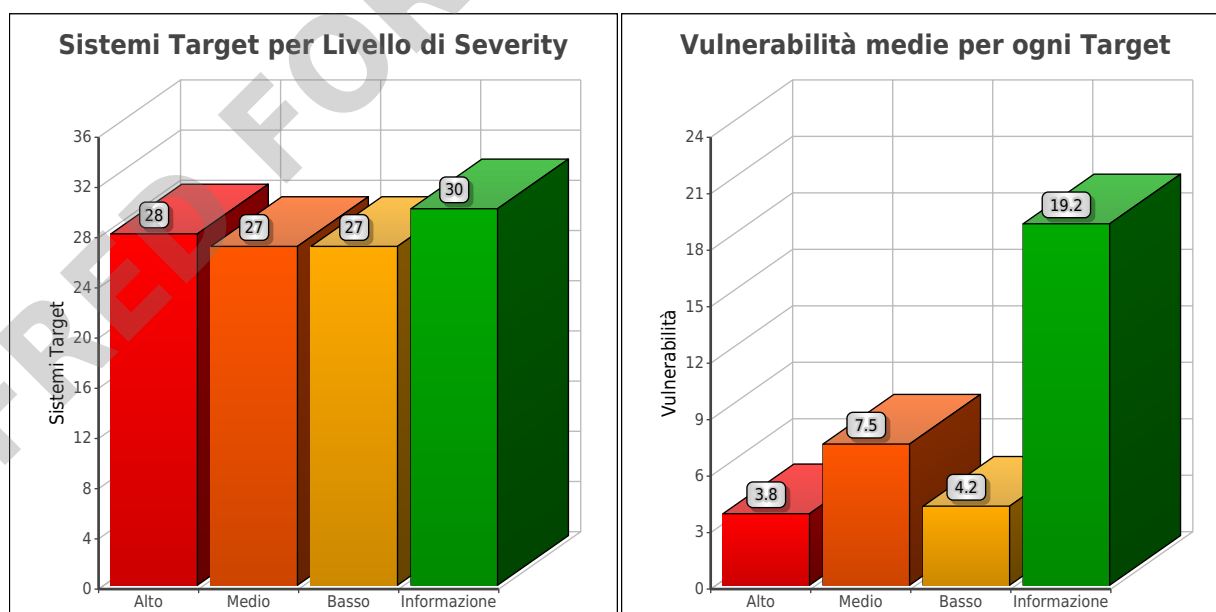
FRED FOR SECURITY DEMO

Analisi dei Risultati

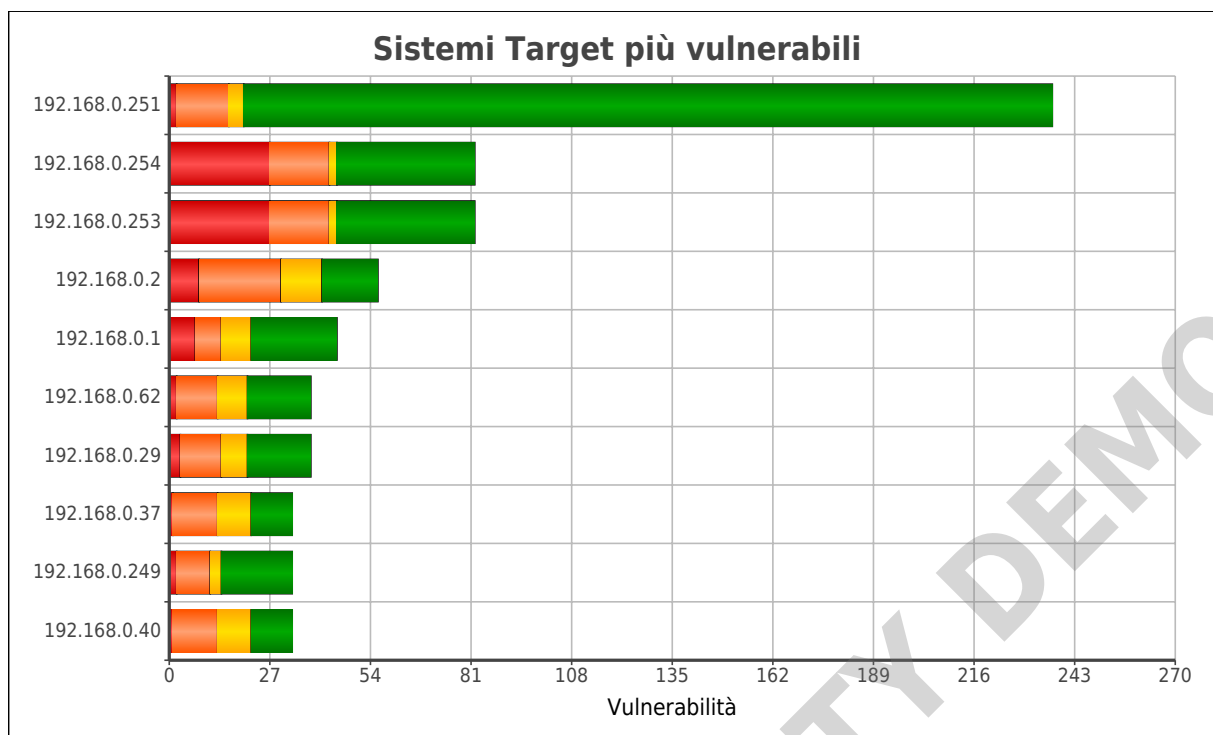
Un totale di **1041** potenziali vulnerabilità sono state individuate nei sistemi di destinazione, con un rapporto di **11.0%** di vulnerabilità di livello Alto. Le vulnerabilità di livello Alto sono state trovate in **28** Target. La vulnerabilità più frequente è '**Mail Server sent to files attack**', con il livello di Severity 'Alto', trovata su 1 Target. Il sistema di destinazione con il maggior numero di vulnerabilità è '**192.168.0.251**', con un totale di **237** vulnerabilità. Sistemi Target privi di vulnerabilità: .



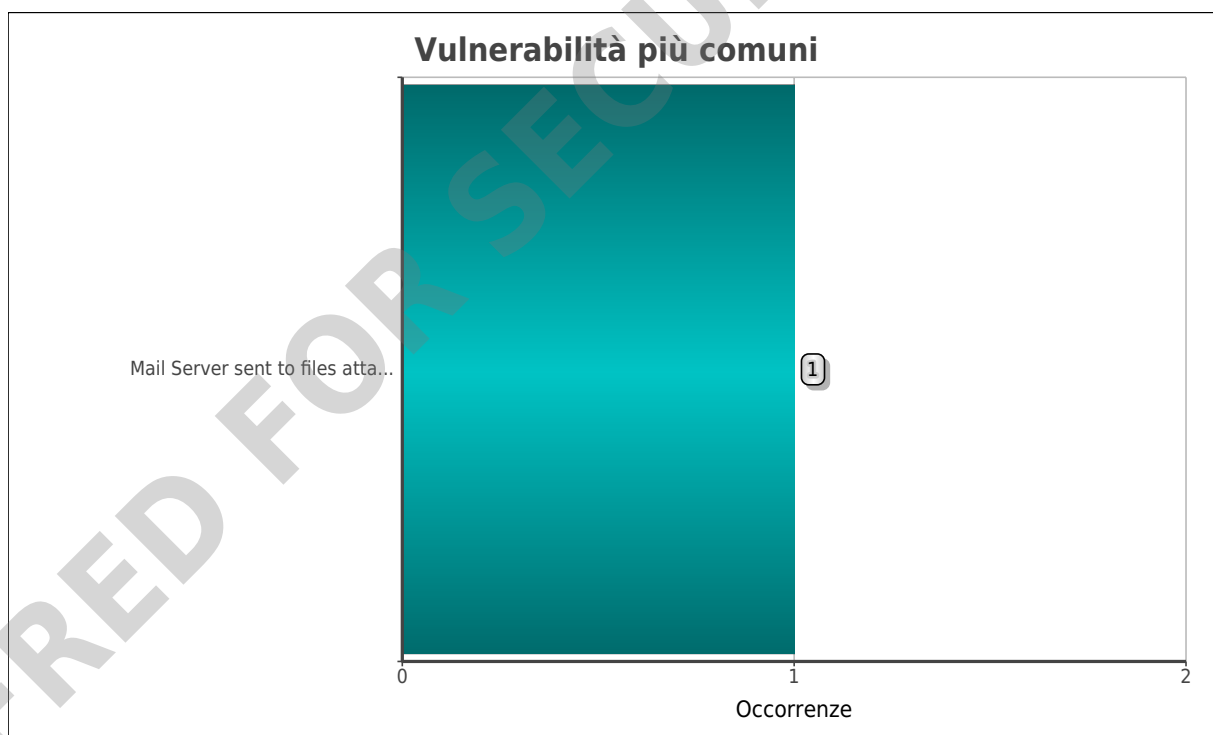
Numero totale di vulnerabilità



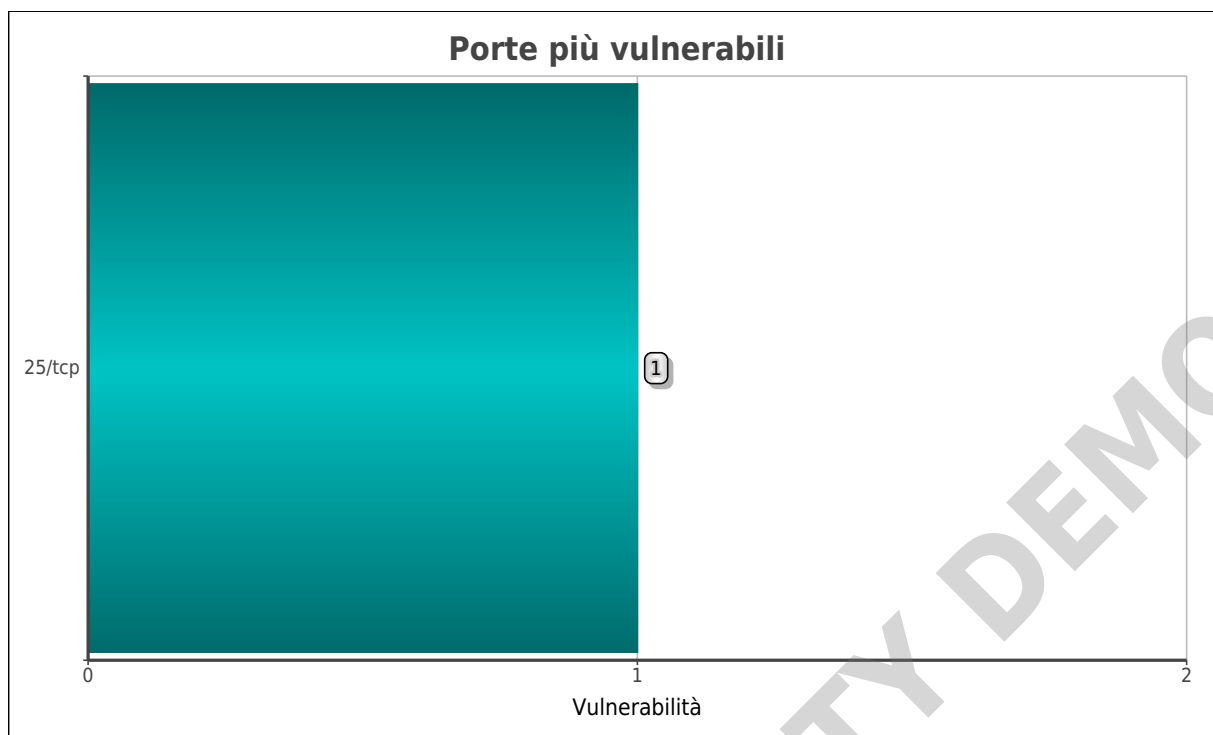
- (1) Numero di target per ogni tipo di Severity
 (2) Distribuzione delle vulnerabilità su ciascun Target



Target più vulnerabili, con dettagli sulla Severity



Elenco delle vulnerabilità più frequenti, con numero di occorrenze



Elenco delle porte più vulnerabili, in base al numero di vulnerabilità rilevate in quella porta

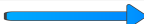
Traceroute

Questo è il risultato di una traceroute da admin ai sistemi esaminati:

traceroute to 192.168.0.1 (192.168.0.1), 15 hops max, 60 byte packets

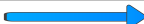
Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.1	192.168.0.1		0.350	

traceroute to 192.168.0.2 (192.168.0.2), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.2	192.168.0.2		0.288	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

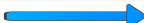
traceroute to 192.168.0.3 (192.168.0.3), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.3	192.168.0.3		0.346	

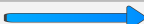
traceroute to 192.168.0.4 (192.168.0.4), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.4	192.168.0.4		0.487	

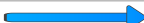
traceroute to 192.168.0.13 (192.168.0.13), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.13	192.168.0.13		6.082	

traceroute to 192.168.0.17 (192.168.0.17), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	*	*	-	-	-
2	192.168.0.17	192.168.0.17		0.876	

traceroute to 192.168.0.25 (192.168.0.25), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.25	192.168.0.25		0.739	

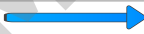
traceroute to 192.168.0.27 (192.168.0.27), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.27	192.168.0.27		1.010	

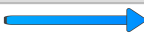
traceroute to 192.168.0.29 (192.168.0.29), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.29	192.168.0.29		0.762	

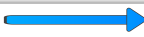
traceroute to 192.168.0.30 (192.168.0.30), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.30	192.168.0.30		2.660	

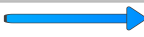
traceroute to 192.168.0.34 (192.168.0.34), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.34	192.168.0.34		0.901	

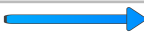
traceroute to 192.168.0.37 (192.168.0.37), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.37	192.168.0.37		0.342	

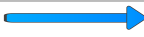
traceroute to 192.168.0.40 (192.168.0.40), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.40	192.168.0.40		0.402	

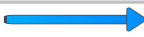
traceroute to 192.168.0.46 (192.168.0.46), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.46	192.168.0.46		2.518	

traceroute to 192.168.0.54 (192.168.0.54), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.54	192.168.0.54		0.322	

traceroute to 192.168.0.62 (192.168.0.62), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.62	192.168.0.62		2.401	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.100 (192.168.0.100), 15 hops max, 60 byte packets

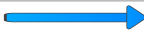
Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.100	192.168.0.100		0.347	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

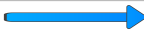
traceroute to 192.168.0.101 (192.168.0.101), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.101	192.168.0.101		0.484	

traceroute to 192.168.0.120 (192.168.0.120), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.120	192.168.0.120		0.409	

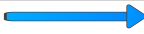
traceroute to 192.168.0.121 (192.168.0.121), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.121	192.168.0.121		0.236	

traceroute to 192.168.0.201 (192.168.0.201), 15 hops max, 60 byte packets

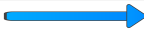
Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.201	192.168.0.201		0.336	

traceroute to 192.168.0.205 (192.168.0.205), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.205	192.168.0.205		0.335	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.222 (192.168.0.222), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.222	192.168.0.222		2.047	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.225 (192.168.0.225), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.225	192.168.0.225		0.549	

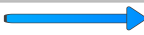
A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.235 (192.168.0.235), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.235	192.168.0.235		0.343	

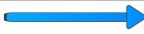
A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.248 (192.168.0.248), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.248	192.168.0.248		0.475	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.249 (192.168.0.249), 15 hops max, 60 byte packets

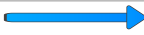
Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.249	192.168.0.249		0.484	

traceroute to 192.168.0.251 (192.168.0.251), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.251	192.168.0.251		0.539	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.253 (192.168.0.253), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.253	192.168.0.253		0.284	

A protezione del sistema esaminato è stato trovato un dispositivo di filtraggio dei pacchetti. In genere si tratta di un sistema di firewall o di un router con ACL (Access Control Lists). Anche in presenza di un

tale dispositivo, in caso di una cattiva configurazione il sistema potrebbe presentare delle vulnerabilità.

traceroute to 192.168.0.254 (192.168.0.254), 15 hops max, 60 byte packets

Hop	Nome	IP	Località	Med(ms)	Grafico
1	192.168.0.254	192.168.0.254		0.485	

FRED FOR SECURITY DEMO

Sistemi operativi

Sono stati identificati i seguenti sistemi operativi:

Sistema Target: 192.168.0.1



Microsoft Windows

Sistema Target: 192.168.0.2



Microsoft Windows

Sistema Target: 192.168.0.3



Linux 2.2.x-3.x

Sistema Target: 192.168.0.4



Microsoft Windows

Sistema Target: 192.168.0.13

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.17

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.25



Microsoft Windows

Sistema Target: 192.168.0.27



Linux 2.2.x-3.x

Sistema Target: 192.168.0.29



Linux

Sistema Target: 192.168.0.30



Windows XP

Sistema Target: 192.168.0.34

Microsoft Windows

Sistema Target: 192.168.0.37

Linux 3.x

Sistema Target: 192.168.0.40

Linux 3.x

Sistema Target: 192.168.0.46

Microsoft Windows

Sistema Target: 192.168.0.54

Linux 2.2.x-3.x

Sistema Target: 192.168.0.62

Linux

Sistema Target: 192.168.0.100

Linux 2.2.x-3.x

Sistema Target: 192.168.0.101

Windows XP

Sistema Target: 192.168.0.120

Linux 2.2.x-3.x

Sistema Target: 192.168.0.121

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.201

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.205

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.222

Windows XP

Sistema Target: 192.168.0.225

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.235

Non è stato possibile identificare il sistema operativo per questo target.

Sistema Target: 192.168.0.248

Ubuntu Linux

Sistema Target: 192.168.0.249

Ubuntu Linux

Sistema Target: 192.168.0.251

Linux 2.2.x-3.x

Sistema Target: 192.168.0.253

Linux 2.2.x-3.x

Sistema Target: 192.168.0.254

Linux 3.x

Porte e servizi individuati

Le seguenti porte e servizi sono state individuate sui sistemi esaminati:

Porte e Servizi per: 192.168.0.1

Porta	Protocollo	Stato	Servizio
25	tcp	open	Simple Mail Transfer
80	tcp	open	World Wide Web HTTP
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service
445	tcp	open	Microsoft-DS
3389	tcp	open	MS WBT Server
5985	tcp	open	WBEM WS-Management HTTP
50007	tcp	open	
137	udp	open	NBTStat
1434	udp	open	ms-sql

Porte e Servizi per: 192.168.0.2

Porta	Protocollo	Stato	Servizio
21	tcp	open	File Transfer [Control]
53	tcp	open	Domain Name Server
80	tcp	open	World Wide Web HTTP
88	tcp	open	Kerberos
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service
389	tcp	open	Lightweight Directory Access Protocol
443	tcp	open	http protocol over TLS/SSL
445	tcp	open	Microsoft-DS
464	tcp	open	kpasswd
593	tcp	open	HTTP RPC Ep Map
636	tcp	open	ldap protocol over TLS/SSL (was sldap)
808	tcp	open	Oracle-VP2
987	tcp	open	cisco RSRB Priority 1 port
1433	tcp	open	Microsoft-SQL-Server
1723	tcp	open	pptp
1801	tcp	open	Microsoft Message Que
2103	tcp	open	Zephyr serv-hm connection
2105	tcp	open	MiniPay
2107	tcp	open	BinTec Admin
3268	tcp	open	Microsoft Global Catalog
3269	tcp	open	Microsoft Global Catalog with LDAP/SSL
3306	tcp	open	MySQL

Porta	Protocollo	Stato	Servizio
3389	tcp	open	MS WBT Server
5504	tcp	open	fcp-cics-gw1
5985	tcp	open	WBEM WS-Management HTTP
6004	tcp	open	
6005	tcp	open	
6006	tcp	open	
6007	tcp	open	
6009	tcp	open	
6010	tcp	open	
6011	tcp	open	
6067	tcp	open	
6161	tcp	open	PATROL Internet Srv Mgr
7070	tcp	open	ARCP
28000	tcp	open	NX License Manager
53	udp	open	DNS
53	udp	open	DNSStatusRequest
137	udp	open	NBTStat
1434	udp	open	ms-sql
123	udp	open	ntp

Porte e Servizi per: 192.168.0.3

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
88	tcp	open	Kerberos
389	tcp	open	Lightweight Directory Access Protocol
443	tcp	open	http protocol over TLS/SSL
514	tcp	open	cmd
636	tcp	open	ldap protocol over TLS/SSL (was sldap)
1514	tcp	open	Fujitsu Systems Business of America, Inc
2012	tcp	open	
2014	tcp	open	
2015	tcp	open	
2020	tcp	open	
5480	tcp	open	
5580	tcp	open	T-Mobile SMS Protocol Message 0
8084	tcp	open	
9084	tcp	open	IBM AURORA Performance Visualizer
9443	tcp	open	WSO2 Tungsten HTTPS

Porte e Servizi per: 192.168.0.4

Porta	Protocollo	Stato	Servizio
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service

Porta	Protocollo	Stato	Servizio
445	tcp	open	Microsoft-DS
3389	tcp	open	MS WBT Server
5985	tcp	open	WBEM WS-Management HTTP
137	udp	open	NBTStat

Porte e Servizi per: 192.168.0.13

Nessuna Porta o Servizio individuati su questo sistema.

Porte e Servizi per: 192.168.0.17

Porta	Protocollo	Stato	Servizio
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
4343	tcp	open	UNICALL
8080	tcp	open	HTTP Alternate (see port 80)
8081	tcp	open	Sun Proxy Admin Service

Porte e Servizi per: 192.168.0.25

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
53	tcp	open	Domain Name Server
54	tcp	open	XNS Clearinghouse
80	tcp	open	World Wide Web HTTP
8081	tcp	open	Sun Proxy Admin Service
8082	tcp	open	Utilistor (Client)
8083	tcp	open	Utilistor (Server)
8084	tcp	open	
53	udp	open	DNS
53	udp	open	DNSStatusRequest

Porte e Servizi per: 192.168.0.27

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL

Porte e Servizi per: 192.168.0.29

Porta	Protocollo	Stato	Servizio
80	tcp	open	World Wide Web HTTP
82	tcp	open	XFER Utility
554	tcp	open	Real Time Streaming Protocol (RTSP)
5196	tcp	open	
6060	tcp	open	

Porta	Protocollo	Stato	Servizio
7070	tcp	open	ARCP
7100	tcp	open	X Font Service
20000	tcp	open	DNP
30000	tcp	open	
30001	tcp	open	Pago Services 1
30002	tcp	open	Pago Services 2
49152	tcp	open	

Porte e Servizi per: 192.168.0.30

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
23	tcp	open	Telnet
80	tcp	open	World Wide Web HTTP
1506	tcp	open	Universal Time daemon (utcd)
1513	tcp	open	Fujitsu Systems Business of America, Inc
161	udp	open	SNMPv3
161	udp	open	snmp-public

Porte e Servizi per: 192.168.0.34

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
53	tcp	open	Domain Name Server
54	tcp	open	XNS Clearinghouse
80	tcp	open	World Wide Web HTTP
8081	tcp	open	Sun Proxy Admin Service
8082	tcp	open	Utilistor (Client)
8083	tcp	open	Utilistor (Server)
8084	tcp	open	
53	udp	open	DNS
53	udp	open	DNSStatusRequest

Porte e Servizi per: 192.168.0.37

Porta	Protocollo	Stato	Servizio
21	tcp	open	File Transfer [Control]
25	tcp	open	Simple Mail Transfer
80	tcp	open	World Wide Web HTTP
139	tcp	open	NETBIOS Session Service
427	tcp	open	Server Location
445	tcp	open	Microsoft-DS
515	tcp	open	spooler
631	tcp	open	IPP (Internet Printing Protocol)
8080	tcp	open	HTTP Alternate (see port 80)
9100	tcp	open	PDL Data Streaming Port

Porta	Protocollo	Stato	Servizio
20080	tcp	open	
137	udp	open	NBTStat
161	udp	open	SNMPv3
161	udp	open	snmp-public

Porte e Servizi per: 192.168.0.40

Porta	Protocollo	Stato	Servizio
21	tcp	open	File Transfer [Control]
25	tcp	open	Simple Mail Transfer
80	tcp	open	World Wide Web HTTP
139	tcp	open	NETBIOS Session Service
427	tcp	open	Server Location
445	tcp	open	Microsoft-DS
515	tcp	open	spooler
631	tcp	open	IPP (Internet Printing Protocol)
8080	tcp	open	HTTP Alternate (see port 80)
9100	tcp	open	PDL Data Streaming Port
20080	tcp	open	
137	udp	open	NBTStat
161	udp	open	SNMPv3
161	udp	open	snmp-public

Porte e Servizi per: 192.168.0.46

Porta	Protocollo	Stato	Servizio
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service
3389	tcp	open	MS WBT Server
5040	tcp	open	
56000	tcp	open	
53	udp	open	DNS
53	udp	open	DNSStatusRequest
137	udp	open	NBTStat

Porte e Servizi per: 192.168.0.54

Porta	Protocollo	Stato	Servizio
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
515	tcp	open	spooler
631	tcp	open	IPP (Internet Printing Protocol)
3911	tcp	open	Printer Status Port
8080	tcp	open	HTTP Alternate (see port 80)
9100	tcp	open	PDL Data Streaming Port
161	udp	open	snmp-public

Porte e Servizi per: 192.168.0.62

Porta	Protocollo	Stato	Servizio
80	tcp	open	World Wide Web HTTP
82	tcp	open	XFER Utility
554	tcp	open	Real Time Streaming Protocol (RTSP)
6060	tcp	open	
20000	tcp	open	DNP
30000	tcp	open	
30001	tcp	open	Pago Services 1
30002	tcp	open	Pago Services 2

Porte e Servizi per: 192.168.0.100

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
427	tcp	open	Server Location
443	tcp	open	http protocol over TLS/SSL
902	tcp	open	self documenting Telnet Door
5989	tcp	open	WBEM CIM-XML (HTTPS)
8000	tcp	open	iRDMI
8300	tcp	open	Transport Management Interface
9080	tcp	open	Groove GLRPC

Porte e Servizi per: 192.168.0.101

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
427	tcp	open	Server Location
443	tcp	open	http protocol over TLS/SSL
902	tcp	open	self documenting Telnet Door
5989	tcp	open	WBEM CIM-XML (HTTPS)
8000	tcp	open	iRDMI
8300	tcp	open	Transport Management Interface
9080	tcp	open	Groove GLRPC

Porte e Servizi per: 192.168.0.120

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
17988	tcp	open	
17990	tcp	open	
161	udp	open	SNMPv3

Porte e Servizi per: 192.168.0.121

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
17988	tcp	open	
17990	tcp	open	
161	udp	open	SNMPv3

Porte e Servizi per: 192.168.0.201

Porta	Protocollo	Stato	Servizio
23	tcp	open	Telnet
4370	tcp	open	ELPRO V2 Protocol Tunnel

Porte e Servizi per: 192.168.0.205

Porta	Protocollo	Stato	Servizio
23	tcp	open	Telnet
4370	tcp	open	ELPRO V2 Protocol Tunnel

Porte e Servizi per: 192.168.0.222

Porta	Protocollo	Stato	Servizio
23	tcp	open	Telnet
80	tcp	open	World Wide Web HTTP

Porte e Servizi per: 192.168.0.225

Porta	Protocollo	Stato	Servizio
135	tcp	open	DCE endpoint resolution
139	tcp	open	NETBIOS Session Service
445	tcp	open	Microsoft-DS
515	tcp	open	spooler
683	tcp	open	CORBA IIOP
1112	tcp	open	Intelligent Communication Protocol
1801	tcp	open	Microsoft Message Que
2103	tcp	open	Zephyr serv-hm connection
2105	tcp	open	MiniPay
2107	tcp	open	BinTec Admin
49154	tcp	open	
49155	tcp	open	
55555	tcp	open	
137	udp	open	NBTStat

Porte e Servizi per: 192.168.0.235

Porta	Protocollo	Stato	Servizio
5000	tcp	open	

Porte e Servizi per: 192.168.0.248

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
111	tcp	open	SUN Remote Procedure Call
443	tcp	open	http protocol over TLS/SSL
2049	tcp	open	
9390	tcp	open	OpenVAS Transfer Protocol
32767	tcp	open	FileNet BPM WS-ReliableMessaging Client
111	udp	open	RPCCheck
111	udp	open	rpc

Porte e Servizi per: 192.168.0.249

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
111	tcp	open	SUN Remote Procedure Call
443	tcp	open	http protocol over TLS/SSL
2049	tcp	open	
9390	tcp	open	OpenVAS Transfer Protocol
32767	tcp	open	FileNet BPM WS-ReliableMessaging Client
111	udp	open	RPCCheck
111	udp	open	rpc

Porte e Servizi per: 192.168.0.251

Porta	Protocollo	Stato	Servizio
21	tcp	open	File Transfer [Control]
80	tcp	open	World Wide Web HTTP
4649	tcp	open	
5963	tcp	open	Indy Application Server
8000	tcp	open	iRDMI
8010	tcp	open	
60030	tcp	open	

Porte e Servizi per: 192.168.0.253

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
541	tcp	open	uucp-rlogin

Porte e Servizi per: 192.168.0.254

Porta	Protocollo	Stato	Servizio
22	tcp	open	The Secure Shell (SSH) Protocol
80	tcp	open	World Wide Web HTTP
443	tcp	open	http protocol over TLS/SSL
541	tcp	open	uucp-rlogin

FRED FOR SECURITY DEMO

Segnalatori di Versione individuati

I seguenti Segnalatori di Versione (Version Banner) sono stati letti sui sistemi esaminati. Si consiglia vivamente di riconfigurare questi segnalatori con informazioni false o con nessuna informazione affatto.

Segnalatori di Versione per: 192.168.0.1

Nome	SMTP Mail Server Version Banner
Porta	25
Dettagli	220 CERT-SERVER Microsoft ESMTP MAIL Service, Version: 10.0.17763.1697 ready at Thu, 14 Sep 2023 15:17:55 +0200
Soluzione	It is highly adviceable to configure this output to return bogus or no information at all. UNIX: Sendmail 1:Open up the sendmail.cf file 2:Find the line saying O SmtgGreetingMessage= PARAMETERS (Where the parameters can be several \$ codes) 3:Change the line to O SmtgGreetingMessage=\$j (And nothing more). WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level. If you have already removed the version please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Microsoft-IIS/10.0
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	5985
Dettagli	Microsoft-IIS/10.0
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.2

Nome	BIND/NAMED Version Banner
Porta	53
Dettagli	Microsoft DNS 6.1.7601 (1DB15F75)
Soluzione	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "". If you have already made it return bogus information please ignore this check.

Nome	FTP Version Banner
Porta	21
Dettagli	220-FileZilla Server 0.9.60 beta;220-written by Tim Kosse (tim.kosse@filezilla-project.org);220 Please visit https://filezilla-project.org/
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Microsoft-IIS/7.5
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	5985
Dettagli	Microsoft-IIS/7.5
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	443
Dettagli	Microsoft-IIS/7.5
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.3

Nome	SSHd Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_7.4
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	9084
Dettagli	Jetty(9.4.20.v20190813)
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	9443
Dettagli	Jetty(9.4.20.v20190813)
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	9443

Dettagli	Anonymous
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.4

Nome	HTTP Version Banner
Porta	5985
Dettagli	Microsoft-HTTPAPI/2.0
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.13

Nessuno

Segnalatori di Versione per: 192.168.0.17

Nome	RTSP Version Banner
Porta	80
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: OPTIONS * RTSP/1.0

Nome	RTSP Version Banner
Porta	8081
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: OPTIONS * RTSP/1.0

Nome	HTTP Version Banner
Porta	80
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	8080
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	8081

Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	443
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	4343
Dettagli	
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.25

Nome	BIND/NAMED Version Banner
Porta	53
Dettagli	Microsoft DNS 6.1.7601 (1DB15F75)
Soluzione	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "" . If you have already made it return bogus information please ignore this check.

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-dropbear
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.27

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_6.2
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Hydra/0.1.8
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.29

Nome	HTTP Version Banner
Porta	82
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	82
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30000
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30001
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30001
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	49152
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.30

Nome	SSHd Version Banner
Porta	22
Dettagli	SSH-2.0-Mocana SSH 6.3
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.34

Nome	BIND/NAMED Version Banner
Porta	53
Dettagli	Microsoft DNS 6.1.7601 (1DB15F75)
Soluzione	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "" . If you have already made it return bogus information please ignore this check.

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-dropbear
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.37

Nome	FTP Version Banner
Porta	21
Dettagli	220 (vsFTPD 2.2.2)
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	SMTP Mail Server Version Banner
Porta	25
Dettagli	220 192.168.0.37 ESMTP Sendmail 8.14.3/8.14.3; Tue, 19 Sep 2023 15:34:57 +0200
Soluzione	It is highly advisable to configure this output to return bogus or no information at all. UNIX: Sendmail 1:Open up the sendmail.cf file 2:Find the line saying O SmtgGreetingMessage= PARAMETERS (Where the parameters can be several \$ codes) 3:Change the line to O SmtgGreetingMessage=\$j (And nothing more). WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level. If you have already removed the version please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	631
Dettagli	Apache

Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0
------------------	---

Nome	HTTP Version Banner
Porta	8080
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	20080
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.40

Nome	FTP Version Banner
Porta	21
Dettagli	220 (vsFTPd 2.2.2)
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	SMTP Mail Server Version Banner
Porta	25
Dettagli	220 192.168.0.40 ESMTP Sendmail 8.14.3/8.14.3; Thu, 27 Oct 2016 07:33:56 +0100
Soluzione	It is highly adviceable to configure this output to return bogus or no information at all. UNIX: Sendmail 1:Open up the sendmail.cf file 2:Find the line saying O SmtgGreetingMessage= PARAMETERS (Where the parameters can be several \$ codes) 3:Change the line to O SmtgGreetingMessage=\$j (And nothing more). WINDOWS: This is a more complicated process if running exchange and it is therefor recommended to remove at firewall level. If you have already removed the version please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	631
Dettagli	Apache

Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0
------------------	---

Nome	HTTP Version Banner
Porta	8080
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	20080
Dettagli	Apache
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.46

Nome	BIND/NAMED Version Banner
Porta	53
Dettagli	Microsoft DNS 6.1.7601 (1DB15F75)
Soluzione	It is recommended to configure the bind to return bogus information. This can be done by setting the named.conf version "" . If you have already made it return bogus information please ignore this check.

Nome	HTTP Version Banner
Porta	56000
Dettagli	wugg
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.54

Nome	HTTP Version Banner
Porta	3911
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	3911
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.62

Nome	HTTP Version Banner
Porta	82
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	82
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30000
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30001
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	30001
Dettagli	gSOAP/2.7
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.100

Nome	SSHd Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_8.1
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.101

Nome	SSHd Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_8.1
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.120

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-mpSSH_0.2.1
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.121

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-mpSSH_0.2.1
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.201

Nome	Telnet Version Banner
Porta	23
Dettagli	ZEM800 login:
Soluzione	It is highly advisable to configure this output to return bogus or no information at all.

Segnalatori di Versione per: 192.168.0.205

Nome	Telnet Version Banner
Porta	23
Dettagli	ZEM800 login:
Soluzione	It is highly advisable to configure this output to return bogus or no information at all.

Segnalatori di Versione per: 192.168.0.222

Nome	HTTP Version Banner
Porta	80
Dettagli	Web Switch
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	Telnet Version Banner
Porta	23
Dettagli	***** User Access Login *****;;User:

Soluzione	It is highly adviceable to configure this output to return bogus or no information at all.
------------------	--

Segnalatori di Versione per: 192.168.0.225

Nessuno

Segnalatori di Versione per: 192.168.0.235

Nessuno

Segnalatori di Versione per: 192.168.0.248

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	443
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	443
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.249

Nome	SSHD Version Banner
Porta	22
Dettagli	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTP Version Banner
Porta	443
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Nome	HTTPS Version Banner
Porta	443
Dettagli	nginx
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.251

Nome	FTP Version Banner
Porta	21
Dettagli	220 Nucleus FTP Server (Version 1.7) ready.
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Nome	HTTP Version Banner
Porta	80
Dettagli	Henry/1.1
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning. AttackString: HEAD / HTTP/1.0

Segnalatori di Versione per: 192.168.0.253

Nome	SSHd Version Banner
Porta	22
Dettagli	SSH-2.0-WAm_R
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

Segnalatori di Versione per: 192.168.0.254

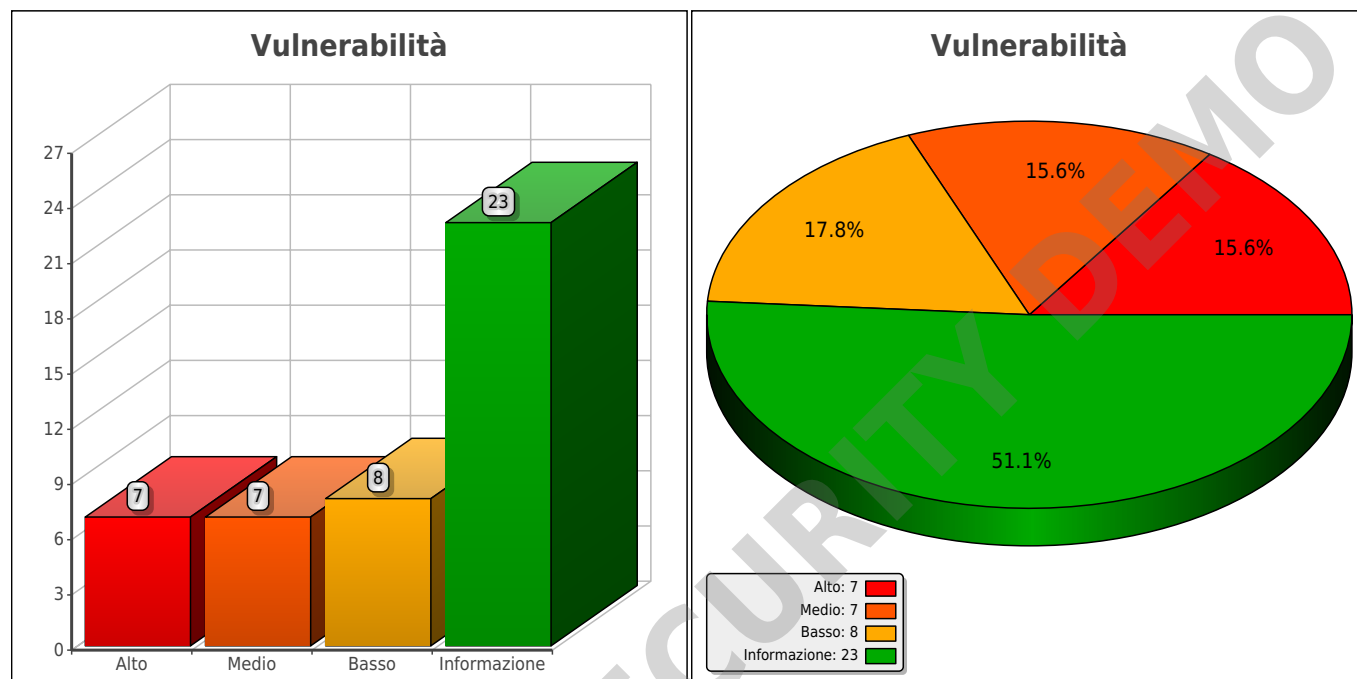
Nome	SSHd Version Banner
Porta	22

Dettagli	SSH-2.0-WAm_R
Soluzione	It is highly recommended to configure this output to return bogus or no information at all. If you have done that already please ignore this warning.

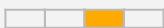
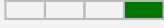
FRED FOR SECURITY DEMO

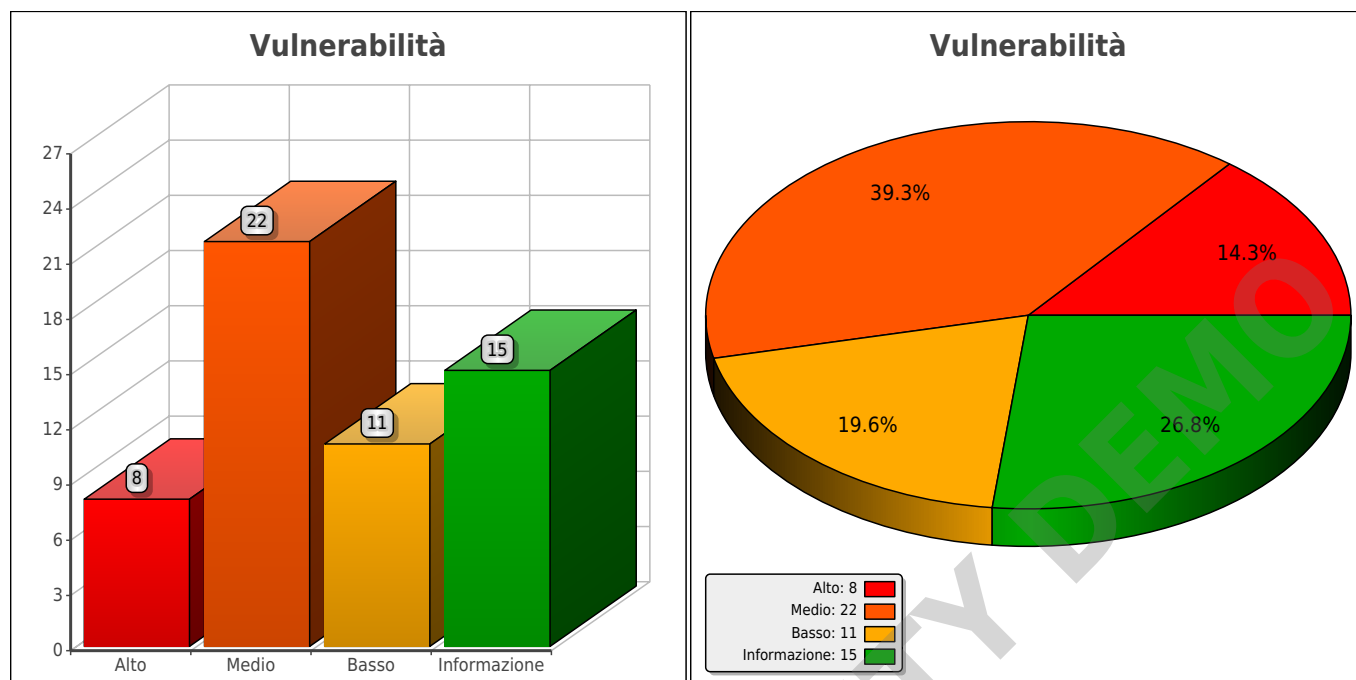
Elenco delle Vulnerabilità

Sistema Target: 192.168.0.1

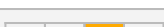
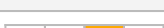


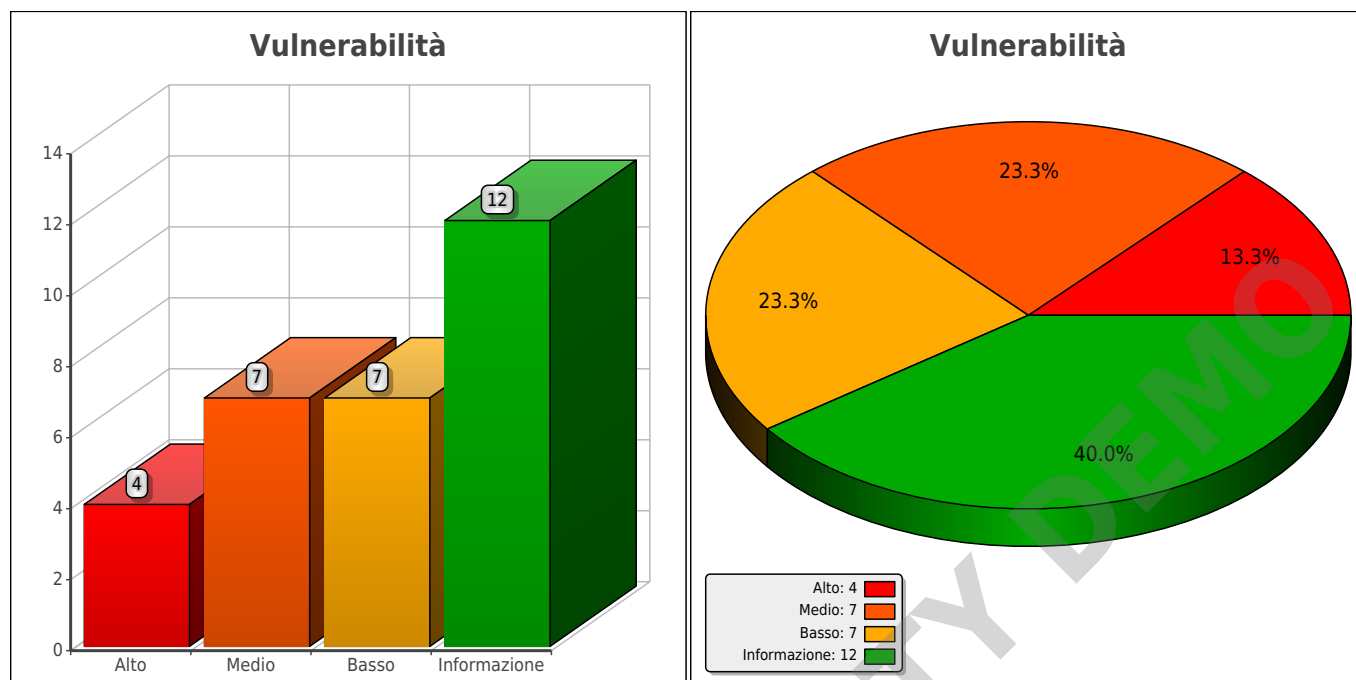
Livello rischio	Vulnerabilità
	Mail Server sent to files attack
	Mailto Files attack
	Windows Terminal Services RDP
	Microsoft SQL Server
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	Mail Server Decode Vulnerability
	File ?var?.cap Information Disclosure
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Lethal Attack 1 HTTP Crawler Cross Site Scripting Reflected XSRF
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag X-Content-Type-Options
	Missing Web Security Header Tag X-Xss-Protection HTTP
	NetBIOS service listening 137 UDP
	Possible Service/Game: pc game port Identified
	Web Login Box #check2
	HTTP only port without SSL found
	Lethal Attack 1 HTTP Internal Server Error
	MAC address obtained via NetBIOS

Livello rischio	Vulnerabilità
	It is possible to obtain remote NetBIOS name table
	NetBIOS service listening 139 TCP
	All Protocols Tested
	SMTP Ehlo Command
	Mailserver Help Command information
	Interesting directory HTTP /home/ Identified
	Interesting directory HTTP /workstation/ Identified
	Interesting directory HTTP /Home/ Identified
	Interesting directory HTTP /fileadmin/gymfyn/Almenp?d/Kurser/Midtvejs_Matematik_Materialer/Matematik kkens_metoder/ Identified
	Identified Operating System Check #2 Microsoft Windows via Banner
	MAC Address 00-50-56-8c-c5-05 VMware, Inc.
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	System time via remote Web Server
	SEO Check HTTP code 302 usage
	IIS Identified
	Web Server Application Firewall: Reason: The server header is different when an attack is detected.;
	Interesting directory HTTP /certificates/ Identified
	Interesting directory HTTP /Account/ Identified
	System Time Revealed via. ICMP TimeStamp Request
	Interesting directory HTTP /Home/Index/ Identified
	Interesting directory HTTP /Tempor?ra%20Internetfiler/Low/Content.IE5/ Identified
	Interesting directory HTTP /account/ Identified
	Interesting directory HTTP /account/login/ Identified
	Direct HTTP 334390 & HTTPS 0 Connections

Sistema Target: 192.168.0.2

Livello rischio	Vulnerabilità
	Microsoft SQL Server
	Messagequeue Server Execution Overflow
	MSSql service listening
	Windows Terminal Services RDP
	Delf acz ctf port Malware Backdoor Port Identified
	Microsoft Message Queueing Service
	RPC Port identified
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	Game: Orbz Buffer Overflow
	SCADA Web Client Alaram Server / Schneider / PowerSCADA System Identified 5504
	Missing Web Security Header Tag X-Xss-Protection HTTP
	File thisissimpleanexistentfile Information Disclosure
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag X-Content-Type-Options
	MySQL Service running
	Microsoft Windows RPC
	X11 Server / Microsoft Windows RPC over HTTP
	X11 Server
	Point-To-Point (PPTP) Protocol tcp port 1723 identified
	Lethal Attack 1 HTTP Crawler Cross Site Scripting XSS
	Lethal Attack 1 HTTP Crawler Cross Site Scripting Reflected XSRF

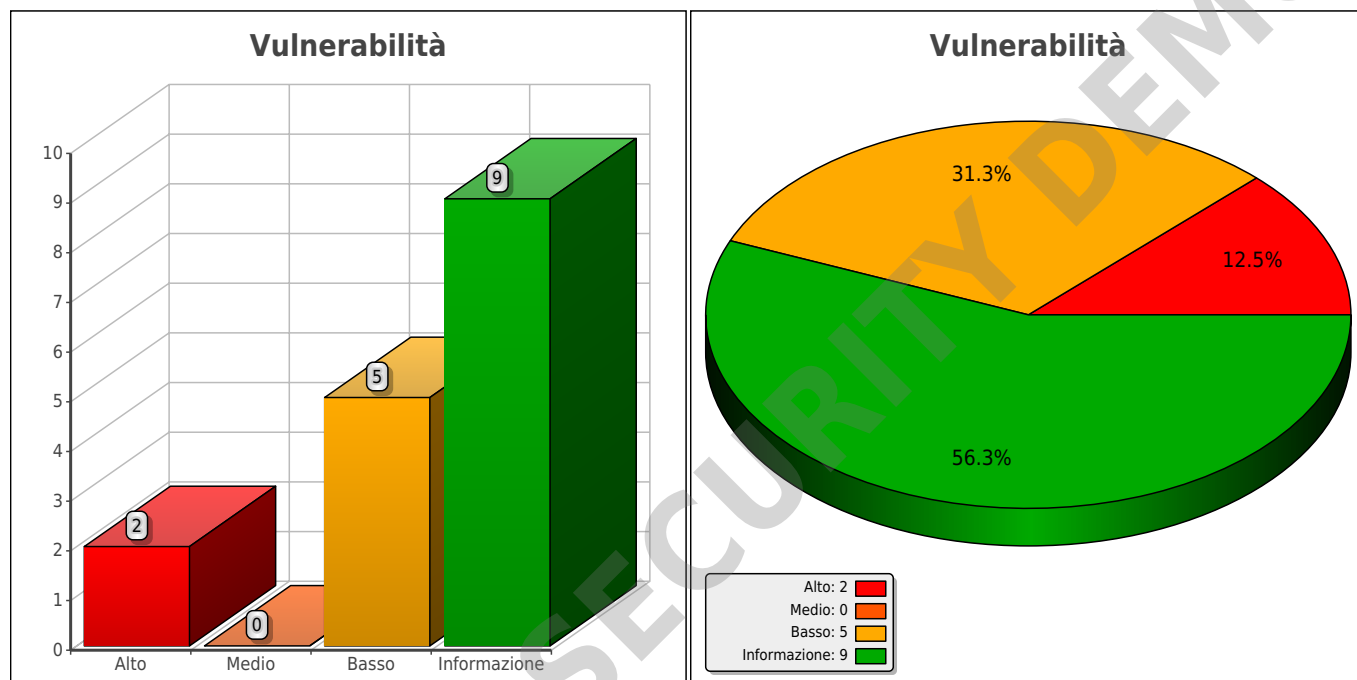
Livello rischio	Vulnerabilità
	Microsoft Windows 2107 tcp RPC
	Microsoft Windows 2105 tcp RPC
	X11 Sniff AttackServer
	Microsoft Windows 2103 tcp RPC
	DNS Recursion Allowed
	Lightweight Directory Access Protocol (LDAP)
	NetBIOS service listening 139 TCP
	NetBIOS service listening 137 UDP
	Possible Service/Game: Tales of Pirates Identified
	Possible Service/Game: kerberos firewall off can leak operating system Identified
	It is possible to obtain remote NetBIOS name table
	LDAP Service
	MAC address obtained via NetBIOS
	Web Server Path Disclosure
	HTTP only port without SSL found
	Possible Service/Game: Star Wars Identified
	NTPd Service found PORT 123 TCP
	Identified Operating System Check #2 Microsoft Windows via Banner
	All Protocols Tested
	Web Server Application Firewall: Reason: The server header is different when an attack is detected.;
	IIS Identified
	Identified Operating System Windows 7 or 8 via Packet Check #3
	SSL Client Information
	SSL Certificate information
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN
	System Time Revealed via. ICMP TimeStamp Request
	Direct HTTP 334616 & HTTPS 1 Connections

Sistema Target: 192.168.0.3

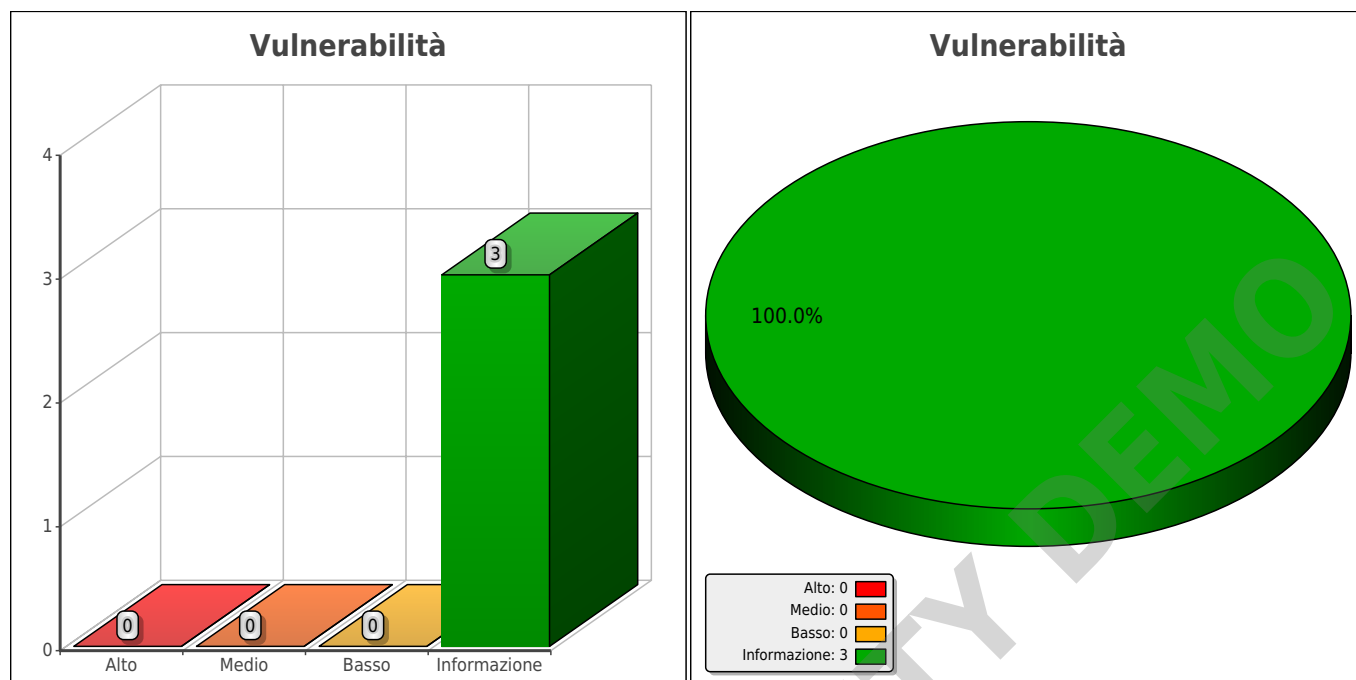
Livello rischio	Vulnerabilità
	SCADA System RSH RUGGEDCOM RS910 Overflow
	Backdoor WinRemoteShell / IBM Tivoli ODBC Command Execution
	SSH Service Accessible
	zoom remote exploit Port Identified
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Jetty Web Server File Geronimo cal2.jsp Cross Site Scripting
	Rsh service on TCP port 514
	Syslog service found on UDP 514
	Lightweight Directory Access Protocol (LDAP)
	HTTP only port without SSL found
	LDAP Service
	Web Server Path Disclosure
	Possible Service/Game: kerberos firewall off can leak operating system Identified
	Possible Service/Game: OpenEye Server Identified
	Possible Service/Game: X10 AirSight XX39A Identified
	All Protocols Tested
	Interesting directory HTTP /vci/downloads/ Identified
	Possible Web Server Application Firewall: The site http://192.168.0.3:9084 is behind a SecureIIS;
	MAC Address 00-0c-29-55-3a-09 VMware, Inc.
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	SSL Client Information
	SSL Certificate information

Livello rischio	Vulnerabilità
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 9443
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
	System time via remote Web Server
	Remote system answers to PING command
	Direct HTTP 501636 & HTTPS 2 Connections

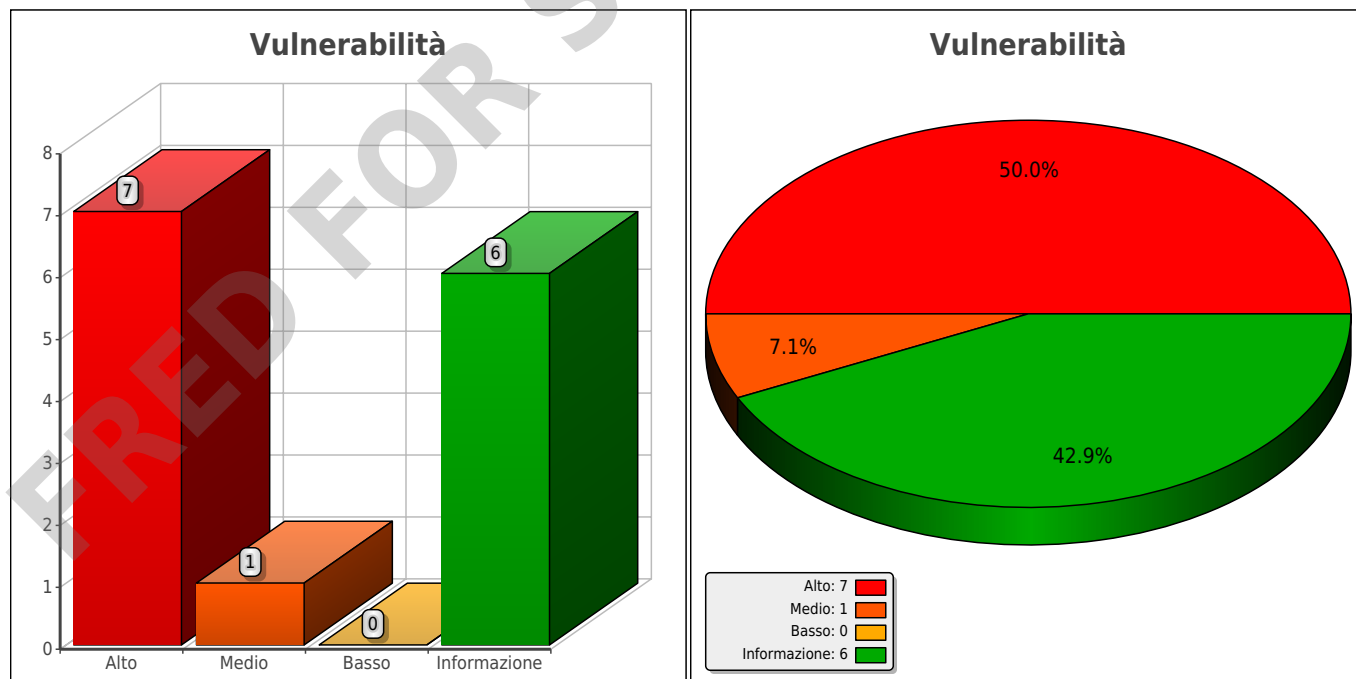
Sistema Target: 192.168.0.4



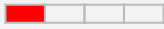
Livello rischio	Vulnerabilità
	Windows Terminal Services RDP
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	It is possible to obtain remote NetBIOS name table
	MAC address obtained via NetBIOS
	HTTP only port without SSL found
	NetBIOS service listening 137 UDP
	NetBIOS service listening 139 TCP
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	MAC Address 00-50-56-8c-c3-03 VMware, Inc.
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	System time via remote Web Server
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Identified Operating System Check #2 Microsoft Windows via Banner
	Direct HTTP 167181 & HTTPS 0 Connections

Sistema Target: 192.168.0.13

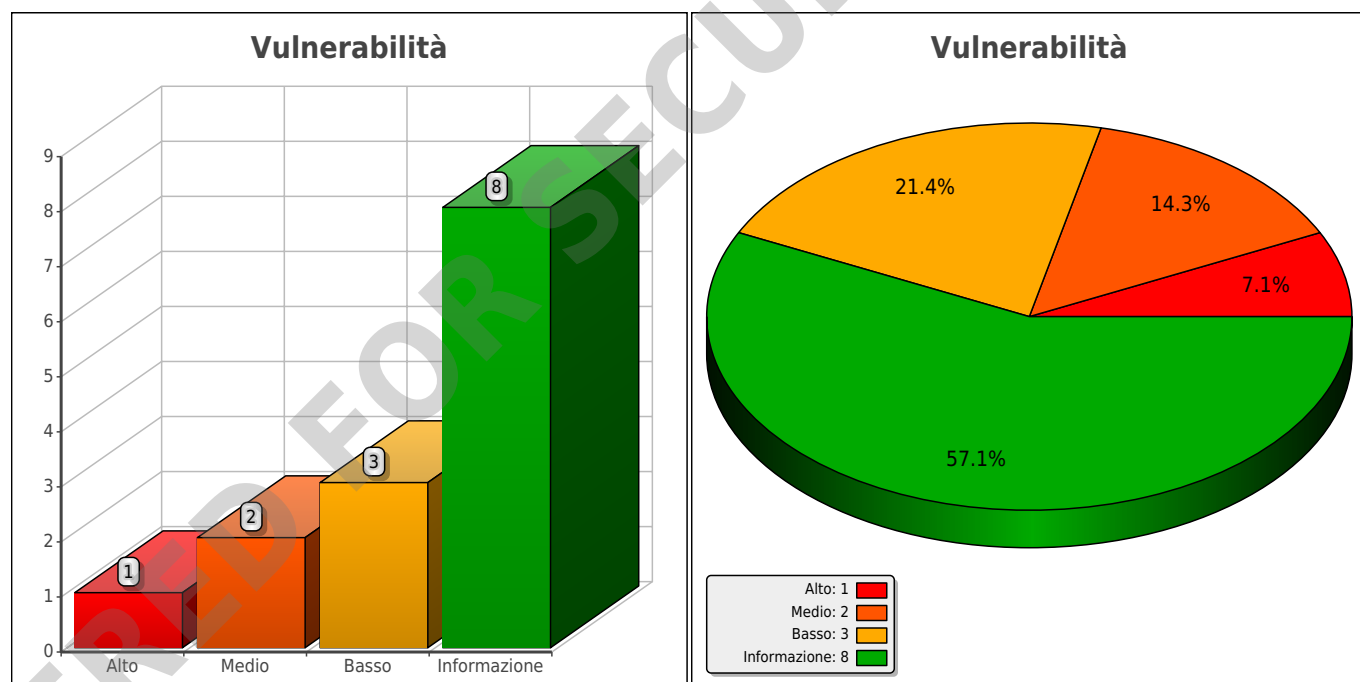
Livello rischio	Vulnerabilità
	MAC Address 28-29-86-04-61-53 APC by Schneider Electric
	Remote system answers to PING command
	Direct HTTP 0 & HTTPS 0 Connections

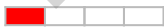
Sistema Target: 192.168.0.17

Livello rischio	Vulnerabilità
	Directory OCR ANPR Camera Traversal LFI
	File sgms/auth Authentication Bypass
	File /swarm.cgi Aruba Instant Remote Command Execution (RCE)

Livello rischio	Vulnerabilità
	File 80sec内部专用过世界杀软体积最小功能超强超猛宇宙第一.asp Information Disclosure webshell
	File Jspspy%20web~shell%20V1.0%20*MADE%20by%20孤水绕城%20QQ540410588.jsp Information Disclosure webshell
	File MYSQL%20Manager%20-Asp.net%20Silic%20Group%20Hacker%20Army专用版本.aspx Information Disclosure webshell
	File response_packet_from_icmpsh_slave_containing_output_of_command_whoami.png Information Disclosure webshell
	File shell~ Information Disclosure webshell
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	MAC Address d0-15-a6-cc-28-64 Adapter manufacturer: UNKNOWN
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	System time via remote Web Server

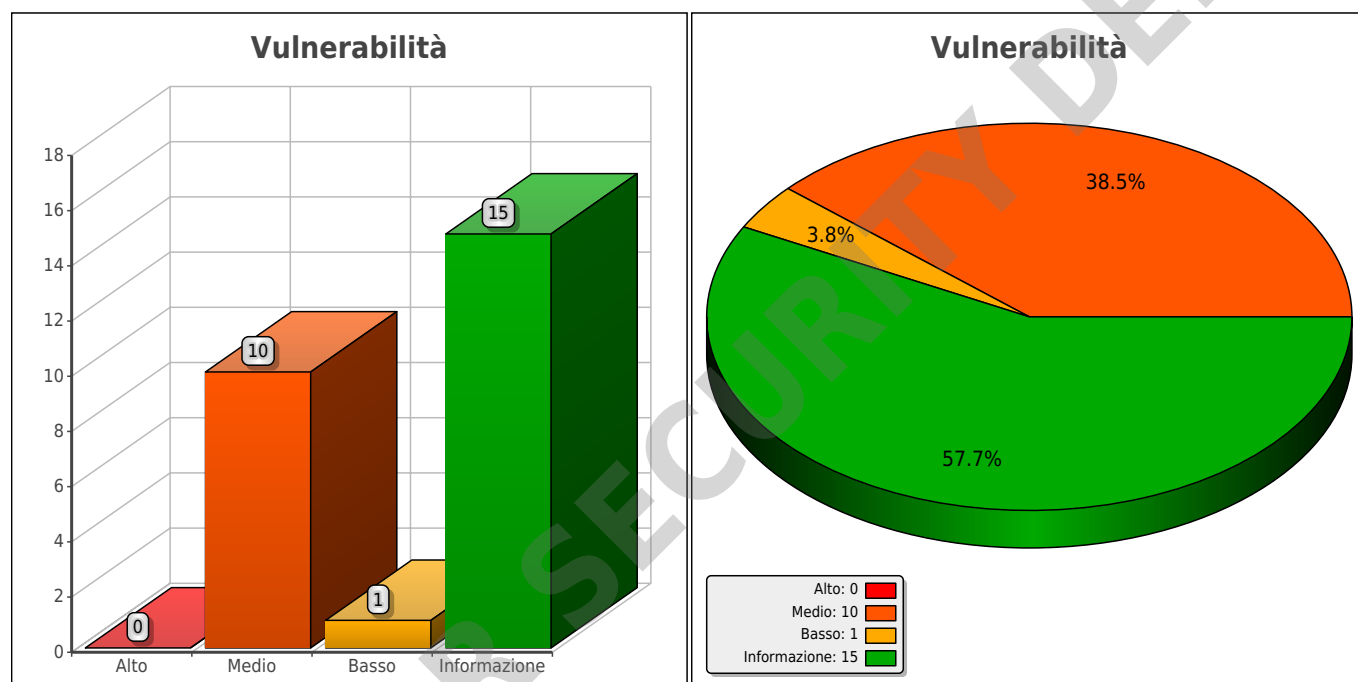
Sistema Target: 192.168.0.25



Livello rischio	Vulnerabilità
	SSH Service Accessible
	DNS Recursion Allowed
	8081 Port Identification
	HTTP only port without SSL found
	ASP.NET path disclosure
	Possible Service/Game: directtv Identified
	Identified Operating System Check #2 Microsoft Windows via Banner

Livello rischio	Vulnerabilità
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	MAC Address e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Direct HTTP 334382 & HTTPS 0 Connections

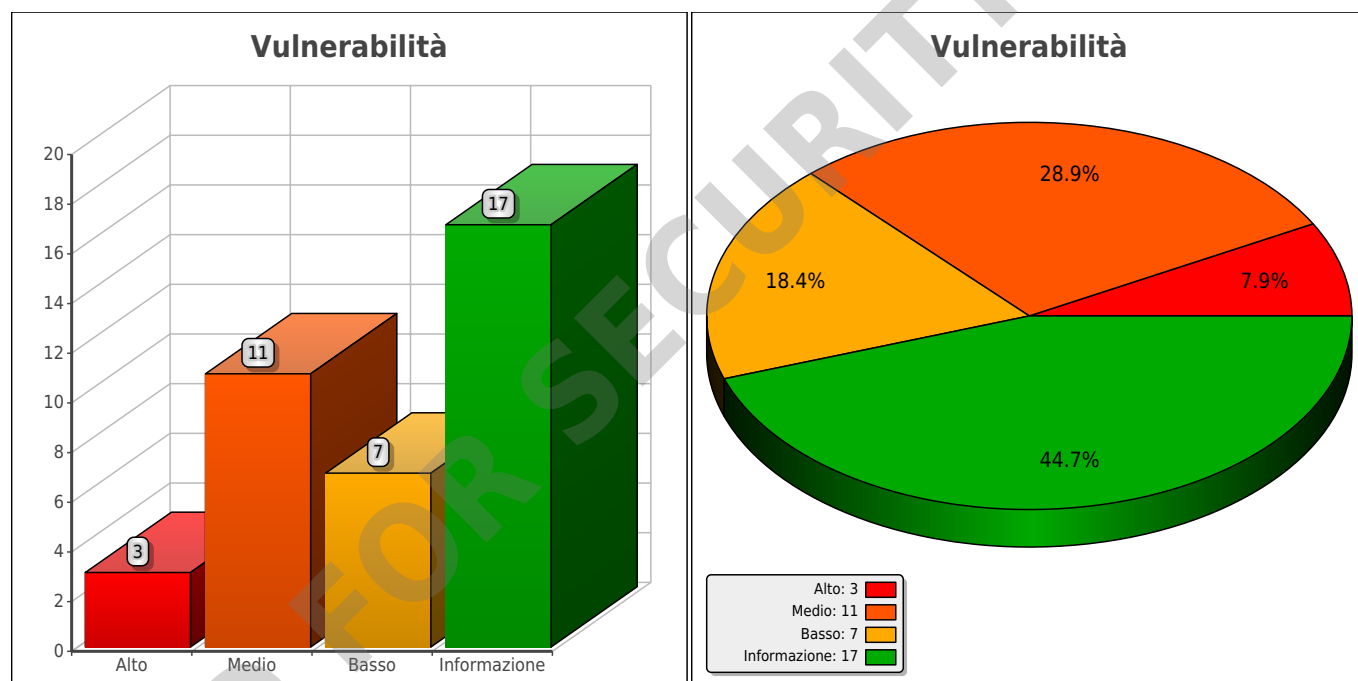
Sistema Target: 192.168.0.27



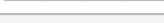
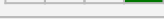
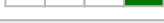
Livello rischio	Vulnerabilità
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag Strict-Transport-Security
	File /js/home.js Information Disclosure
	File /home.html Information Disclosure
	Missing Web Security Header Tag Permissions-Policy
	SSL PFS Forward Secrecy Check
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Content-Type-Options
	HTTP only port without SSL found
	Interesting directory HTTP /help/ Identified
	Interesting directory HTTP /./ Identified
	Interesting directory HTTP /%00/ Identified
	Interesting directory HTTP /%00/interact.sh/ Identified

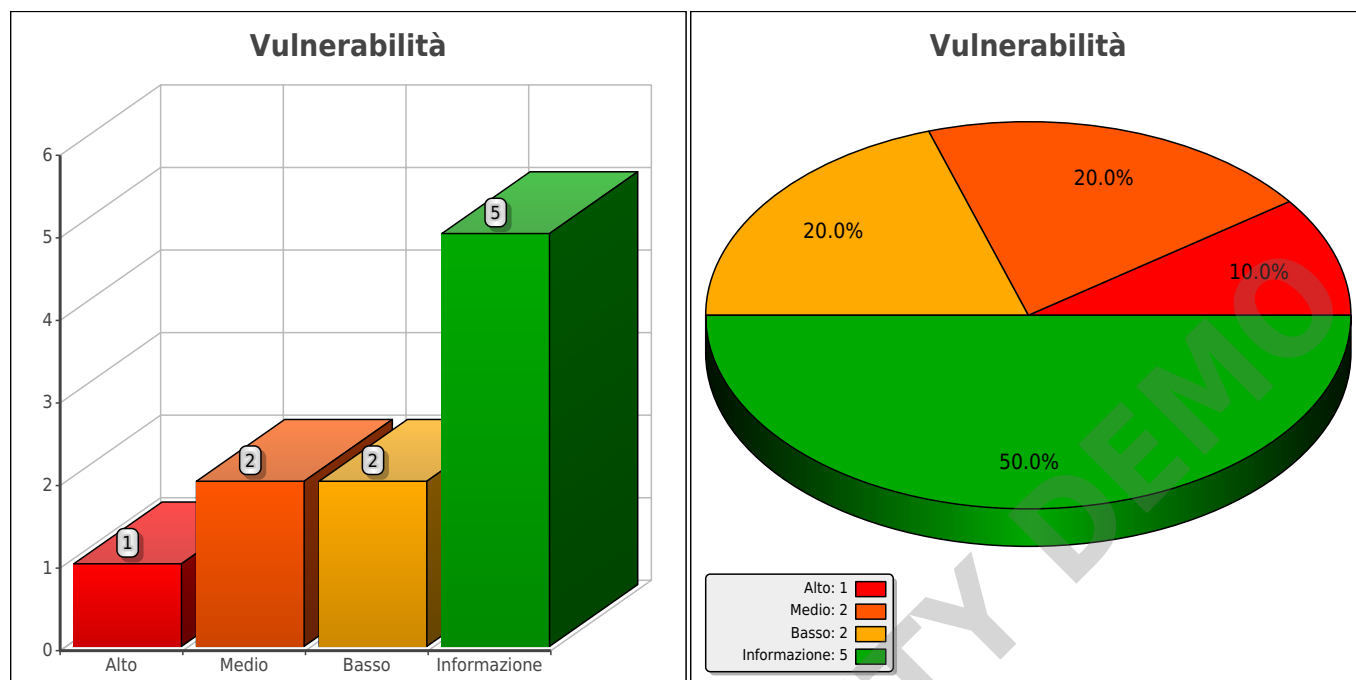
Livello rischio	Vulnerabilità
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	SSL Client Information
	SSL Certificate information
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address b0-7d-47-37-98-d4 Cisco Systems, Inc
	File /login.html admin interface identified

Sistema Target: 192.168.0.29

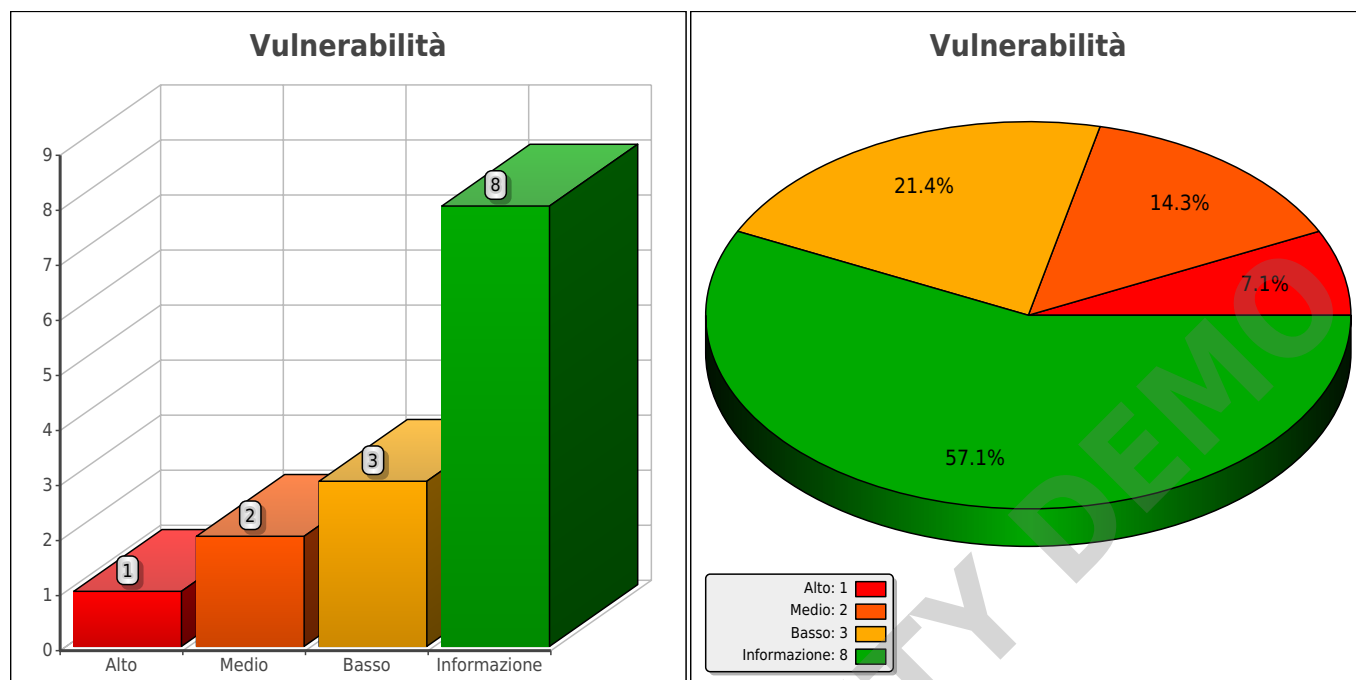


Livello rischio	Vulnerabilità
	Apple RTSP quicktime Remote Preauth Code Execution
	X Font Service found on the remote system
	Microsoft(R) Biztalk Server Vulnerability
	ctf australia 2014 / SCADA PLC RUGGEDCOM DNP3 System Identified
	Missing Web Security Header Tag X-Content-Type-Options
	uTorrent Peer to Peer Web Server
	Web Server Authentication Method NTLM Disclosure
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Permissions-Policy

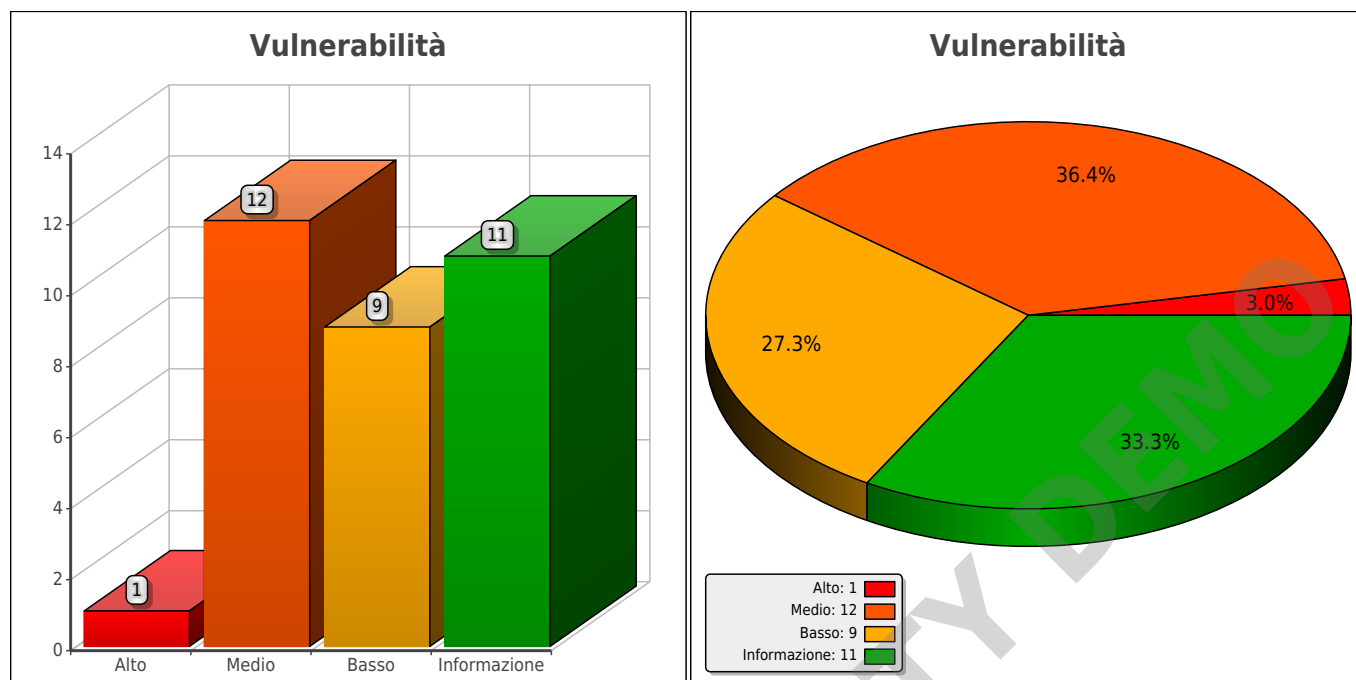
Livello rischio	Vulnerabilità
	Web Server Authentication Method Basic Disclosure
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Sage Content Management System Cross Site Scripting
	Oracle 9iAS Access of SOAP documentation
	File userslist.asp Path Disclosure
	ASP.NET path disclosure
	Possible Service/Game: Star Wars Identified
	Possible Service/Game: freephoneline Identified
	HTTP only port without SSL found
	Lethal Attack 1 HTTP Possible CGI
	Identified Operating System Check #2 Linux via Banner
	All Protocols Tested
	Interesting directory HTTP ../ Identified
	Identified Operating System Check #2 Linux via Banner
	MAC Address 48-ea-63-bb-4f-55 Zhejiang Uniview Technologies Co., Ltd.
	Interesting directory HTTP ../../../../ Identified
	Interesting directory HTTP /../ Identified
	Interesting directory HTTP /../ Identified
	Interesting directory HTTP /../ Identified
	Interesting directory HTTP /../ Identified
	Interesting directory HTTP /.. Identified
	Interesting directory HTTP /..%00/ Identified
	Interesting directory HTTP /..%00 Identified
	Interesting directory HTTP /%00/ Identified
	Interesting directory HTTP /%00/interact.sh/ Identified
	System time via remote Web Server
	Remote system answers to PING command
	Direct HTTP 784276 & HTTPS 0 Connections

Sistema Target: 192.168.0.30


Livello rischio	Vulnerabilità
	SSH Service Accessible
	Target ip address system reverses traffic
	Telnet Service
	HTTP only port without SSL found
	SNMP service detected on udp
	All Protocols Tested
	MAC Address 20-67-7c-9f-33-80 Hewlett Packard Enterprise
	Remote system answers to PING command
	Identified Operating System Windows XP via Packet Check #3
	Direct HTTP 5805 & HTTPS 0 Connections

Sistema Target: 192.168.0.34

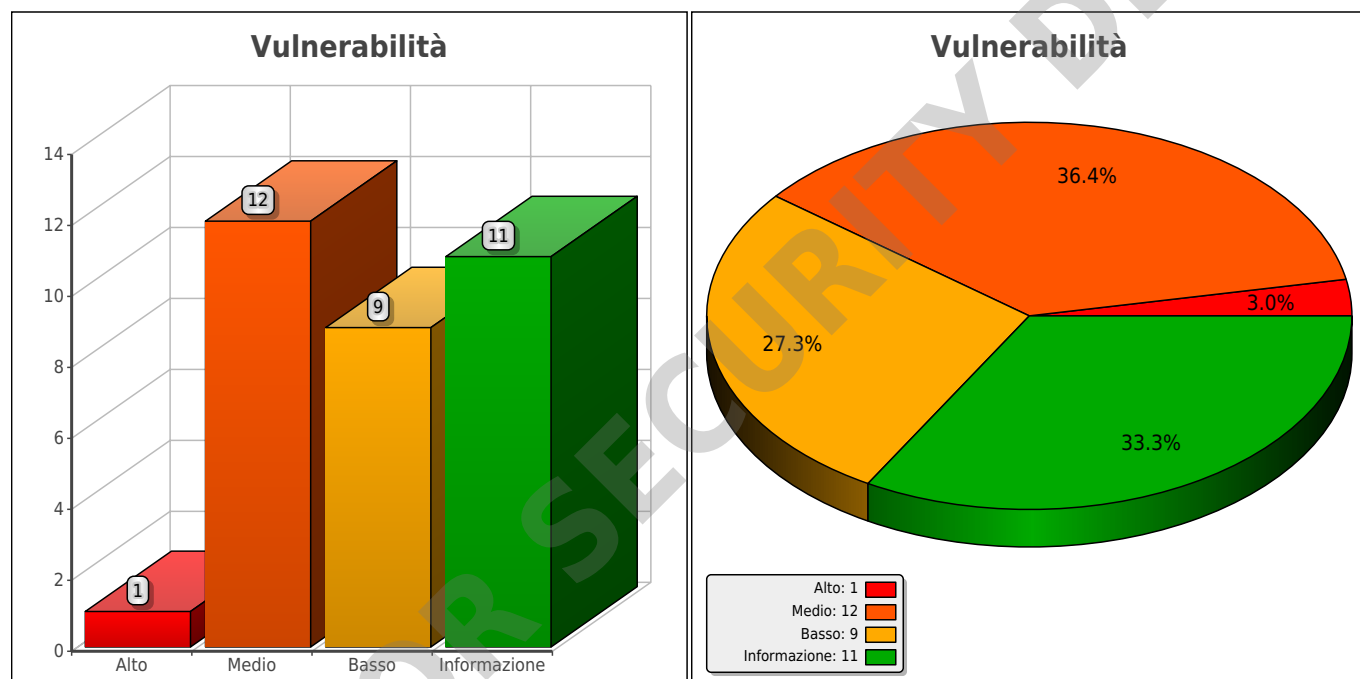
Livello rischio	Vulnerabilità
	SSH Service Accessible
	DNS Recursion Allowed
	8081 Port Identification
	HTTP only port without SSL found
	ASP.NET path disclosure
	Possible Service/Game: directtv Identified
	Identified Operating System Check #2 Microsoft Windows via Banner
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	MAC Address ac-86-74-6f-8f-c0 Open Mesh, Inc.
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Direct HTTP 335610 & HTTPS 0 Connections

Sistema Target: 192.168.0.37

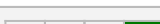
Livello rischio	Vulnerabilità
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	Missing Web Security Header Tag Strict-Transport-Security
	DeleGate Web Server Denial of Service
	vsftpd DoS
	VMware ESXI / Possible Novell Client running Port 427 TCP
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Content-Type-Options
	NetBIOS User Name Retrieval #1
	Open Netbios Shares Without Username and Password
	Open Netbios Shares
	Sendmail Man in the Middle Attacks
	List of Netbios service lists installed
	HTTP only port without SSL found
	NetBIOS service listening 137 UDP
	MAC address obtained via NetBIOS
	It is possible to obtain remote NetBIOS name table
	HP Laserjet or brand Printer Identified
	NetBIOS service listening 139 TCP
	SNMP service detected on udp
	Printer Spooler access port 515 TCP
	SMTP Ehlo Command
	All Protocols Tested
	Mailserver Help Command information

Livello rischio	Vulnerabilità
	Possible Web Server Application Firewall: The site http://192.168.0.37:631 is behind a SecureIIS;
	System Time Revealed via ICMP TimeStamp Request
	Identified Operating System Linux 3.x via Packet Check #3
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address 00-80-91-b9-bb-29 TOKYO ELECTRIC CO.,LTD
	Direct HTTP 503536 & HTTPS 0 Connections

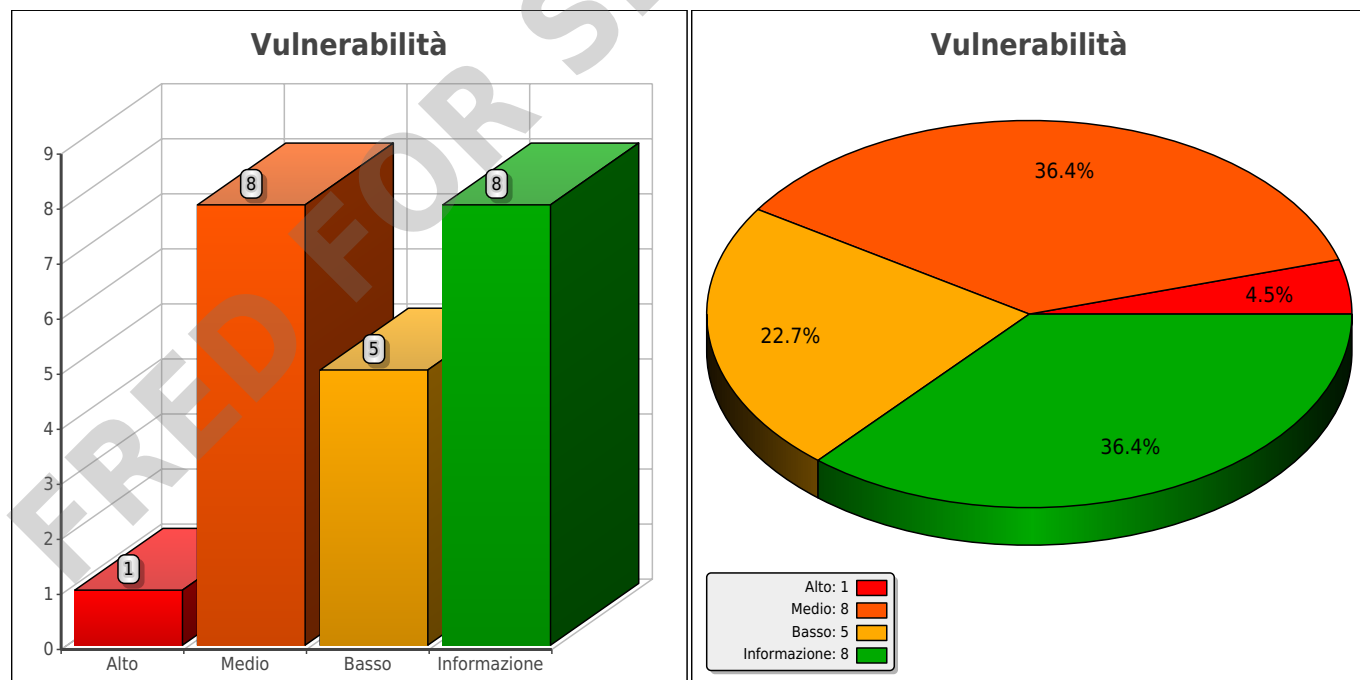
Sistema Target: 192.168.0.40



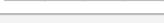
Livello rischio	Vulnerabilità
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	Missing Web Security Header Tag Strict-Transport-Security
	DeleGate Web Server Denial of Service
	vsftpd DoS
	VMware ESXI / Possible Novell Client running Port 427 TCP
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Content-Type-Options
	NetBIOS User Name Retrieval #1
	Open Netbios Shares Without Username and Password
	Open Netbios Shares
	Sendmail Man in the Middle Attacks
	List of Netbios service lists installed

Livello rischio	Vulnerabilità
	HTTP only port without SSL found
	NetBIOS service listening 137 UDP
	MAC address obtained via NetBIOS
	It is possible to obtain remote NetBIOS name table
	HP Laserjet or brand Printer Identified
	NetBIOS service listening 139 TCP
	SNMP service detected on udp
	Printer Spooler access port 515 TCP
	SMTP Ehlo Command
	All Protocols Tested
	Mailserver Help Command information
	Possible Web Server Application Firewall: The site http://192.168.0.40:631 is behind a SecureIIS;
	System Time Revealed via. ICMP TimeStamp Request
	Identified Operating System Linux 3.x via Packet Check #3
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address 00-80-91-b8-52-1b TOKYO ELECTRIC CO.,LTD
	Direct HTTP 503536 & HTTPS 0 Connections

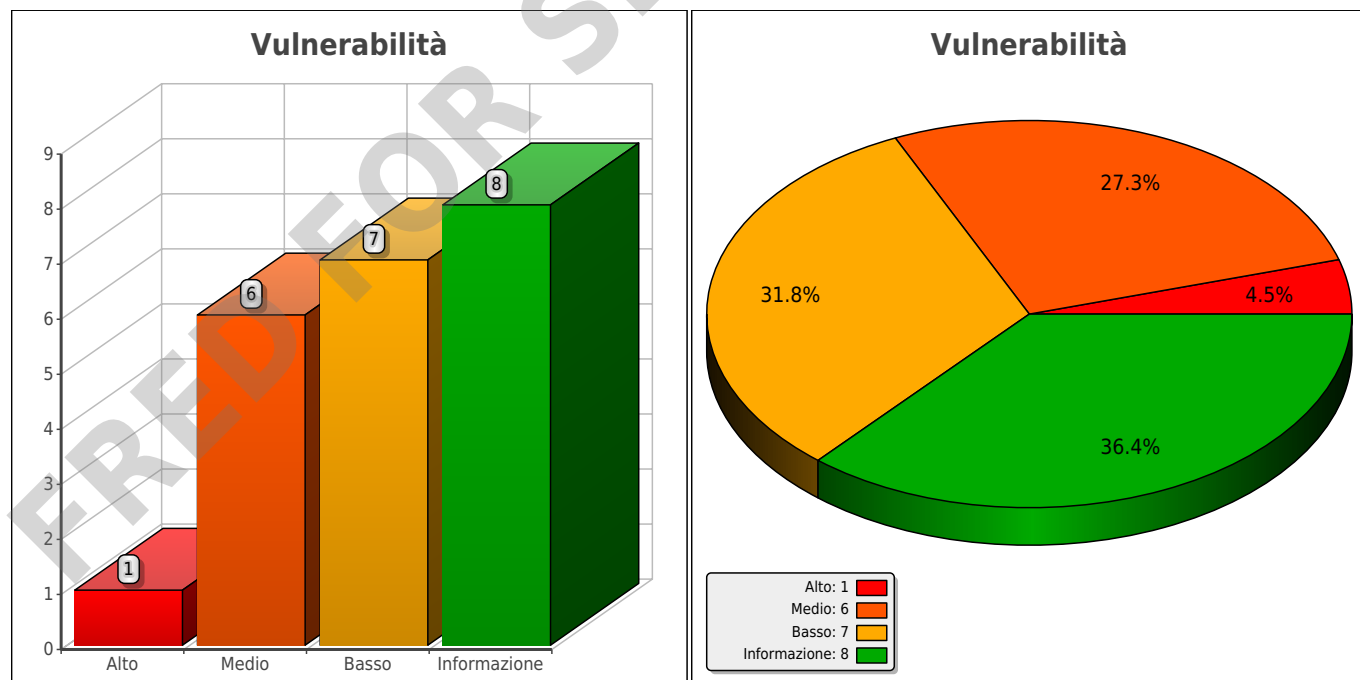
Sistema Target: 192.168.0.46



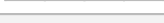
Livello rischio	Vulnerabilità
	Windows Terminal Services RDP
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Missing Web Security Header Tag Strict-Transport-Security

Livello rischio	Vulnerabilità
	Missing Web Security Header Tag Permissions-Policy
	DNS Recursion Allowed
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag X-Content-Type-Options
	NetBIOS service listening 139 TCP
	NetBIOS service listening 137 UDP
	It is possible to obtain remote NetBIOS name table
	MAC address obtained via NetBIOS
	HTTP only port without SSL found
	Identified Operating System Check #2 Microsoft Windows via Banner
	All Protocols Tested
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address 00-28-f8-30-ae-2b Intel Corporate
	System Time Revealed via. ICMP TimeStamp Request
	Direct HTTP 2608 & HTTPS 0 Connections

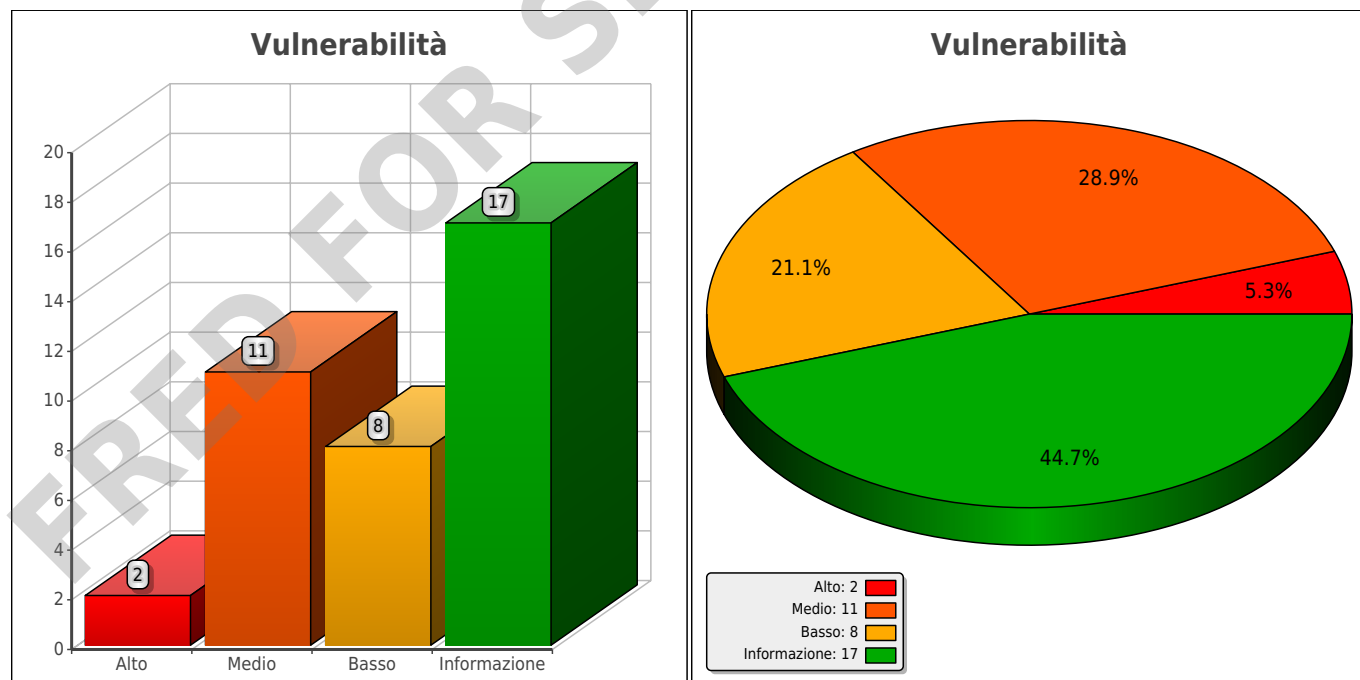
Sistema Target: 192.168.0.54



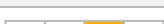
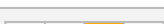
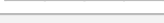
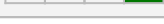
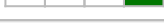
Livello rischio	Vulnerabilità
	Microsoft(R) Biztalk Server Vulnerability
	Missing Web Security Header Tag Permissions-Policy
	Easycom/safecom Print Server Remote Denial of Service

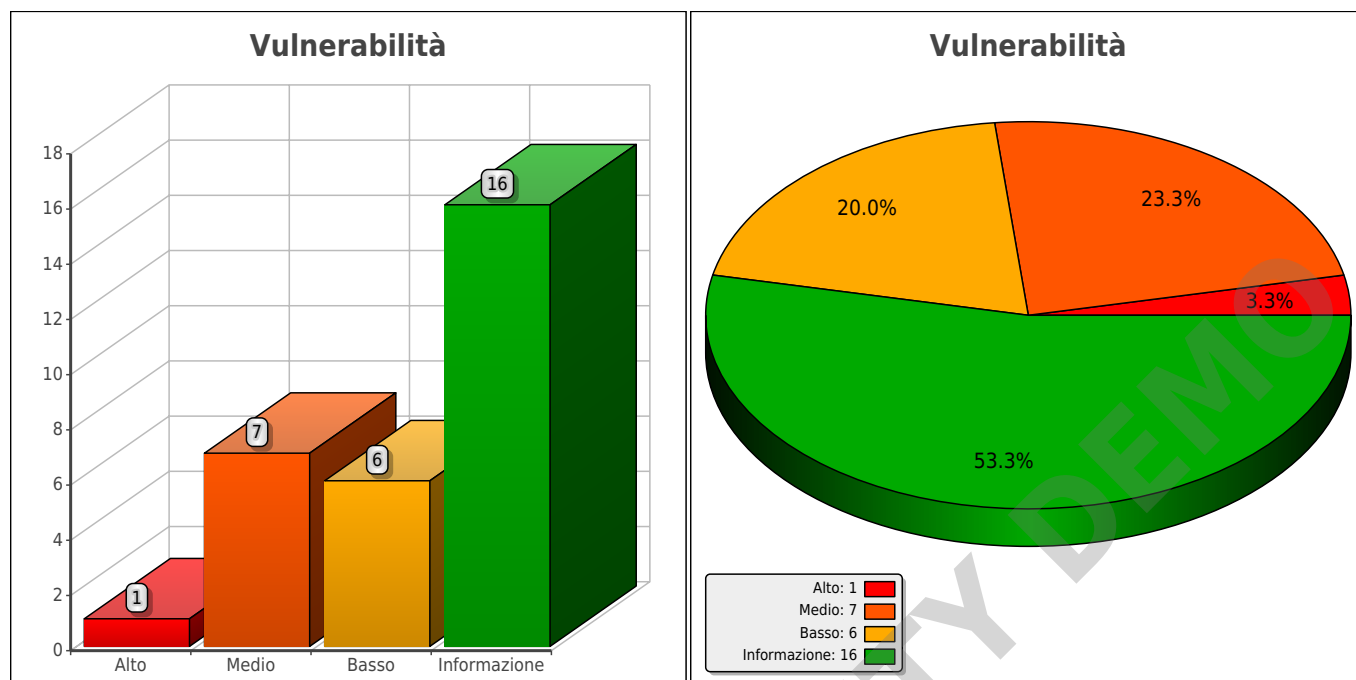
Livello rischio	Vulnerabilità
	CUPS Service Identified
	SSL PFS Forward Secrecy Check
	Missing Web Security Header Tag X-Xss-Protection SSL
	Missing Web Security Header Tag Referrer-Policy SSL
	ASP.NET path disclosure
	Printer Spooler access port 515 TCP
	HTTP only port without SSL found
	SNMP service detected on udp
	unsafe Web Security Header Tag Content-Security-Policy
	HP Laserjet or brand Printer Identified
	Oracle 9iAS Access of SOAP documentation
	All Protocols Tested
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	MAC Address e0-70-ea-fa-de-fa HP Inc.
	SSL Client Information
	SSL Certificate information
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
	Remote system answers to PING command
	Direct HTTP 167834 & HTTPS 2 Connections

Sistema Target: 192.168.0.62



Livello rischio	Vulnerabilità
	Apple RTSP quicktime Remote Preauth Code Execution
	Microsoft(R) Biztalk Server Vulnerability
	Missing Web Security Header Tag X-Content-Type-Options

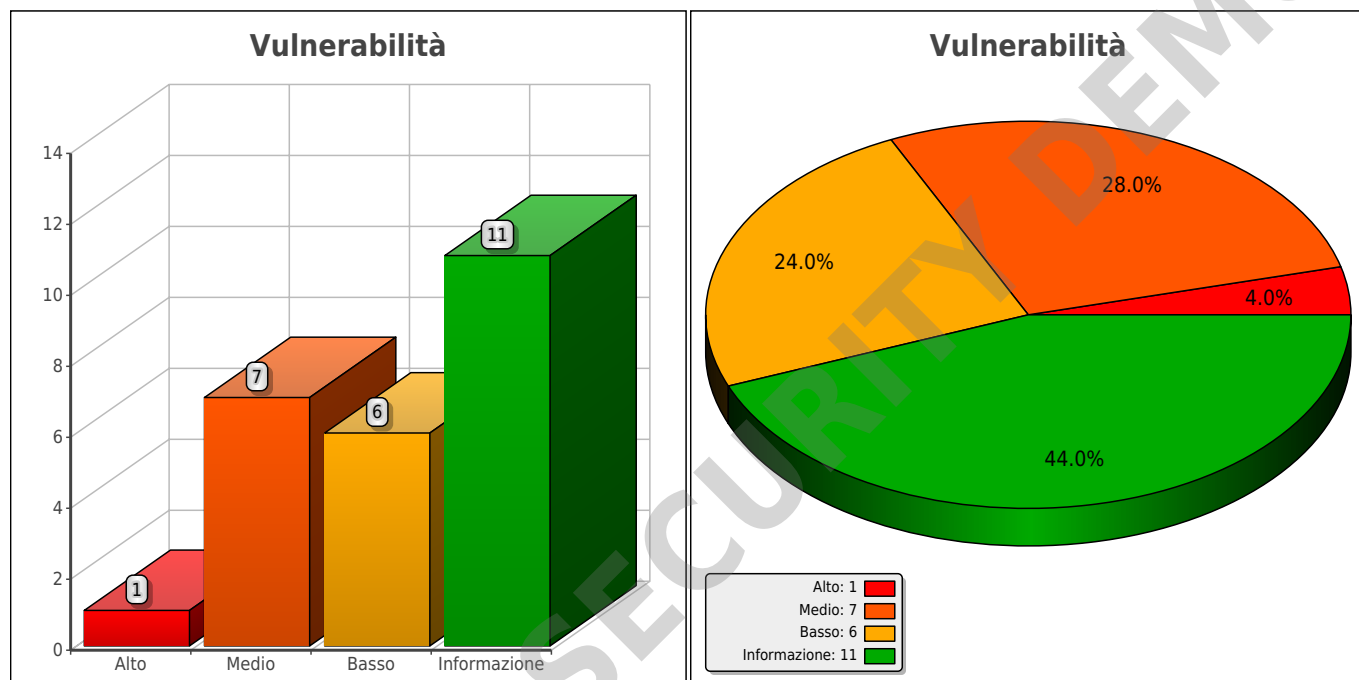
Livello rischio	Vulnerabilità
	uTorrent Peer to Peer Web Server
	Web Server Authentication Method Basic Disclosure
	Web Server Authentication Method NTLM Disclosure
	ctf australia 2014 / SCADA PLC RUGGEDCOM DNP3 System Identified
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag Permissions-Policy
	Sage Content Management System Cross Site Scripting
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Missing Web Security Header Tag Content-Security-Policy
	ASP.NET path disclosure
	File userslist.asp Path Disclosure
	Possible Service/Game: freephoneline Identified
	Internal IP disclosure Check #3 192.168.
	Oracle 9iAS Access of SOAP documentation
	unsafe Web Security Header Tag Content-Security-Policy
	HTTP only port without SSL found
	Lethal Attack 1 HTTP Possible CGI
	All Protocols Tested
	Interesting directory HTTP /.../.../ Identified
	Identified Operating System Check #2 Linux via Banner
	Interesting directory HTTP /../ Identified
	MAC Address 48-ea-63-89-94-cf Zhejiang Uniview Technologies Co., Ltd.
	Interesting directory HTTP /...../ Identified
	Interesting directory HTTP /...../ Identified
	Interesting directory HTTP /...../ Identified
	Interesting directory HTTP /.. Identified
	Interesting directory HTTP /..%00/ Identified
	Interesting directory HTTP /..%00 Identified
	Interesting directory HTTP /%00/ Identified
	Interesting directory HTTP /%00/interact.sh/ Identified
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	System time via remote Web Server
	Remote system answers to PING command
	Direct HTTP 648478 & HTTPS 0 Connections

Sistema Target: 192.168.0.100

Livello rischio	Vulnerabilità
	SSH Service Accessible
	Missing Web Security Header Tag X-Xss-Protection HTTP
	VMWare ESXi / Novell Groupwise Messenger Detection TCP
	VMware ESXI / Possible Novell Client running Port 427 TCP
	Missing Web Security Header Tag Permissions-Policy
	Allaire /%3f.jsp JRun Directory browsing Vulnerability
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag X-Frame-Options
	VMware Authentication Daemon
	VMware Auth Service Identification
	Possible Service/Game: Remote Potato Identified
	Possible Service/Game: X-Lite Identified
	Web Server Path Disclosure
	HTTP only port without SSL found
	All Protocols Tested
	SSL Client Information
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	System Time Revealed via. ICMP TimeStamp Request
	SSL Certificate information
	File /ui/index.html Information Disclosure
	Interesting directory /ui/ HTTPS
	Interesting directory // HTTPS
	Interesting directory ../ HTTPS
	Interesting directory ./ HTTPS
	Interesting directory /%3f/ HTTPS

Livello rischio	Vulnerabilità
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address 08-f1-ea-93-cd-fe Hewlett Packard Enterprise
	Direct HTTP 167885 & HTTPS 160331 Connections

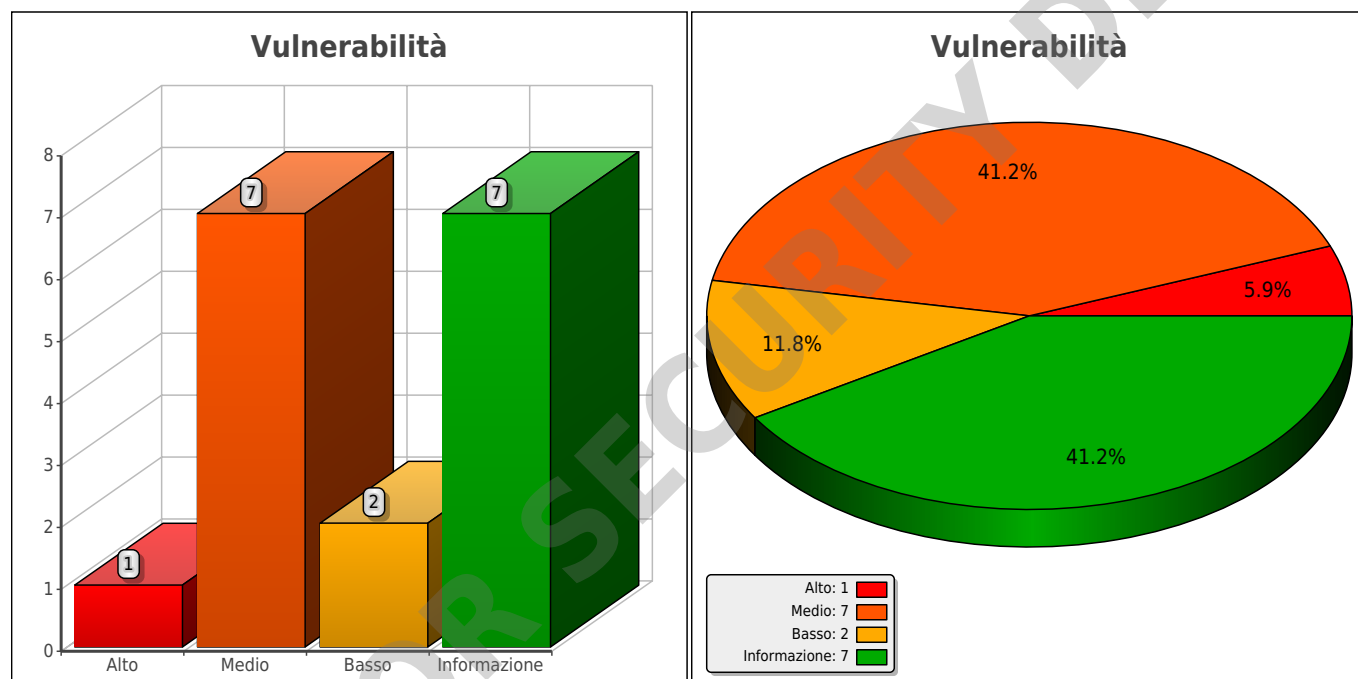
Sistema Target: 192.168.0.101



Livello rischio	Vulnerabilità
	SSH Service Accessible
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Missing Web Security Header Tag Referrer-Policy
	VMWare ESXi / Novell Groupwise Messenger Detection TCP
	VMware ESXI / Possible Novell Client running Port 427 TCP
	Allaire /%3f.jsp JRun Directory browsing Vulnerability
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag X-Frame-Options
	VMware Authentication Daemon
	VMware Auth Service Identification
	HTTP only port without SSL found
	Possible Service/Game: Remote Potato Identified
	Possible Service/Game: X-Lite Identified
	Web Server Path Disclosure
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	Identified Operating System Windows XP via Packet Check #3

Livello rischio	Vulnerabilità
	SSL Client Information
	SSL Certificate information
	File /ui/index.html Information Disclosure
	System time via remote Web Server
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address 08-f1-ea-93-c4-50 Hewlett Packard Enterprise
	Direct HTTP 167885 & HTTPS 56380 Connections

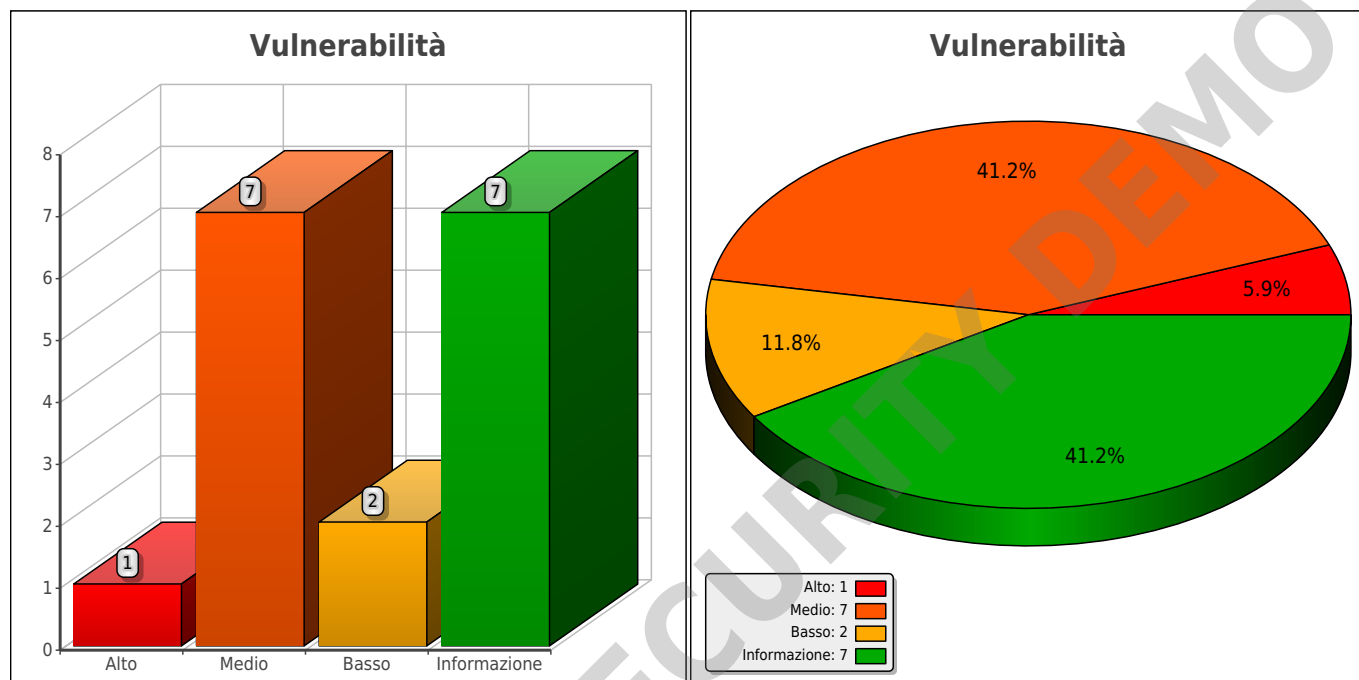
Sistema Target: 192.168.0.120



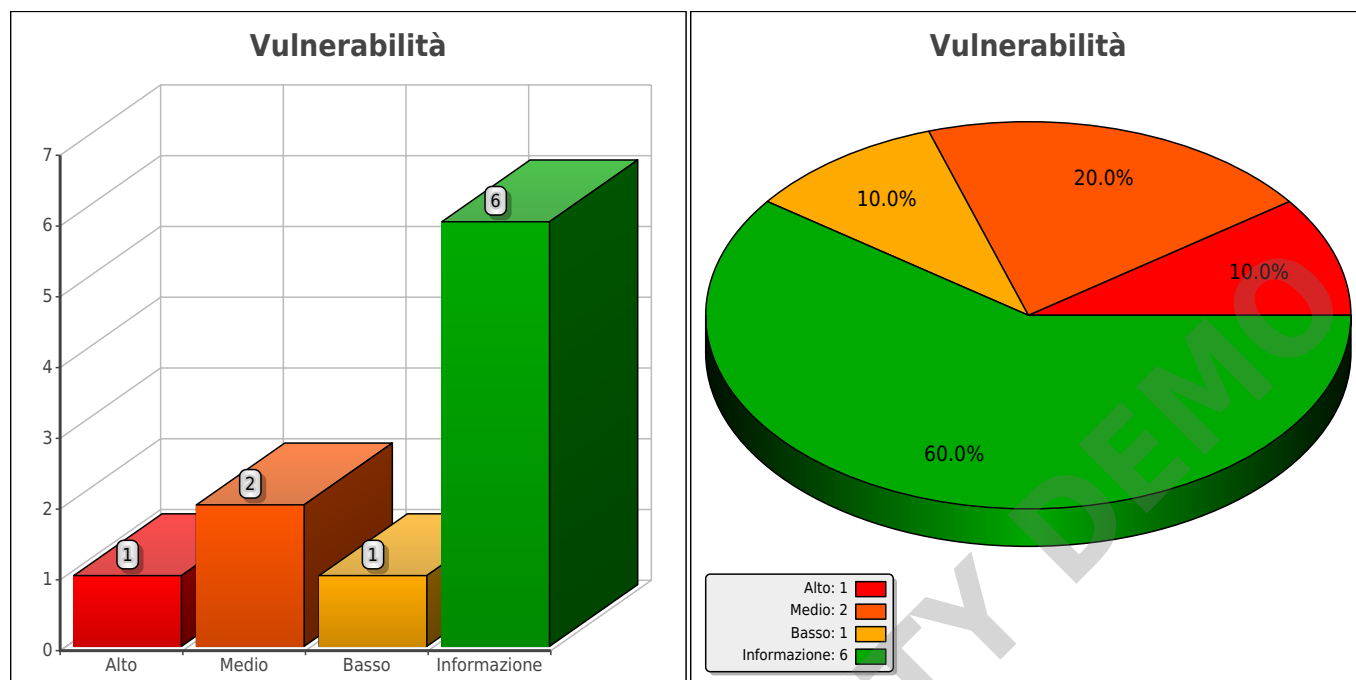
Livello rischio	Vulnerabilità
	SSH Service Accessible
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag Content-Security-Policy
	Target ip address system reverses traffic
	Worldspan gateway Denial of Service
	WorldSpan Res Gateway Denial of Service
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Referrer-Policy
	HTTP only port without SSL found
	SNMP service detected on udp
	All Protocols Tested
	Remote system answers to PING command
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	SSL Client Information

Livello rischio	Vulnerabilità
	SSL Certificate information
	System time via remote Web Server
	Direct HTTP 4538 & HTTPS 160331 Connections

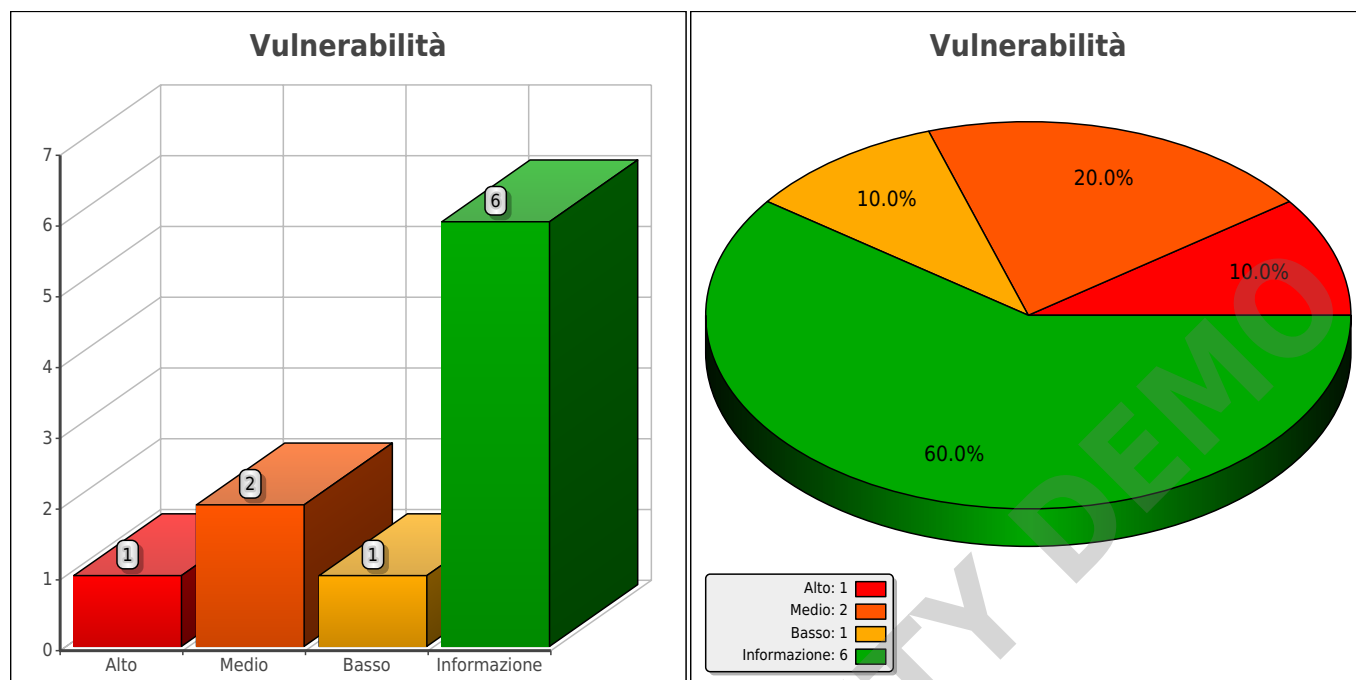
Sistema Target: 192.168.0.121



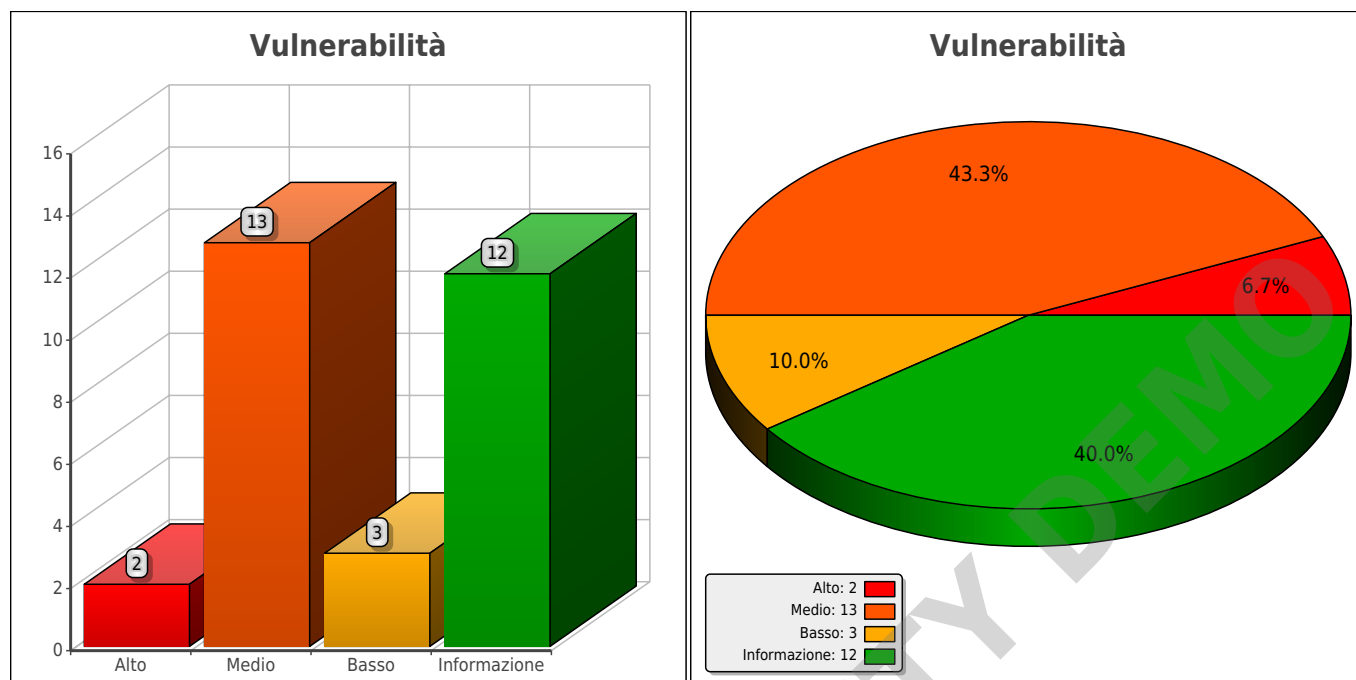
Livello rischio	Vulnerabilità
	SSH Service Accessible
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag Content-Security-Policy
	Worldspan gateway Denial of Service
	Target ip address system reverses traffic
	WorldSpan Res Gateway Denial of Service
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Referrer-Policy
	HTTP only port without SSL found
	SNMP service detected on udp
	All Protocols Tested
	MAC Address 08-f1-ea-93-c4-4e Hewlett Packard Enterprise
	SSL Client Information
	SSL Certificate information
	System time via remote Web Server
	Remote system answers to PING command
	Direct HTTP 4476 & HTTPS 160331 Connections

Sistema Target: 192.168.0.201

Livello rischio	Vulnerabilità
■ ■ ■ ■	Telnet Service Default Password
■ ■ ■ ■	Login interface identified on the target telnet service
■ ■ ■ ■	Telnet Service
■ ■ ■ ■	Possible Service/Game: TimeWolf Identified
■ ■ ■ ■	All Protocols Tested
■ ■ ■ ■	System Time Revealed via. ICMP TimeStamp Request
■ ■ ■ ■	MAC Address 00-17-61-11-a2-45 Private
■ ■ ■ ■	System Time Revealed ICMP TimeStamp
■ ■ ■ ■	Remote system answers to PING command
■ ■ ■ ■	Direct HTTP 51 & HTTPS 0 Connections

Sistema Target: 192.168.0.205

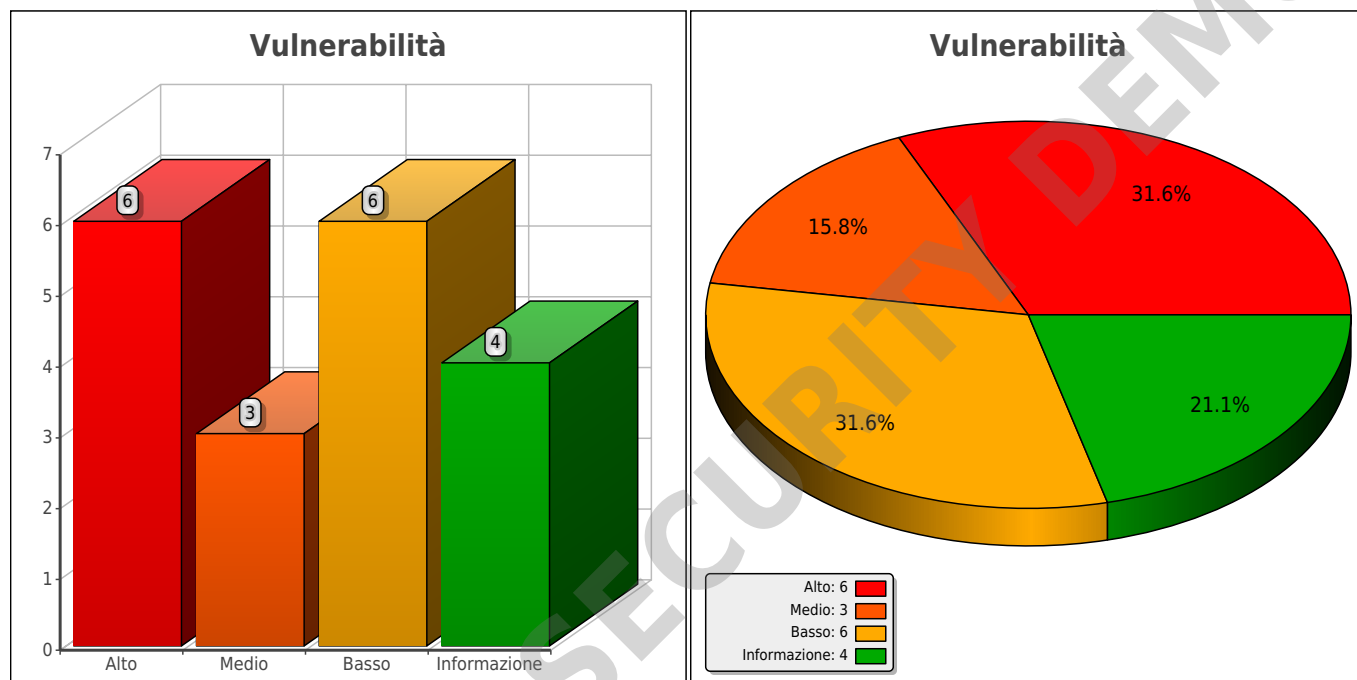
Livello rischio	Vulnerabilità
	Telnet Service Default Password
	Login interface identified on the target telnet service
	Telnet Service
	Possible Service/Game: TimeWolf Identified
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	MAC Address 00-17-61-11-e9-a0 Private
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	Direct HTTP 51 & HTTPS 0 Connections

Sistema Target: 192.168.0.222


Livello rischio	Vulnerabilità
■ ■ ■ ■	File post.php Information Disclosure
■ ■ ■ ■	Upload /file.asp identified
■ ■ ■ ■	Missing Web Security Header Tag Permissions-Policy
■ ■ ■ ■	Missing Web Security Header Tag X-Frame-Options
■ ■ ■ ■	Finger accessible via web server
■ ■ ■ ■	Missing Web Security Header Tag Content-Security-Policy
■ ■ ■ ■	Missing Web Security Header Tag Referrer-Policy
■ ■ ■ ■	Missing Web Security Header Tag Strict-Transport-Security
■ ■ ■ ■	Missing Web Security Header Tag X-Content-Type-Options
■ ■ ■ ■	Missing Web Security Header Tag X-Xss-Protection HTTP
■ ■ ■ ■	File /if.cgi Cross Site Scripting
■ ■ ■ ■	File LOGIN accessible on remote web server
■ ■ ■ ■	Login interface identified on the target telnet service
■ ■ ■ ■	Telnet Service
■ ■ ■ ■	File /if.cgi Cross Site Scripting
■ ■ ■ ■	Access to /search
■ ■ ■ ■	HTTP only port without SSL found
■ ■ ■ ■	MRTG Configuration Generator Path Disclosure
■ ■ ■ ■	All Protocols Tested
■ ■ ■ ■	Interesting directory HTTP /docs/NED?action=retrieve&location=. Identified
■ ■ ■ ■	Interesting directory HTTP /doc/%3C?=%ROOT_DIR?%3Eruntime/styles/aqua/ Identified
■ ■ ■ ■	Interesting directory HTTP /dir.php?dir=\\.\\.\\.\\.\\.etc/ Identified
■ ■ ■ ■	System Time Revealed via. ICMP TimeStamp Request
■ ■ ■ ■	Possible Web Server Application Firewall: The site http://192.168.0.222:80 is behind a ModSecurity;
■ ■ ■ ■	Identified Operating System Windows XP via Packet Check #3

Livello rischio	Vulnerabilità
	SEO Check Too many same keywords on a webpage
	Remote system answers to PING command
	System Time Revealed ICMP TimeStamp
	MAC Address e8-94-f6-67-4b-ec TP-LINK TECHNOLOGIES CO.,LTD.
	Direct HTTP 167776 & HTTPS 0 Connections

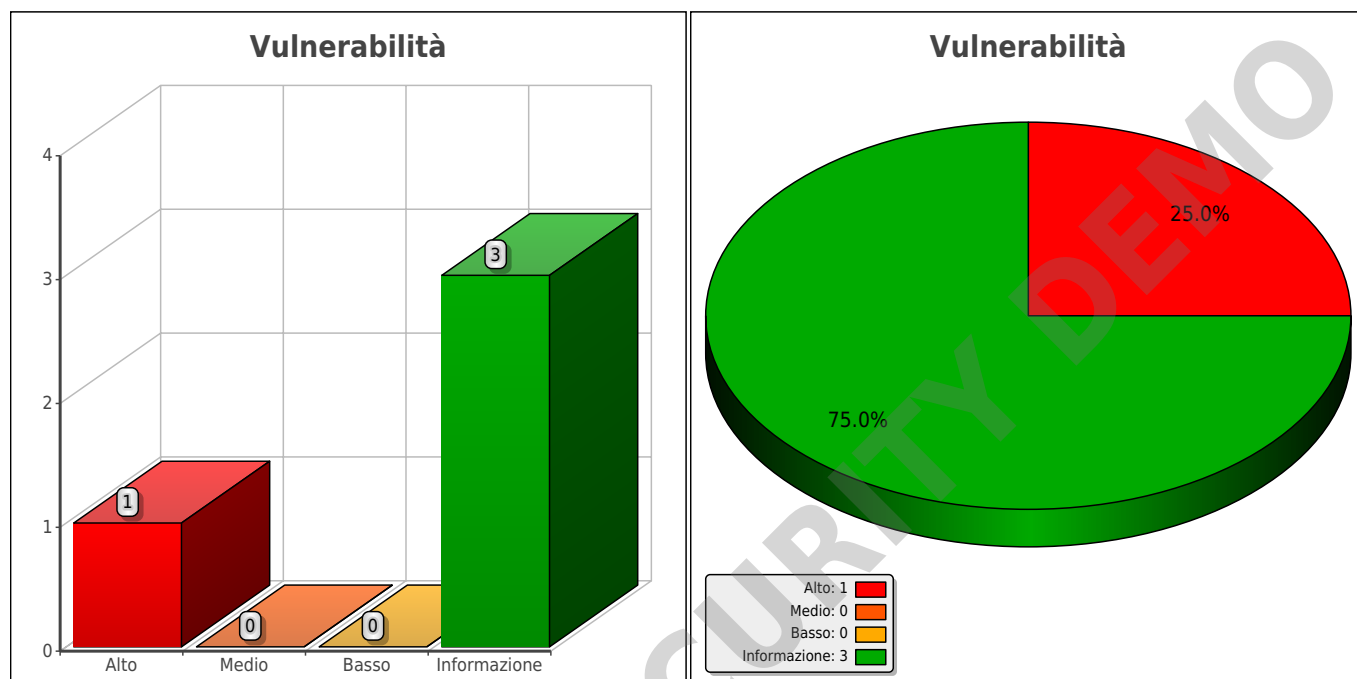
Sistema Target: 192.168.0.225



Livello rischio	Vulnerabilità
	Messagequeue Server Execution Overflow
	ctf Malware Backdoor Port Identified
	possible ctf port Malware Backdoor Port Identified
	Known Backdoor port 55555 / Telnet service identified
	Microsoft Message Queueing Service
	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
	Microsoft Windows 2103 tcp RPC
	Microsoft Windows 2107 tcp RPC
	Microsoft Windows 2105 tcp RPC
	It is possible to obtain remote NetBIOS name table
	MAC address obtained via NetBIOS
	Possible Service/Game: QNAP Identified
	NetBIOS service listening 137 UDP
	NetBIOS service listening 139 TCP
	Printer Spooler access port 515 TCP
	All Protocols Tested
	MAC Address f0-bc-c9-15-16-57 PFU LIMITED

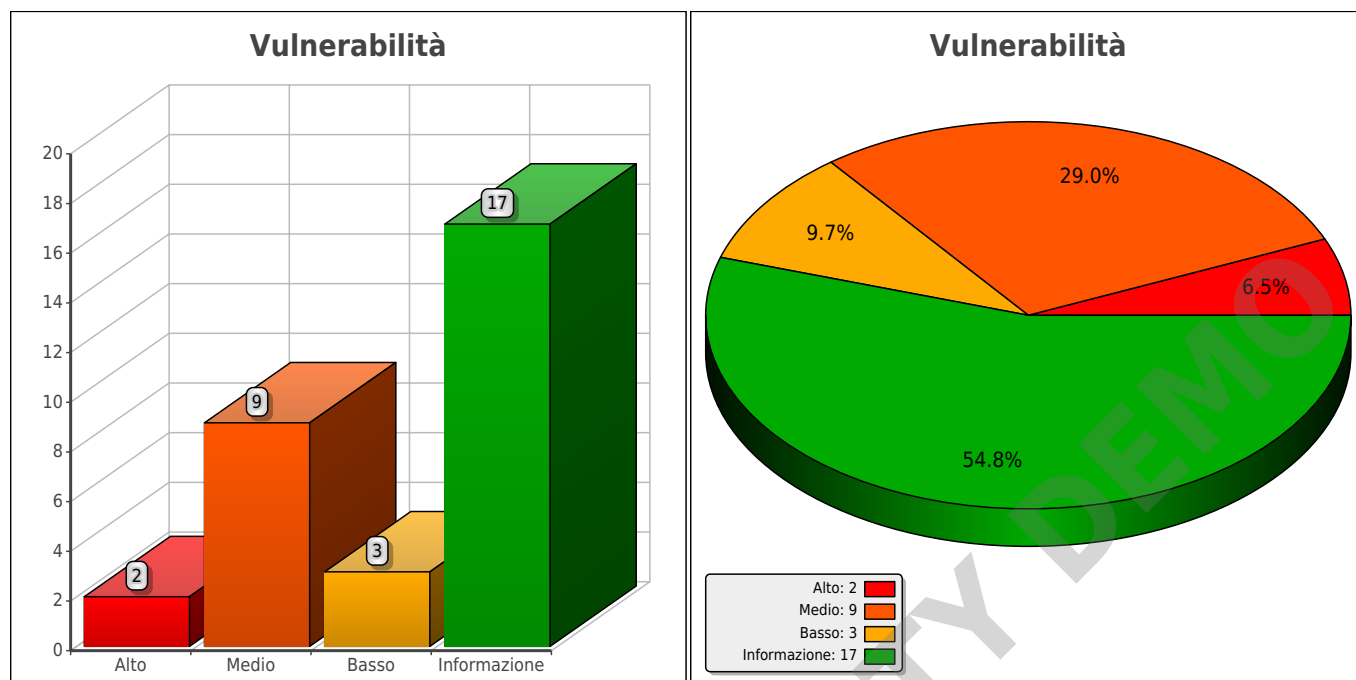
Livello rischio	Vulnerabilità
	Remote system answers to PING command
	Direct HTTP 63 & HTTPS 0 Connections

Sistema Target: 192.168.0.235



Livello rischio	Vulnerabilità
	Possible UPNP on TCP port 5000
	MAC Address d8-80-39-c7-4a-a0 Microchip Technology Inc.
	Remote system answers to PING command
	Direct HTTP 7 & HTTPS 0 Connections

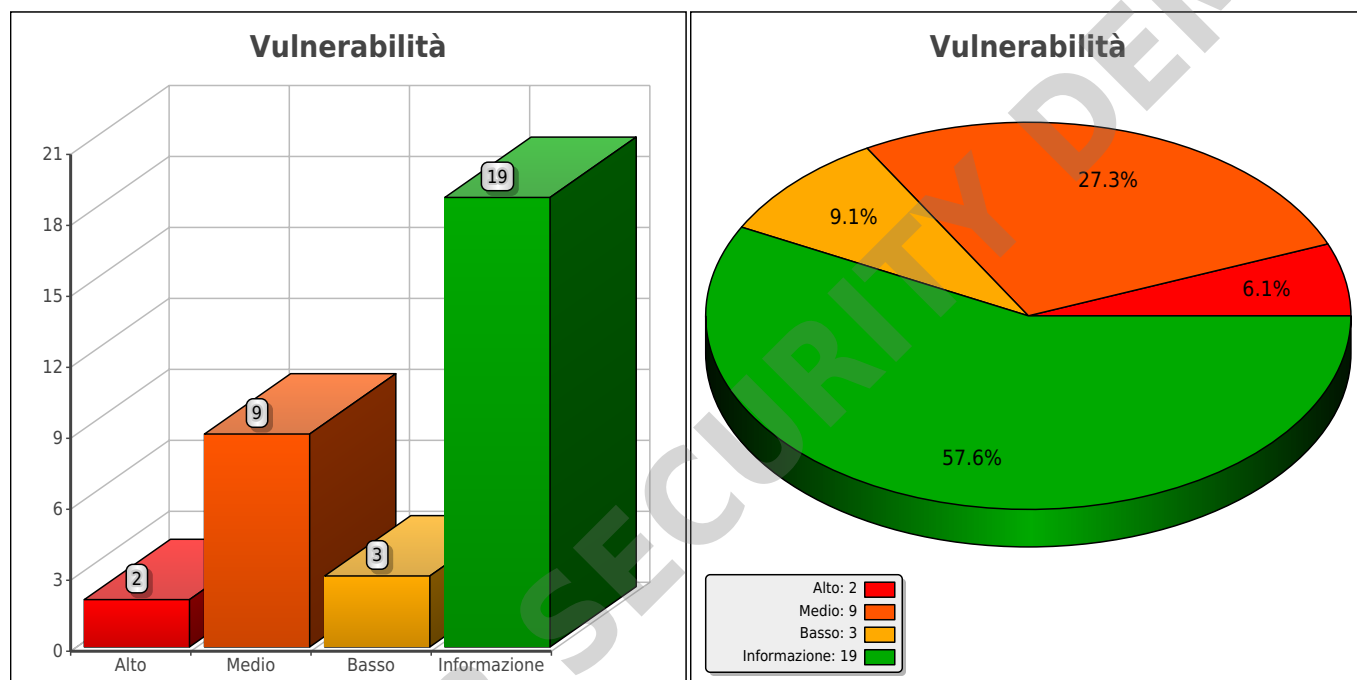
FRED FOR SECURITY DEMO

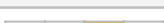
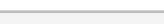
Sistema Target: 192.168.0.248

Livello rischio	Vulnerabilità
	SSH Service Accessible
	RPC Port identified
	RPC port-mapper Vulnerability
	NFS Service running
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag X-Content-Type-Options
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag X-Xss-Protection HTTP
	HTTP only port without SSL found
	Services via RPC
	OpenVAS Service Identification
	SSL Client Information
	Identified Operating System Check #2 Ubuntu Linux via Banner
	All Protocols Tested
	SSL Certificate information
	Remote system answers to PING command
	Interesting directory /vpns/./ HTTPS
	Interesting directory /vpn/./ HTTPS
	Interesting directory /unix/ALEX/Xserver2.10/././ HTTPS
	Interesting directory /unix/ALEX/Xserver2.00/././ HTTPS
	Interesting directory /unix/ALEX/Xserver2.0/././ HTTPS
	Interesting directory /unix/ALEX/Xserver/././ HTTPS

Livello rischio	Vulnerabilità
	Interesting directory /accounts/./ HTTPS
	Interesting directory // HTTPS
	Interesting directory ./ HTTPS
	Interesting directory ../ HTTPS
	System time via remote Web Server
	Direct HTTP 167868 & HTTPS 160331 Connections

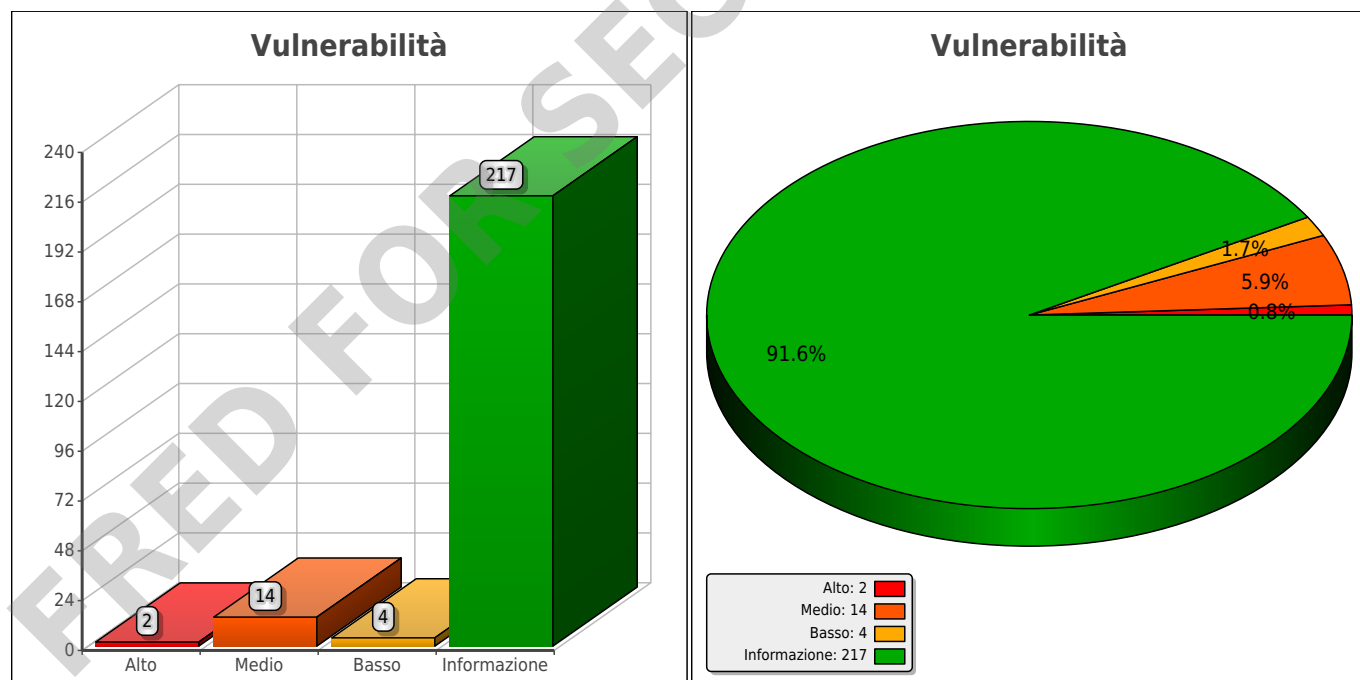
Sistema Target: 192.168.0.249



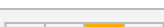
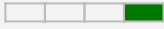
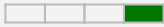
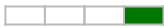
Livello rischio	Vulnerabilità
	SSH Service Accessible
	RPC Port identified
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag X-Xss-Protection HTTP
	Missing Web Security Header Tag X-Frame-Options
	RPC port-mapper Vulnerability
	NFS Service running
	Missing Web Security Header Tag X-Content-Type-Options
	Missing Web Security Header Tag Permissions-Policy
	Missing Web Security Header Tag Content-Security-Policy
	Missing Web Security Header Tag Referrer-Policy
	HTTP only port without SSL found
	OpenVAS Service Identification
	Services via RPC
	SSL Client Information
	Identified Operating System Check #2 Ubuntu Linux via Banner

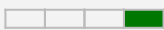
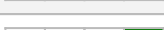
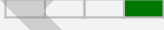
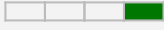
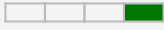
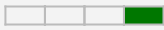
Livello rischio	Vulnerabilità
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	All Protocols Tested
	SSL Certificate information
	MAC Address 00-50-56-a2-0d-52 VMware, Inc.
	Interesting directory /vpns/./ HTTPS
	Interesting directory /vpn/./ HTTPS
	Interesting directory /unix/ALEX/Xserver2.10/./././ HTTPS
	Interesting directory /unix/ALEX/Xserver2.00/./././ HTTPS
	Interesting directory /unix/ALEX/Xserver2.0/./././ HTTPS
	Interesting directory /unix/ALEX/Xserver/./././ HTTPS
	Interesting directory /accounts/./ HTTPS
	Interesting directory // HTTPS
	Interesting directory ./ HTTPS
	Interesting directory ./ HTTPS
	System time via remote Web Server
	Remote system answers to PING command
	Direct HTTP 167868 & HTTPS 160331 Connections

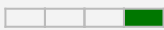
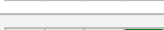
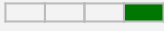
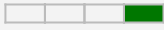
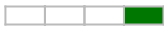
Sistema Target: 192.168.0.251

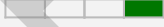
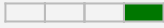
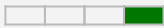


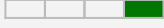
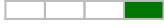
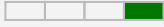
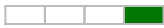
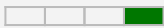
Livello rischio	Vulnerabilità
	Lethal Attack 1 HTTP Blind SQL Injection
	File /login.htm~ Information Disclosure
	File /Login.html Information Disclosure
	Missing Web Security Header Tag Content-Security-Policy
	File /banner.html Information Disclosure

Livello rischio	Vulnerabilità
	File /login.htm Information Disclosure
	File /login.html~ Information Disclosure
	File /login.htm~ Information Disclosure
	Missing Web Security Header Tag Permissions-Policy
	Apache HBase Hadoop database Port Identification
	Missing Web Security Header Tag Referrer-Policy
	Missing Web Security Header Tag Strict-Transport-Security
	Missing Web Security Header Tag X-Content-Type-Options
	Missing Web Security Header Tag X-Frame-Options
	Missing Web Security Header Tag X-Xss-Protection HTTP
	File /Login.htm Information Disclosure
	Possible Service/Game: Video Patrol Identified
	Possible Service/Game: X-Lite Identified
	S-HTTP web server Detected
	S-HTTP web server Detected #2
	Interesting directory HTTP /maintenance.html/ Identified
	Interesting directory HTTP /mapix/mapix/doc/en/changes.html/ Identified
	Interesting directory HTTP /mapix/doc/en/changes.html/ Identified
	Interesting directory HTTP /manual/index.html/ Identified
	Interesting directory HTTP /logon.html/ Identified
	Interesting directory HTTP /mail.html/ Identified
	Interesting directory HTTP /logs.html/ Identified
	Interesting directory HTTP /logs.htm/ Identified
	Interesting directory HTTP /logon/logon.html/ Identified
	Interesting directory HTTP /members.htm/ Identified
	Interesting directory HTTP /member/login.html/ Identified
	All Protocols Tested
	Interesting directory HTTP /members.html/ Identified
	Interesting directory HTTP /members/login.html/ Identified
	Interesting directory HTTP /modelsearch/admin.html/ Identified
	Interesting directory HTTP /modelsearch/index.html/ Identified
	Interesting directory HTTP /modelsearch/login.html/ Identified
	Interesting directory HTTP /moderator.html/ Identified
	Interesting directory HTTP /moderator/admin.html/ Identified
	Interesting directory HTTP /moderator/login.html/ Identified
	Interesting directory HTTP /login.html/ Identified
	Interesting directory HTTP /netadmin.htm/ Identified
	Interesting directory HTTP /netadmin.html/ Identified
	Interesting directory HTTP /logon.htm/ Identified
	Interesting directory HTTP /includes/webadmin.html/ Identified
	Interesting directory HTTP /login.htm/ Identified

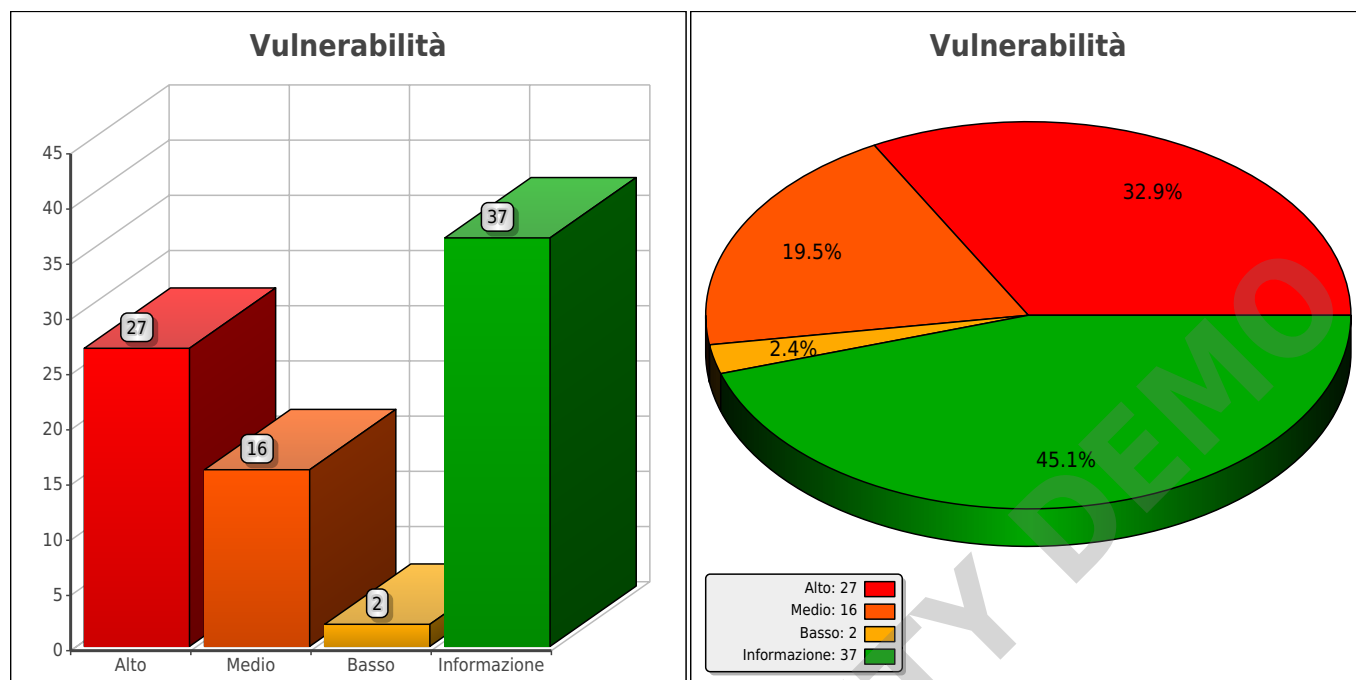
Livello rischio	Vulnerabilità
	Interesting directory HTTP /help.htm/ Identified
	Interesting directory HTTP /error.html/ Identified
	Interesting directory HTTP /error404.htm/ Identified
	Interesting directory HTTP /estore/annotated-index.html/ Identified
	Interesting directory HTTP /estore/index.html/ Identified
	Interesting directory HTTP /examples/jsp/cal/cal1.jsp\x00.html Identified
	Interesting directory HTTP /examples/servlets/index.html/ Identified
	Interesting directory HTTP /file_upload.htm/ Identified
	Interesting directory HTTP /file_upload.html/ Identified
	Interesting directory HTTP /fileadmin.html/ Identified
	Interesting directory HTTP /grabbed.html/ Identified
	Interesting directory HTTP /home.html/ Identified
	Interesting directory HTTP /log.html/ Identified
	Interesting directory HTTP /imprint.html/ Identified
	Interesting directory HTTP /ooladug/index.html/ Identified
	Interesting directory HTTP /index.htm/ Identified
	Interesting directory HTTP /index1.htm/ Identified
	Interesting directory HTTP /install.htm/ Identified
	Interesting directory HTTP /install.html/ Identified
	Interesting directory HTTP /installation.htm/ Identified
	Interesting directory HTTP /installation.html/ Identified
	Interesting directory HTTP /linktous.html/ Identified
	Interesting directory HTTP /log.htm/ Identified
	Interesting directory HTTP /nucleus/documentation/history.html/ Identified
	Interesting directory HTTP /post.html/ Identified
	Interesting directory HTTP /ooladug/index.html/cgi-bin/ Identified
	Interesting directory HTTP /v1/test/js/console.html/ Identified
	Interesting directory HTTP /sysadmin.html/ Identified
	Interesting directory HTTP /test.htm/ Identified
	Interesting directory HTTP /test.html/ Identified
	Interesting directory HTTP /test2.html/ Identified
	Interesting directory HTTP /tiny_mce/plugins/filemanager/examples.html/ Identified
	Interesting directory HTTP /tiny_mce/plugins/imagemanager/pages/im/index.html/ Identified
	Interesting directory HTTP /upload.htm/ Identified
	Interesting directory HTTP /upload.html/ Identified
	Interesting directory HTTP /ur-admin.html/ Identified
	Interesting directory HTTP /user.html/ Identified
	Interesting directory HTTP /webadmin.html/ Identified
	Interesting directory HTTP /subscribe.html/ Identified
	Interesting directory HTTP /webadmin/admin.html/ Identified
	Interesting directory HTTP /webadmin/index.html/ Identified

Livello rischio	Vulnerabilità
	Interesting directory HTTP /webadmin/login.html/ Identified
	Interesting directory HTTP /webdav/index.html/ Identified
	Interesting directory HTTP /webstats.html/ Identified
	Interesting directory HTTP /wp-content/plugins/akismet/webadmin.html/ Identified
	Interesting directory HTTP /wp-content/plugins/google-sitemap-generator/webadmin.html/ Identified
	Interesting directory HTTP /wwwstats.htm/ Identified
	File /login.html admin interface identified
	PHP Identified #4
	Interesting directory HTTP /swagger-ui.html/ Identified
	Interesting directory HTTP /stssys.htm/ Identified
	Interesting directory HTTP /order.htm/ Identified
	Interesting directory HTTP /private.html/ Identified
	Interesting directory HTTP /pages/admin/admin-login.html/ Identified
	Interesting directory HTTP /panel-administracion/admin.html/ Identified
	Interesting directory HTTP /panel-administracion/index.html/ Identified
	Interesting directory HTTP /panel-administracion/login.html/ Identified
	Interesting directory HTTP /password.html/ Identified
	Interesting directory HTTP /passwords.html/ Identified
	Interesting directory HTTP /popup.htm/ Identified
	Interesting directory HTTP /popup.html/ Identified
	Interesting directory HTTP /email.htm/ Identified
	Interesting directory HTTP /postinfo.html/ Identified
	Interesting directory HTTP /readme.html/ Identified
	Interesting directory HTTP /start.html/ Identified
	Interesting directory HTTP /recherche.html/ Identified
	Interesting directory HTTP /relogin.htm/ Identified
	Interesting directory HTTP /relogin.html/ Identified
	Interesting directory HTTP /reset.html/ Identified
	Interesting directory HTTP /searchresults.html/ Identified
	Interesting directory HTTP /settings.html/ Identified
	Interesting directory HTTP /signin.htm/ Identified
	Interesting directory HTTP /signin.html/ Identified
	Interesting directory HTTP /siteadmin/login.html/ Identified
	Interesting directory HTTP /ss_vms_admin_sm/admin/account.html/ Identified
	Interesting directory HTTP /entrar.html/ Identified
	Interesting directory HTTP /docs/html/admin/ch01s04.html/ Identified
	Interesting directory HTTP /docs/html/developer/ch03s15.html/ Identified
	Interesting directory HTTP /admin.htm.php/ Identified
	Interesting directory HTTP /_layouts/userinfo.htm/ Identified
	Interesting directory HTTP /_vti_inf.html/ Identified
	Interesting directory HTTP /_vti_info.html/ Identified

Livello rischio	Vulnerabilità
	Interesting directory HTTP /account.html/ Identified
	Interesting directory HTTP /account/login.htm/ Identified
	Interesting directory HTTP /account/login.html/ Identified
	Interesting directory HTTP /accounts.htm/ Identified
	Interesting directory HTTP /accounts.html/ Identified
	Interesting directory HTTP /adm.htm/ Identified
	Interesting directory HTTP /adm.html/ Identified
	Interesting directory HTTP /adm/index.html/ Identified
	Interesting directory HTTP /admin.htm/ Identified
	Interesting directory HTTP /_layouts/alllibs.htm/ Identified
	Interesting directory HTTP /admin.html.php/ Identified
	Interesting directory HTTP /admin.html/ Identified
	Interesting directory HTTP /admin.phpadmin.html/ Identified
	Interesting directory HTTP /admin/account.html/ Identified
	Interesting directory HTTP /admin/admin-login.html/ Identified
	Interesting directory HTTP /admin/admin.html/ Identified
	Interesting directory HTTP /admin/adminLogin.htm/ Identified
	Interesting directory HTTP /admin/adminLogin.html/ Identified
	Interesting directory HTTP /admin/admin_login.html/ Identified
	Interesting directory HTTP /admin/controlpanel.htm/ Identified
	Interesting directory HTTP /admin/controlpanel.html/ Identified
	Interesting directory HTTP /_layouts/settings.htm/ Identified
	Interesting directory HTTP /_admin.html/ Identified
	Interesting directory HTTP /admin/index.html/ Identified
	Interesting directory HTTP /Administrator.htm/ Identified
	Remote system answers to PING command
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Interesting directory HTTP /%00/interact.sh/ Identified
	Interesting directory HTTP /docs/cplugError.html/ Identified
	Interesting directory HTTP /%00/ Identified
	Interesting directory HTTP /ADMIN/login.html/ Identified
	Interesting directory HTTP /Adm.htm/ Identified
	Interesting directory HTTP /Adm.html/ Identified
	Interesting directory HTTP /Admin.htm/ Identified
	Interesting directory HTTP /Admin.html/ Identified
	Interesting directory HTTP /Administration.html/ Identified
	Interesting directory HTTP /Administrator.html/ Identified
	Interesting directory HTTP /WebSphereSamples/YourCo/main.html/ Identified
	Interesting directory HTTP /CFIDE/Administrator/startstop.html/ Identified
	Interesting directory HTTP /ErrorPage.htm/ Identified
	Interesting directory HTTP /Login.htm/ Identified

Livello rischio	Vulnerabilità
	Interesting directory HTTP /Login.html/ Identified
	Interesting directory HTTP /Members.htm/ Identified
	Interesting directory HTTP /Members.html/ Identified
	Interesting directory HTTP /Privacy.html/ Identified
	Interesting directory HTTP /README.htm/ Identified
	Interesting directory HTTP /README.html/ Identified
	Interesting directory HTTP /Secret/Gallery1.htm/ Identified
	Interesting directory HTTP /WebSphereSamples/SingleSamples/AccountAndTransfer/create.html/ Identified
	Interesting directory HTTP /WebSphereSamples/SingleSamples/Increment/increment.html/ Identified
	Interesting directory HTTP /admin/home.html/ Identified
	Interesting directory HTTP /admin/login.htm/ Identified
	Interesting directory HTTP /docs/html/developer/ch02.html/ Identified
	Interesting directory HTTP /conf.html/ Identified
	Interesting directory HTTP /bb-admin/admin.html/ Identified
	Interesting directory HTTP /bb-admin/index.html/ Identified
	Interesting directory HTTP /bb-admin/login.html/ Identified
	Interesting directory HTTP /cancel.html/ Identified
	Interesting directory HTTP /cgi-bin/index.html/ Identified
	Interesting directory HTTP /changelog.html/ Identified
	Interesting directory HTTP /checkapache.html/ Identified
	Interesting directory HTTP /city.html/ Identified
	Interesting directory HTTP /ckeditor/ckfinder/ckfinder.html/ Identified
	Interesting directory HTTP /ckfinder/ckfinder.html/ Identified
	Interesting directory HTTP /cms/design.htm/ Identified
	Interesting directory HTTP /config.html/ Identified
	Interesting directory HTTP /auth.html/ Identified
	Interesting directory HTTP /controlpanel.htm/ Identified
	Interesting directory HTTP /controlpanel.html/ Identified
	Interesting directory HTTP /cp.html/ Identified
	Interesting directory HTTP /dashboard.html/ Identified
	Interesting directory HTTP /demo/ejb/index.html/ Identified
	Interesting directory HTTP /desktop/index_framed.htm/ Identified
	Interesting directory HTTP /doc/en/changes.html/ Identified
	Interesting directory HTTP /docs/CHANGELOG.html/ Identified
	Interesting directory HTTP /docs/html/admin/ch01.html/ Identified
	MAC Address 00-60-b9-b8-0a-26 NEC Platforms, Ltd
	Interesting directory HTTP /docs/html/admin/ch03s07.html/ Identified
	Interesting directory HTTP /docs/html/admin/index.html/ Identified
	Interesting directory HTTP /auth/login.html/ Identified
	Interesting directory HTTP /auth.htm/ Identified

Livello rischio	Vulnerabilità
	Interesting directory HTTP /admin/login.html/ Identified
	Interesting directory HTTP /admincontrol.html/ Identified
	Interesting directory HTTP /admin1.htm/ Identified
	Interesting directory HTTP /admin1.html/ Identified
	Interesting directory HTTP /admin2.html/ Identified
	Interesting directory HTTP /adminLogin.html/ Identified
	Interesting directory HTTP /admin_area/admin.html/ Identified
	Interesting directory HTTP /admin_area/index.html/ Identified
	Interesting directory HTTP /admin_area/login.html/ Identified
	Interesting directory HTTP /admin_login.html/ Identified
	Interesting directory HTTP /adminarea/admin.html/ Identified
	Interesting directory HTTP /adminarea/index.html/ Identified
	Interesting directory HTTP /adminarea/login.html/ Identified
	Interesting directory HTTP /admincontrol/login.html/ Identified
	Interesting directory HTTP /aphtpasswd.html/ Identified
	Interesting directory HTTP /admincp/index.html/ Identified
	Interesting directory HTTP /administr8.html/ Identified
	Interesting directory HTTP /administration.html/ Identified
	Interesting directory HTTP /administrator.htm/ Identified
	Interesting directory HTTP /administrator.html/ Identified
	Interesting directory HTTP /administrator/account.html/ Identified
	Interesting directory HTTP /administrator/index.html/ Identified
	Interesting directory HTTP /administrator/login.html/ Identified
	Interesting directory HTTP /adminpanel.html/ Identified
	Interesting directory HTTP /admins.html/ Identified
	Interesting directory HTTP /analog.html/ Identified
	Interesting directory HTTP /apadminred.html/ Identified
	Direct HTTP 167886 & HTTPS 0 Connections

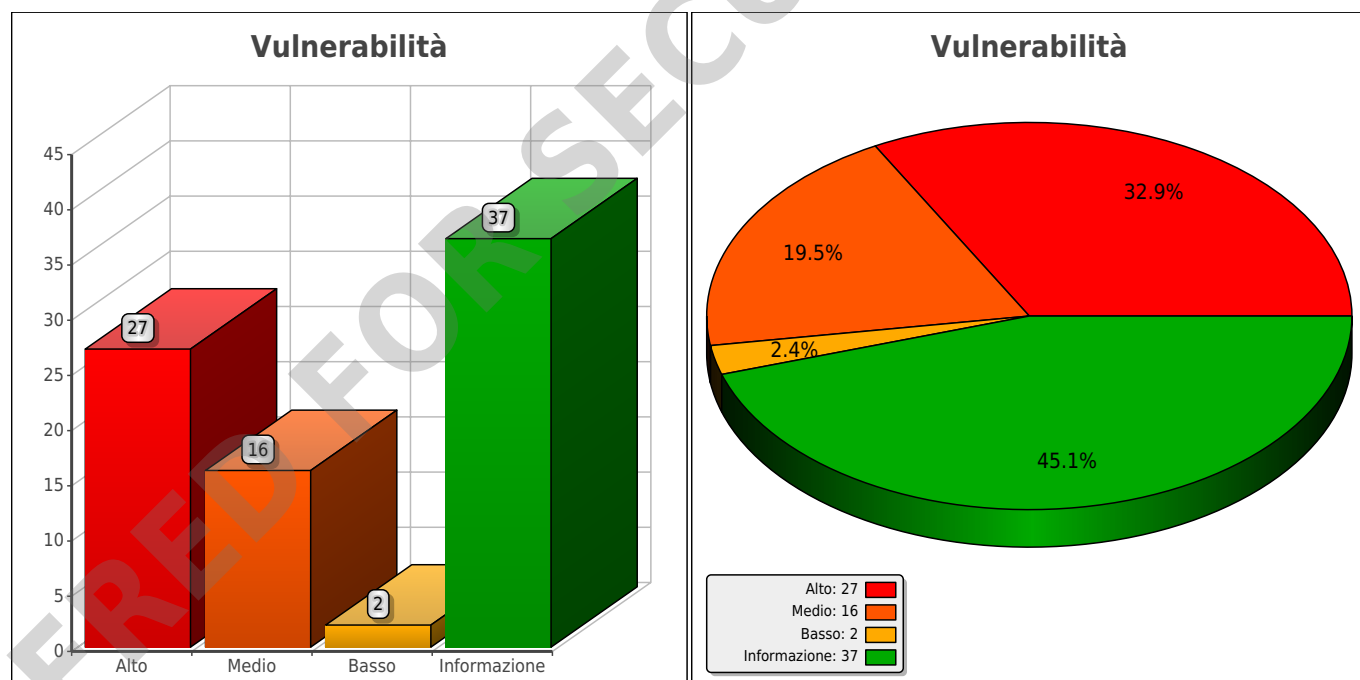
Sistema Target: 192.168.0.253

Livello rischio	Vulnerabilità
	File /login/login.php~ Information Disclosure
	File /login/oauth Information Disclosure
	File /login/userverify.cgi Information Disclosure
	File /login/myaccount.php Information Disclosure
	File /login/login~ Information Disclosure
	File /login/dologin Information Disclosure
	File /login/login.asp Information Disclosure
	File /login/home/login.php Information Disclosure
	File CTF pwnos v2 login.php Information Disclosure
	File login.php Remote Command Execution (RCE)
	File /login/login/default.php Information Disclosure
	File /login/loginindex.php Information Disclosure
	File /login/maindefault.php Information Disclosure
	File /login/mainmain.aspx Information Disclosure
	File /login/oauth~ Information Disclosure
	File /login/index.asp Information Disclosure
	File /login/search/password.log Information Disclosure
	File /login/.viewevent.asp Information Disclosure
	File /accounts.php Information Disclosure
	File /login/admin Information Disclosure
	File /login/admin~ Information Disclosure
	File /login/administrator Information Disclosure
	File /login/api/filezilla.xml Information Disclosure
	File /login/cpanel Information Disclosure
	File /login/cpanel~ Information Disclosure

Livello rischio	Vulnerabilità
	SSH Service Accessible
	File /login/.env Information Disclosure
	File /login Information Disclosure
	File /login/index Information Disclosure
	File /login/admin/admin.asp~ Information Disclosure
	File /login/cpanel.html Information Disclosure
	File /login/admin/admin.asp Information Disclosure
	File /login/index~ Information Disclosure
	File /logout Information Disclosure
	File thisissimpleanexistentfile Information Disclosure
	SSL PFS Forward Secrecy Check
	File /login/kefuxian.mvc~ Information Disclosure
	File /login/cpanel.html Information Disclosure
	File /login/super~ Information Disclosure
	File /login/super Information Disclosure
	File /login/login~ Information Disclosure
	File /login/login Information Disclosure
	File /login/kefuxian.mvc Information Disclosure
	HTTP only port without SSL found
	Web Server Path Disclosure
	SSL Certificate information
	SSL Client Information
	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 541
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	Interesting directory /login/api/ HTTPS
	MAC Address e0-23-ff-6e-03-df Fortinet, Inc.
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	System time via remote Web Server
	Interesting directory /error/ HTTPS
	Interesting directory /login/ HTTPS
	Interesting directory /login/activex/ HTTPS
	Interesting directory /login/admin/ HTTPS
	Interesting directory /login/admin/admin.asp/ HTTPS
	Interesting directory /login/admin/db/ HTTPS
	Interesting directory /login/admin/scripts/ HTTPS
	Interesting directory /login/admin/web/ HTTPS
	Interesting directory /login/administrator/ HTTPS
	Interesting directory /login/cpanel/ HTTPS

Livello rischio	Vulnerabilità
	Interesting directory /login/super/ HTTPS
	Interesting directory /login/default.asp/exchange/ HTTPS
	Interesting directory /login/facebook/ HTTPS
	Interesting directory /login/home/ HTTPS
	Interesting directory /login/index/ HTTPS
	Interesting directory /login/log/ HTTPS
	Interesting directory /login/log/suse/ HTTPS
	Interesting directory /login/login.php/ HTTPS
	Interesting directory /login/login/ HTTPS
	Interesting directory /login/oauth/ HTTPS
	Interesting directory /login/oauth/twitter/ HTTPS
	Interesting directory /login/oauth/v2/ HTTPS
	Interesting directory /login/oauth/v2/yahoo/ HTTPS
	Interesting directory /login/perl/ HTTPS
	Interesting directory /login/search/ HTTPS
	Direct HTTP 167845 & HTTPS 160331 Connections

Sistema Target: 192.168.0.254



Livello rischio	Vulnerabilità
	File /login/login.php~ Information Disclosure
	File /login/oauth Information Disclosure
	File /login/userverify.cgi Information Disclosure
	File /login/myaccount.php Information Disclosure
	File /login/login~ Information Disclosure
	File /login/dologin Information Disclosure

Livello rischio	Vulnerabilità
	File /login/login.asp Information Disclosure
	File /login/home/login.php Information Disclosure
	File CTF pwnos v2 login.php Information Disclosure
	File login.php Remote Command Execution (RCE)
	File /login/login/default.php Information Disclosure
	File /login/loginindex.php Information Disclosure
	File /login/maindefault.php Information Disclosure
	File /login/mainmain.aspx Information Disclosure
	File /login/oauth~ Information Disclosure
	File /login/index.asp Information Disclosure
	File /login/search/password.log Information Disclosure
	File /login/.viewevent.asp Information Disclosure
	File /accounts.php Information Disclosure
	File /login/admin Information Disclosure
	File /login/admin~ Information Disclosure
	File /login/administrator Information Disclosure
	File /login/api/filezilla.xml Information Disclosure
	File /login/cpanel Information Disclosure
	File /login/cpanel~ Information Disclosure
	SSH Service Accessible
	File /login/.env Information Disclosure
	File /login Information Disclosure
	File /login/index Information Disclosure
	File /login/admin/admin.asp~ Information Disclosure
	File /login/cpanel.html Information Disclosure
	File /login/admin/admin.asp Information Disclosure
	File /login/index~ Information Disclosure
	File /logout Information Disclosure
	File thisissimpleanexistentfile Information Disclosure
	SSL PFS Forward Secrecy Check
	File /login/kefuxian.mvc~ Information Disclosure
	File /login/cpanel.html Information Disclosure
	File /login/super~ Information Disclosure
	File /login/super Information Disclosure
	File /login/login~ Information Disclosure
	File /login/login Information Disclosure
	File /login/kefuxian.mvc Information Disclosure
	HTTP only port without SSL found
	Web Server Path Disclosure
	SSL Certificate information
	SSL Client Information

Livello rischio	Vulnerabilità
	Identified Operating System Linux 3.x via Packet Check #3
	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 541
	All Protocols Tested
	System Time Revealed via. ICMP TimeStamp Request
	Interesting directory /login/api/ HTTPS
	MAC Address e0-23-ff-6e-03-df Fortinet, Inc.
	System Time Revealed ICMP TimeStamp
	Remote system answers to PING command
	System time via remote Web Server
	Interesting directory /error/ HTTPS
	Interesting directory /login/ HTTPS
	Interesting directory /login/activex/ HTTPS
	Interesting directory /login/admin/ HTTPS
	Interesting directory /login/admin/admin.asp/ HTTPS
	Interesting directory /login/admin/db/ HTTPS
	Interesting directory /login/admin/scripts/ HTTPS
	Interesting directory /login/admin/web/ HTTPS
	Interesting directory /login/administrator/ HTTPS
	Interesting directory /login/cpanel/ HTTPS
	Interesting directory /login/super/ HTTPS
	Interesting directory /login/default.asp/exchange/ HTTPS
	Interesting directory /login/facebook/ HTTPS
	Interesting directory /login/home/ HTTPS
	Interesting directory /login/index/ HTTPS
	Interesting directory /login/log/ HTTPS
	Interesting directory /login/log/suse/ HTTPS
	Interesting directory /login/login.php/ HTTPS
	Interesting directory /login/login/ HTTPS
	Interesting directory /login/oauth/ HTTPS
	Interesting directory /login/oauth/twitter/ HTTPS
	Interesting directory /login/oauth/v2/ HTTPS
	Interesting directory /login/oauth/v2/yahoo/ HTTPS
	Interesting directory /login/perl/ HTTPS
	Interesting directory /login/search/ HTTPS
	Direct HTTP 167845 & HTTPS 160331 Connections

Vulnerabilità

Sistema Target: 192.168.0.1

Vulnerabilità	Mail Server sent to files attack
Livello rischio	Alto
Porta	25/tcp
SPID	1750
CVE	CVE-1999-0096
CVSS	CVE-1999-0096 - CVSS Score V2: 5
Impatto	The remote SMTP mail server did not complain when issued the command <code>;;MAIL FROM: root@this_host;;RCPT TO: testing;;</code> . This probably means that it is possible to send mail directly to program files, which is a serious threat, since this allows anyone to overwrite any file on the remote system.
Soluzione	Please upgrade your SMTP Mail server you are running to the latest version. *NOTE This may be a false positive on some systems that does not validate that your MAIL FROM command has a valid domain name request in it.
Output della vulnerabilità / Evidenze	
	AttackString: AttackOutput: 250 2.1.5 testing@CERT-SERVER

Vulnerabilità	Mailto Files attack
Livello rischio	Alto
Porta	25/tcp
SPID	1764
CVE	CVE-1999-0096
CVSS	CVE-1999-0096 - CVSS Score V2: 5
Impatto	It is possible to connect to the remote mail server software and issue a MAIL FROM: <code> /usr/ucb/tail /usr/bin/sh</code> and RCPT TO: root and by that execute commands on the target system with the same privileges as the web server software. Attackers can use this to compromise the system.
Soluzione	Please upgrade to the latest version of your mail server software. *NOTE This may be a false positive against some systems that does not validate that a valid domain has been supplied in the MAIL FROM: command.
Output della vulnerabilità / Evidenze	
	AttackString: AttackOutput: 250 2.1.5 root@CERT-SERVER

Vulnerabilità	Windows Terminal Services RDP
Livello rischio	Alto
Porta	3389/tcp
SPID	2390
CVE	CVE-2002-0444
CVE	CVE-2001-0860
CVSS	CVE-2002-0444 - CVSS Score V2: 7.5

CVSS	CVE-2001-0860 - CVSS Score V2: 7.5
Impatto	The Terminal Services has been found running. Terminal Services is used to remotely obtain a graphical login interface. If an attacker has gained a valid login and password the attacker can be able to use this service to gain further access on the remote system. The identified service is also known to a remote Denial of Service vulnerability.
Soluzione	Be sure to change the default port. Either disable the Terminal Services from Start->Control-Panel->Administrative Tools->Service and find it and set it to disable and or block incoming TCP traffic to the identified port. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Microsoft SQL Server
Livello rischio	 Alto
Porta	1434/udp
SPID	3033
CVE	CVE-2002-0649
CVSS	CVE-2002-0649 - CVSS Score V2: 7.5
Impatto	The Microsoft SQL server 2000 has been identified on the remote system. It is subject to several vulnerabilities where it is possible for an attacker to gain full access on the remote system.
Soluzione	It is recommended to block incoming traffic to the identified port at firewall level. If you need this service open to specific users it is recommended to only allow their IPs to be able to connect to it. And issue the latest Microsoft patches from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
Livello rischio	 Alto
Porta	445/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening. There has been known exploits like WannaCry on this port and it is recommended to firewall of the port and only allow trusted users to connect to it.

Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Mail Server Decode Vulnerability
Livello rischio	 Alto
Porta	25/tcp
SPID	1762
CVE	CVE-1999-0096
CVSS	CVE-1999-0096 - CVSS Score V2: 5
Impatto	It is possible on the remote mail server software (smtp) to send commands to local file /usr/bin/uudecode. Attackers can use this to compromise the system.
Soluzione	UNIX: This vulnerability is typically found in sendmail. Please upgrade to the latest stable sendmail version from http://www.sendmail.org and remove the /usr/bin/uudecode line from /etc/aliases. WINDOWS: Please upgrade to the latest version of your mail server software. *NOTE This may be a false positive against some systems that does not validate that a domain name has been specified in the MAIL FROM: request.
Output della vulnerabilità / Evidenze	
	AttackString: AttackOutput: 250 2.1.5 decode@CERT-SERVER

Vulnerabilità	File ?var?.cap Information Disclosure
Livello rischio	 Alto
Porta	80/tcp
SPID	61559
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.

Soluzione	Please upgrade to the latest version of the identified software you are running with the found file. Or if the file is sensitive make it unavailable.
Output della vulnerabilità / Evidenze	
	AttackOutput: HTTP/1.1 200 OK
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:33:29 GMT
	Connection: close
	Content-Length: 0

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	 Medio
Porta	80/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Content-Security-Policy
Livello rischio	 Medio
Porta	80/tcp
SPID	58667
Impatto	The Content Security Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Content-Security-Policy: block-all-mixed-content script-src 'self' www.youriste.com ")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	 Medio
Porta	80/tcp
SPID	58666
Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Lethal Attack 1 HTTP Crawler Cross Site Scripting Reflected XSRF
Livello rischio	Medio
Porta	80/tcp
SPID	62584
Impatto	The identified file found in the VULNOUTPUT section are subject to a remote Cross Site Scripting vulnerability. This can allow an attacker to steal cookie based authentication credentials from the target system.
Soluzione	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it. The string reflection is a symptom pf a possible vulnerability, but it's not fully sure that it's vulnerable. To avoid any issues, the best thing to do is not reflect any part of the URL into a form.
Output della vulnerabilità / Evidenze	
	Lethal Attack Crawler Possible Cross Site Scripting Reflected: (GET http://192.168.0.1/Account/Login/yop)

Vulnerabilità	Missing Web Security Header Tag Strict-Transport-Security
Livello rischio	Medio
Porta	80/tcp
SPID	58665
Impatto	The HTTP Web Security Header Strict Transport Security is a recommended feature to increase the security on your website and strengthens your implementation of TLS by forcing the User Agent to use HTTPS. It is often know as HSTS that forces the web site to make the web browsers know it should be accessed only by using HTTPS instead of the insecure HTTP.
Soluzione	Fix by adding to your site: header("Strict-Transport-Security: max-age=31536000 includeSubDomains")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Content-Type-Options
Livello rischio	Medio
Porta	80/tcp
SPID	58664
Impatto	X-Content-Type-Options Security Header is used to prevent a browser from trying to MIME sniff the sensitive content type & forces the browser to use the declared content-type. The HTTP Security header is used by the server to indicate the MIME types advertised in the Content-Type headers to not be changed. This can prevent MIME type sniffing. The header was first introduced by Microsoft in Internet Explorer IE 8 to allows webmasters block content sniffing that could transform non-executable MIME types into executable MIME type. Other web browsers have introduced it as well. It is recommended by penetration testing process to expect this header to be set. The only valid value you can set for for this header is nosniff.
Soluzione	Fix by adding to your site: header("X-Content-Type-Options: nosniff")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Xss-Protection HTTP
Livello rischio	Medio
Porta	80/tcp
SPID	58662

Impatto	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP.
Soluzione	To add the header please see: https://scotthelme.co.uk/hardening-your-http-response-headers/#x-xss-protection X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1 mode=block" FIX: header("X-Xss-Protection: 1 mode=block") .
Output della vulnerabilità / Evidenze	

Vulnerabilità	NetBIOS service listening 137 UDP
Livello rischio	☐ ☐ ☒ Basso
Porta	137/udp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Possible Service/Game: pc game port Identified
Livello rischio	☐ ☐ ☒ Basso
Porta	50007/tcp
SPID	61487
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Web Login Box #check2
Livello rischio	☐ ☒ ☐ Basso
Porta	80/tcp
SPID	58191
Impatto	The identified web server found is known to be a login Web interface. This could be subject to attack from attackers by using default passwords such as: admin Pass: admin or even blank username and admin as password. This can allow attackers and automated worm scripts to easily compromise routers.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found serv. NOTE: If you are already running the latest version please ignore this check.
Output della vulnerabilità / Evidenze	
	AttackString: GET / HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Location: /Account/Login
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:43:44 GMT
	Connection: close

Vulnerabilità	HTTP only port without SSL found
Livello rischio	☐ ☒ ☐ Basso
Porta	80/tcp, 5985/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.1:80/tcp matches http-apache-2

Vulnerabilità	Lethal Attack 1 HTTP Internal Server Error
Livello rischio	☐ ☒ ☐ Basso
Porta	80/tcp
SPID	62583
Impatto	The identified files found in the VULNOUTPUT section reveals sensitive error information. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it.
Output della vulnerabilità / Evidenze	

Lethal Attack Crawler Internal Server Error: (POST http://192.168.0.1/Account/Login?__RequestVerificationToken=admin' OR '1'='1' %00&password=1&username=1)

Vulnerabilità	MAC address obtained via NetBIOS
Livello rischio	Basso
SPID	1771
Impatto	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	MAC Address: 00-50-56-8c-c5-05

Vulnerabilità	It is possible to obtain remote NetBIOS name table
Livello rischio	Basso
SPID	1770
Impatto	Attackers can use this information to base other attacks on.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	Name Service Type ----- CERT-SERVER Workstation Service WORKGROUP Domain Name CERT-SERVER File Server Service

Vulnerabilità	NetBIOS service listening 139 TCP
Livello rischio	Basso
Porta	139/tcp
SPID	1990

Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	All Protocols Tested
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.1:25/tcp matches smtp
	Protocol on 192.168.0.1:80/tcp matches http
	Protocol on 192.168.0.1:80/tcp matches http-apache-2
	Protocol on 192.168.0.1:80/tcp matches http-iis
	Protocol on 192.168.0.1:135/tcp matches netbios-session
	Protocol on 192.168.0.1:139/tcp matches netbios-session
	Protocol on 192.168.0.1:3389/tcp matches ssl
	Protocol on 192.168.0.1:5985/tcp matches http
	Protocol on 192.168.0.1:5985/tcp matches http-apache-2
	Protocol on 192.168.0.1:50007/tcp matches ms-sql
	Protocol on 192.168.0.1:50007/tcp matches sybase

Vulnerabilità	SMTP Ehlo Command
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	25/tcp
SPID	1765
CVE	CVE-1999-0531
CVSS	

Impatto	It is possible on the target SMTP mail server software to retrieve information by using the EHLO command instead of the normal HELO. Attackers can use this information to perform more specific attacks.
Soluzione	Disable the EHLO command on your mail service software if allowed. WINDOWS: Microsoft(R) Exchange 1:Open up regedit.exe 2:Goto following registry key HKEY_LOCAL_MACHINE\SystemCurrentControlSet\Services\MSExchange\MCParameters 3:In regedit Choose Edit and then choose New DWORD Value. 4:Add the type AdvertiseSMTPExtensions under Value data type 0 for more information please see http://www.microsoft.com/Exchange/ UNIX: Please upgrade to the latest version of your mail service software running. The latest sendmail can be obtained from http://www.sendmail.org and there click on mail server.
Output della vulnerabilità / Evidenze	
	AttackString: EHLO hotmail.com
	AttackOutput: 250-CERT-SERVER Hello [192.168.0.51]
	250-TURN
	250-SIZE 2097152
	250-ETRN
	250-PIPELINING
	250-DSN
	250-ENHANCEDSTATUSCODES
	250-8bitmime
	250-BINARYMIME
	250-CHUNKING
	250-VRFY
	250 OK

Vulnerabilità	Mailserver Help Command information
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	25/tcp
SPID	1769
Impatto	It is possible to issue a SMTP Mailserver Mail command. This command often reveals the version number of the mail server software. Attackers can use this information to base other attacks on.
Soluzione	Disable your smtp Help Command. UNIX: On sendmail edit the sendmail.cf and uncomment the line O HelpFile=/etc/helpfile. And or change the line O PrivacyOptions=goaway Further more edit the /etc/mail/helpfile and delete everything in the file so that it only says one line #vers 2 . Before modifying files always make a backup first. WINDOWS: If running exchange or similar this is not an easy option to do and therefor it is recommended to remove at firewall level. If your mail server command is not revealing anything please ignore this check.
Output della vulnerabilità / Evidenze	
	AttackString: HELP
	AttackOutput: 214-This server supports the following commands:
	214 HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN
	BDAT VRFY

Vulnerabilità	Interesting directory HTTP /home/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /home/ HTTP/1.0 AttackOutput: HTTP/1.1 302 Found Location: /Account/Login Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 14 Sep 2023 13:30:17 GMT Connection: close

Vulnerabilità	Interesting directory HTTP /workstation/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /workstation/ HTTP/1.0 AttackOutput: HTTP/1.1 302 Found Location: http:///Account/Login?ReturnUrl=%2Fworkstation%2F Server: Microsoft-IIS/10.0 X-Powered-By: ASP.NET Date: Thu, 14 Sep 2023 13:30:44 GMT Connection: close

Vulnerabilità	Interesting directory HTTP /Home/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /Home/ HTTP/1.0

AttackOutput: HTTP/1.1 302 Found
Location: /Account/Login
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 14 Sep 2023 13:29:49 GMT
Connection: close

Vulnerabilità	Interesting directory HTTP /fileadmin/gymfyn/Almenp?d/Kurser/Midtvejs_Matematik_Material/Matematikkkens_metoder/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackOutput: HTTP/1.1 200 OK
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:30:15 GMT
	Connection: close
	Content-Length: 0

Vulnerabilità	Identified Operating System Check #2 Microsoft Windows via Banner
Livello rischio	Informazione
Porta	80/tcp, 5985/tcp, 25/tcp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the https Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Location: /Account/Login
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:27:48 GMT
	Connection: close

Vulnerabilità	MAC Address 00-50-56-8c-c5-05 VMware, Inc.
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 00-50-56-8c-c5-05 VMware, Inc.

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	20:05:32

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.1: icmp_seq=0 ttl=128 time=0.4 ms

Vulnerabilità	System time via remote Web Server
Livello rischio	Informazione

Porta	80/tcp, 5985/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Thu, 14 Sep 2023 13:18:02 GMT

Vulnerabilità	SEO Check HTTP code 302 usage
Livello rischio	Informazione
SPID	46135
Impatto	Using HTTP 302 codes can give you very bad ranking in the search engines
Soluzione	You must always use 301 redirects instead of 302 redirects.
Output della vulnerabilità / Evidenze	
	http://192.168.0.1/Account/Login

Vulnerabilità	IIS Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	3761
Impatto	It is possible via the banner from the web server software to detect some presence of IIS. IIS has a known history of several security vulnerabilities. Attackers can use this information to do IIS specified attacks. If you do not want to remove the version banner and you are already running the latest IIS then please ignore this check.
Soluzione	To remove the banner from the IIS can be done by setting an ISAPI filter designed to set the banner using the SetHeader function call. And or install the URLScan http://www.microsoft.com/technet/security/tools/urlscan.msp
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check.
	k. AttackString: HEAD / HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found

Location: /Account/Login
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 14 Sep 2023 13:27:48 GMT
Connection: close

Vulnerabilità	Web Server Application Firewall: Reason: The server header is different when an attack is detected.;
Livello rischio	Informazione
Porta	80/tcp
SPID	13481
Impatto	The remote host reveals what type of Web Application Firewall it is running. This information is critical for an attacker because then the attacker can much better target the attacks.
Soluzione	It is recommended to set your software to not reveal its program name.
Output della vulnerabilità / Evidenze	
	AttackOutput: Reason: The server header is different when an attack is detected.

Vulnerabilità	Interesting directory HTTP /certificates/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /certificates/ HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Location: http:///Account/Login?ReturnUrl=%2Fcertificates%2F
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:30:06 GMT
	Connection: close

Vulnerabilità	Interesting directory HTTP /Account/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	

AttackString: GET /Account/ HTTP/1.0
AttackOutput: HTTP/1.1 302 Found
Location: http:///Account/Login?ReturnUrl=%2FAccount%2F
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 14 Sep 2023 13:29:48 GMT
Connection: close

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 12:42:33

Vulnerabilità	Interesting directory HTTP /Home/Index/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /Home/Index/ HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Location: /Account/Login
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:29:50 GMT
	Connection: close

Vulnerabilità	Interesting directory HTTP /Tempor?ra%20Internetfiler/Low/Content.IE5/ Identified
---------------	---

Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackOutput: HTTP/1.1 200 OK
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:29:51 GMT
	Connection: close
	Content-Length: 0

Vulnerabilità	Interesting directory HTTP /account/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /account/ HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Location: http:///Account/Login?ReturnUrl=%2Faccount%2F
	Server: Microsoft-IIS/10.0
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 13:29:53 GMT
	Connection: close

Vulnerabilità	Interesting directory HTTP /account/login/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /account/login/ HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	Cache-Control: no-cache, no-store

Sistema Target: 192.168.0.2

Vulnerabilità	Microsoft SQL Server
Livello rischio	Alto
Porta	1434/udp
SPID	3033
CVE	CVE-2002-0649
CVSS	CVE-2002-0649 - CVSS Score V2: 7.5
Impatto	The Microsoft SQL server 2000 has been identified on the remote system. It is subject to several vulnerabilities where it is possible for an attacker to gain full access on the remote system.
Soluzione	It is recommended to block incoming traffic to the identified port at firewall level. If you need this service open to specific users it is recommended to only allow their IPs to be able to connect to it. And issue the latest Microsoft patches from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Messagequeue Server Execution Overflow
Livello rischio	Alto
Porta	2105/tcp
SPID	11475
Impatto	The identified port found open on the target system with the found service is known to be subject to a remote buffer execution Overflow that an attacker can exploit to execute arbitrary code on the target system.
Soluzione	It is recommended to block incoming traffic to the identified port and or only allow trusted users to connect to it and further more make sure you have the latest version of the service.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	MSSql service listening
Livello rischio	Alto
Porta	1433/tcp
SPID	2124
CVE	CVE-2002-0056
CVE	CVE-2001-0542

CVE	CVE-2001-0344
CVE	CVE-2000-1088
CVE	CVE-2000-1087
CVE	CVE-2000-1086
CVE	CVE-2000-1085
CVE	CVE-2000-1085
CVE	CVE-2000-1084
CVE	CVE-2000-1083
CVE	CVE-2000-1082
CVE	CVE-2000-1081
CVSS	CVE-2002-0056 - CVSS Score V2: 7.5
CVSS	CVE-2001-0542 - CVSS Score V2: 7.5
CVSS	CVE-2001-0344 - CVSS Score V2: 7.2
CVSS	CVE-2000-1088 - CVSS Score V2: 4.6
CVSS	CVE-2000-1087 - CVSS Score V2: 4.6
CVSS	CVE-2000-1086 - CVSS Score V2: 4.6
CVSS	CVE-2000-1085 - CVSS Score V2: 4.6
CVSS	CVE-2000-1085 - CVSS Score V2: 4.6
CVSS	CVE-2000-1084 - CVSS Score V2: 4.6
CVSS	CVE-2000-1083 - CVSS Score V2: 2.1
CVSS	CVE-2000-1082 - CVSS Score V2: 4.6
CVSS	CVE-2000-1081 - CVSS Score V2: 4.6
Impatto	The Microsoft(R) SQL service is known to contain several vulnerabilities that can result in: System compromise, theft of data, Denial of Service attacks.
Soluzione	WINDOWS: Either block incoming traffic to the identified port at firewall and or make sure you have the latest Microsoft(R) SQL. From http://support.microsoft.com/default.aspx?scid=fh EN-US sp and there select the SQL you are running and apply latest service pack and simple patches. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Windows Terminal Services RDP
Livello rischio	Alto
Porta	3389/tcp
SPID	2390
CVE	CVE-2002-0444
CVE	CVE-2001-0860
CVSS	CVE-2002-0444 - CVSS Score V2: 7.5
CVSS	CVE-2001-0860 - CVSS Score V2: 7.5

Impatto	The Terminal Services has been found running. Terminal Services is used to remotely obtain a graphical login interface. If an attacker has gained a valid login and password the attacker can be able to use this service to gain further access on the remote system. The identified service is also known to a remote Denial of Service vulnerability.
Soluzione	Be sure to change the default port. Either disable the Terminal Services from Start->Control-Panel->Administrative Tools->Service and find it and set it to disable and or block incoming TCP traffic to the identified port. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Delf acz ctf port Malware Backdoor Port Identified
Livello rischio	Alto
Porta	6161/tcp
SPID	75260
Impatto	Possible Backdoor has been found (This check is only looking for the presense of the port and may be a false positive if you are running something else on the identified port) has listening on the target system. This likely means that your system has been compromised and the Backdoor installed.
Soluzione	Please restore your system from backups and or call your local computer crime unit for further investigation. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Microsoft Message Queuing Service
Livello rischio	Alto
Porta	2103/tcp
SPID	5541
Impatto	IMPACT: The identified port found open on the target web server is known to be the Microsoft Message Queuing Service. It is subject to remote overflow vulnerability. An attacker can exploit this to crash the service and execute arbitrary code on the target system.
Soluzione	It is recommended to set firewall permissions so that the identified port is only open to trusted IP addresses. For the latest version please see http://www.microsoft.com/windows2000/technologies/communications/msmq/default.msp
Output della vulnerabilità / Evidenze	

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	RPC Port identified
Livello rischio	Alto
Porta	593/tcp
SPID	4962
Impatto	The identified port found on the target system is known to be the RPC service. It has a history of several high risk vulnerabilities. This can possible allow an attacker to compromise your system if you are not updated to the latest version.
Soluzione	It is recommended to update to the latest RPC version on your system and or set firewall filtering so that only trusted ip addresses are allowed to connect to it.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
Livello rischio	Alto
Porta	445/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening. There has been known exploits like WannaCry on this port and it is recommended to firewall of the port and only allow trusted users to connect to it.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Game: Orbz Buffer Overflow
Livello rischio	Medio
Porta	28000/tcp
SPID	5159
Impatto	The identified Orbz found running is subject to a remote Denial of Service vulnerability. This can allow an attacker to crash the service.
Soluzione	Please issue the latest patches for your game from http://www.21-6.com/ and or filter incoming traffic so that only trusted ip addresses are allowed to connect to the target port.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	SCADA Web Client Alaram Server / Schneider / PowerSCADA System Identified 5504
Livello rischio	Medio
Porta	5504/tcp
SPID	58494
Impatto	The target service found running can be subject to a remote buffer overflow vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as the identified daemon.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found software. And it is recommended to set firewall permissions so only trusted users can connect to the found IP address. Note if you are running another service on this port you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Missing Web Security Header Tag X-Xss-Protection HTTP
Livello rischio	Medio
Porta	80/tcp
SPID	58662
Impatto	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP.

Soluzione	To add the header please see: https://scotthelme.co.uk/hardening-your-http-response-headers/#x-xss-protection X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1 mode=block" FIX: header("X-Xss-Protection: 1 mode=block")
Output della vulnerabilità / Evidenze	

Vulnerabilità	File thisissimpleanonexistantfile Information Disclosure
Livello rischio	Medio
Porta	80/tcp
SPID	12810
Impatto	Your website responds with 200 OK or 302 Found request to a non-existent file. It should have responded with a 404 error code. Because of this your site does not validate. This can cause it to be much lower ranked on search engines such as Google. And in the end you will lose valuable traffic to your site.
Soluzione	Please fix your error codes so it gives correct 404 errors to non-existent files.
Output della vulnerabilità / Evidenze	
	<pre> AttackString: GET /thisissimpleanonexistantfile HTTP/1.0 AttackOutput: HTTP/1.1 302 Found Content-Type: text/html charset=utf-8 Location: HTTPS://192.168.0.2/THISISSIMPLEANONEXISTANTFILE Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Thu, 14 Sep 2023 14:28:12 GMT Connection: close Content-Length: 165 <html><head><title>Object moved</title></head>&l t;body> <h2>Object moved to here.</h2> </body></html> </pre>

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Content-Security-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58667
Impatto	The Content Security Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Content-Security-Policy: block-all-mixed-content script-src 'self' www.youriste.com ")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58666
Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Strict-Transport-Security
Livello rischio	Medio
Porta	80/tcp
SPID	58665
Impatto	The HTTP Web Security Header Strict Transport Security is a recommended feature to increase the security on your website and strengthens your implementation of TLS by forcing the User Agent to use HTTPS. It is often know as HSTS that forces the web site to make the web browsers know it should be accessed only by using HTTPS instead of the insecure HTTP.
Soluzione	Fix by adding to your site: header("Strict-Transport-Security: max-age=31536000 includeSubDomains")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Frame-Options
Livello rischio	Medio
Porta	80/tcp
SPID	58663
Impatto	X-Frame-Options is used to communicate to the web browser if you want to allow your site to be framed or not. Preventing the web browser from farming your site to defend against attacks such as clickjacking. The X-Frame-Options header can be used to if a web browser is allowed to render a page in a <frame>, <object>, or <iframe>. It is recommended to enable this check in penetration testing process.
Soluzione	Fix by adding to your site: header("X-Frame-Options: SAMEORIGIN")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Content-Type-Options
Livello rischio	Medio
Porta	80/tcp
SPID	58664
Impatto	X-Content-Type-Options Security Header is used to prevent a browser from trying to MIME sniff the sensitive content type & forces the browser to use the declared content-type. The HTTP Security header is used by the server to indicate the MIME types advertised in the Content-Type headers to not be changed. This can prevent MIME type sniffing. The header was first introduced by Microsoft in Internet Explorer IE 8 to allow webmasters block content sniffing that could transform non-executable MIME types into executable MIME type. Other web browsers have introduced it as well. It is recommended by penetration testing process to expect this header to be set. The only valid value you can set for this header is nosniff.
Soluzione	Fix by adding to your site: header("X-Content-Type-Options: nosniff")
Output della vulnerabilità / Evidenze	

Vulnerabilità	MySQL Service running
Livello rischio	Medio
Porta	3306/tcp
SPID	1868
CVE	CVE-2012-1689
CVSS	CVE-2012-1689 - CVSS Score V2: 4
Impatto	The MySQL service has been found running. It is known to have a history of vulnerabilities and in the future several more can occur.
Soluzione	It is highly recommended to block incoming access to the identified port at firewall level. If you need this service open to specific users it is recommended to only allow their IPs to be able to connect to it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	Microsoft Windows RPC
Livello rischio	Medio
Porta	593/tcp
SPID	1925
Impatto	The windows RPC has been identified on the found port. This is a windows service and it is not recommended to be open to the internet. It can be subject of vulnerabilities in the future.
Soluzione	It is recommended to set firewall permissions so that the identified is not accessible from the internet.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	X11 Server / Microsoft Windows RPC over HTTP
Livello rischio	Medio
Porta	6004/tcp
SPID	2106
Impatto	The identified port running is known to contain the X11 windows-system service running. When an attacker has access to this port the attacker can "sniff" keystrokes from the session running or do more specific attacks.
Soluzione	It is highly recommended to block incoming access to the identified port by applying filters at firewall level. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	X11 Server
Livello rischio	Medio
Porta	6005/tcp, 6006/tcp, 6007/tcp, 6009/tcp
SPID	2106
Impatto	The identified port running is known to contain the X11 windows-system service running. When an attacker has access to this port the attacker can "sniff" keystrokes from the session running or do more specific attacks.
Soluzione	It is highly recommended to block incoming access to the identified port by applying filters at firewall level. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Point-To-Point (PPTP) Protocol tcp port 1723 identified
Livello rischio	Medio
Porta	1723/tcp
SPID	53
Impatto	Several services running the identified port is subject to many vulnerabilities specially Denial of Service attacks.

Soluzione	It is recommended at firewall level to filter incoming traffic to the identified port and if it must be open make sure only trusted IPs can connect to it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Lethal Attack 1 HTTP Crawler Cross Site Scripting XSS
Livello rischio	Medio
Porta	80/tcp
SPID	5244
Impatto	The identified file found in the VULNOUTPUT section are subject to a remote Cross Site Scripting vulnerability. This can allow an attacker to steal cookie based authentication credentials from the target system.
Soluzione	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it.
Output della vulnerabilità / Evidenze	
	Lethal Attack Crawler Possible Cross Site Scripting: (GET http://192.168.0.2/`/bin/echo+w00t`)

Vulnerabilità	Lethal Attack 1 HTTP Crawler Cross Site Scripting Reflected XSRF
Livello rischio	Medio
Porta	80/tcp
SPID	62584
Impatto	The identified file found in the VULNOUTPUT section are subject to a remote Cross Site Scripting vulnerability. This can allow an attacker to steal cookie based authentication credentials from the target system.
Soluzione	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it. The string reflection is a symptom pf a possible vulnerability, but it's not fully sure that it's vulnerable. To avoid any issues, the best thing to do is not reflect any part of the URL into a form.
Output della vulnerabilità / Evidenze	
	Lethal Attack Crawler Possible Cross Site Scripting Reflected: (GET http://192.168.0.2/6,6)

Vulnerabilità	Microsoft Windows 2107 tcp RPC
Livello rischio	Medio
Porta	2107/tcp
SPID	1925
Impatto	The windows RPC has been identified on the found port. This is a windows service and it is not recommended to be open to the internet. It can be subject of vulnerabilities in the future.
Soluzione	It is recommended to set firewall permissions so that the identified is not accessible from the internet.

Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Microsoft Windows 2105 tcp RPC
Livello rischio	☐ ☒ ☐ ☐ Medio
Porta	2105/tcp
SPID	1925
Impatto	The windows RPC has been identified on the found port. This is a windows service and it is not recommended to be open to the internet. It can be subject of vulnerabilities in the future.
Soluzione	It is recommended to set firewall permissions so that the identified is not accessible from the internet.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	X11 Sniff AttackServer
Livello rischio	☐ ☒ ☐ ☐ Medio
Porta	6010/tcp
SPID	11481
Impatto	The identified port running is known to contain the X11 windows-system service running. When an attacker has access to this port the attacker can "sniff" keystrokes from the session running or do more specific attacks.
Soluzione	It is highly recommended to block incoming access to the identified port by applying filters at firewall level. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Microsoft Windows 2103 tcp RPC
Livello rischio	☐ ☒ ☐ ☐ Medio
Porta	2103/tcp
SPID	1925
Impatto	The windows RPC has been identified on the found port. This is a windows service and it is not recommended to be open to the internet. It can be subject of vulnerabilities in the future.
Soluzione	It is recommended to set firewall permissions so that the identified is not accessible from the internet.
Output della vulnerabilità / Evidenze	

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	DNS Recursion Allowed
Livello rischio	Medio
SPID	56963
Impatto	The target DNS service is subject to a remote DNS Recursion vulnerability. Attackers can exploit this in DDoS Attacks. Recursion is used to process a DNS request where the DNS server performs the request for the client. Recursion should only be allowed for trusted clients.
Soluzione	Set permissions so only trusted clients can do recursion requests or disable recursion. On Unix* You can edit /etc/bind/named.conf. allow-transfer {"none"} allow-recursion {"none"} recursion no On Windows please see: http://technet.microsoft.com/en-us/library/cc771738.aspx
Output della vulnerabilità / Evidenze	
	yahoo.com mail is handled by 1 mta5.am0.yahoodns.net.

Vulnerabilità	Lightweight Directory Access Protocol (LDAP)
Livello rischio	Basso
Porta	389/tcp, 3268/tcp, 3269/tcp
SPID	8
Impatto	The identified Lightweight Directory Access Protocol can be used by an attacker to enumerate valid users on the target system if it is set with guest permissions.
Soluzione	Please block incoming TCP traffic to port 389 and or only allow trusted hosts to connect. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 139 TCP
Livello rischio	Basso
Porta	139/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.

Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 137 UDP
Livello rischio	☐ ☒ ☐ Basso
Porta	137/udp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Possible Service/Game: Tales of Pirates Identified
Livello rischio	☐ ☒ ☐ Basso

Output della vulnerabilità / Evidenze

```

AttackString: HTTP GET /cfdocs/expeval/ExprCalc.cfm?RequestTimeout=2000
&OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprcalc.cfm HTTP/1
.0 AttackOutput: HTTP/1.1 302 Found
Content-Type: text/html
charset=utf-8
Location: HTTPS://192.168.0.2/CFDOCS/EXPEVAL/EXPRCALC.CFM?REQUEST
TIMEOUT=2000&OPENFILEPATH=D:\INETPUB\WWWROOT\CFDOCS\EXPEVAL/E
XPRCALC.CFM
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Thu, 14 Sep 2023 14:17:17 GMT
Connection: close
Content-Length: 248
<html><head><title>Object moved</title></head>&l
t;body>
<h2>Object moved to <a href="HTTPS://192.168.0.2/CFDOC
S/EXPEVAL/EXPRCALC.CFM?REQUESTTIMEOUT=2000&
OPENFILEPATH=D:\INETPUB\WWWROOT\CFDOCS\EXPEVAL/EXPRCALC.CFM"&g
t;here</a>.</h2>
</body></html>

```

Vulnerabilità HTTP only port without SSL found

Livello rischio	Basso
Porta	80/tcp, 5985/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.

Output della vulnerabilità / Evidenze

AttackOutput: Protocol on 192.168.0.2:80/tcp matches http-iis

Vulnerabilità Possible Service/Game: Star Wars Identified

Livello rischio	Basso
Porta	7070/tcp
SPID	61064
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.

Output della vulnerabilità / Evidenze

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità NTPd Service found PORT 123 TCP

Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	123/udp
SPID	25
CVE	CVE-2001-0414
CVSS	CVE-2001-0414 - CVSS Score V2: 10
Impatto	The Ntpd service is normally listening on TCP or UDP port 123. This service is used for time/date synchronozation. Severale remotely buffer overflows is known to exist in this service.
Soluzione	If you do not use this service block incoming TCP/tcp traffic to port 123 and or upgrade to the latest version of your Ntpd service. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Identified Operating System Check #2 Microsoft Windows via Banner
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	53/udp, 80/tcp, 5985/tcp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operaitng system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Microsoft DNS 6.1.7601 (1DB15F75)

Vulnerabilità	All Protocols Tested
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.2:21/tcp matches smtp
	Protocol on 192.168.0.2:21/tcp matches ftp
	Protocol on 192.168.0.2:80/tcp matches http
	Protocol on 192.168.0.2:80/tcp matches http-apache-2
	Protocol on 192.168.0.2:80/tcp matches http-iis
	Protocol on 192.168.0.2:88/tcp matches mysql
	Protocol on 192.168.0.2:135/tcp matches netbios-session
	Protocol on 192.168.0.2:139/tcp matches netbios-session
	Protocol on 192.168.0.2:389/tcp matches ldap
	Protocol on 192.168.0.2:445/tcp matches ms-ds

Protocol on 192.168.0.2:593/tcp matches http-ncacn
 Protocol on 192.168.0.2:593/tcp matches ms-rpc-proxy-endpoint
 Protocol on 192.168.0.2:1433/tcp matches ms-sql
 Protocol on 192.168.0.2:1433/tcp matches sybase
 Protocol on 192.168.0.2:2103/tcp matches netbios-session
 Protocol on 192.168.0.2:2105/tcp matches netbios-session
 Protocol on 192.168.0.2:2107/tcp matches netbios-session
 Protocol on 192.168.0.2:3268/tcp matches ldap
 Protocol on 192.168.0.2:3306/tcp matches mysql
 Protocol on 192.168.0.2:3306/tcp matches webseal
 Protocol on 192.168.0.2:3389/tcp matches ms-remote-desktop-protocol
 Protocol on 192.168.0.2:5504/tcp matches netbios-session
 Protocol on 192.168.0.2:5985/tcp matches http
 Protocol on 192.168.0.2:5985/tcp matches http-apache-2
 Protocol on 192.168.0.2:6004/tcp matches http-ncacn
 Protocol on 192.168.0.2:6004/tcp matches ms-rpc-proxy-endpoint
 Protocol on 192.168.0.2:6005/tcp matches netbios-session
 Protocol on 192.168.0.2:6006/tcp matches netbios-session
 Protocol on 192.168.0.2:6007/tcp matches netbios-session
 Protocol on 192.168.0.2:6009/tcp matches netbios-session
 Protocol on 192.168.0.2:6010/tcp matches http-ncacn
 Protocol on 192.168.0.2:6010/tcp matches ms-rpc-proxy-endpoint
 Protocol on 192.168.0.2:6011/tcp matches netbios-session
 Protocol on 192.168.0.2:6067/tcp matches netbios-session
 Protocol on 192.168.0.2:6161/tcp matches netbios-session

Vulnerabilità	Web Server Application Firewall: Reason: The server header is different when an attack is detected.;
Livello rischio	Informazione
Porta	80/tcp
SPID	13481
Impatto	The remote host reveals what type of Web Application Firewall it is running. This information is critical for an attacker because then the attacker can much better target the attacks.
Soluzione	It is recommended to set your software to not reveal its program name.
Output della vulnerabilità / Evidenze	
	AttackOutput: Reason: The server header is different when an attack is detected.

Vulnerabilità	IIS Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	3761
Impatto	It is possible via the banner from the web server software to detect some presence of IIS. IIS has a known history of several security vulnerabilities. Attackers can use this information to do IIS specified attacks. If you do not want to remove the version banner and you are already running the latest IIS then please ignore this check.

Soluzione	To remove the banner from the IIS can be done by setting an ISAPI filter designed to set the banner using the SetHeader function call. And or install the URLScan http://www.microsoft.com/technet/security/tools/urlscan.msp
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check
	k. AttackString: HEAD / HTTP/1.0
	AttackOutput: HTTP/1.1 302 Found
	Content-Length: 137
	Content-Type: text/html
	charset=utf-8
	Location: HTTPS://192.168.0.2/
	Server: Microsoft-IIS/7.5
	X-Powered-By: ASP.NET
	Date: Thu, 14 Sep 2023 14:13:09 GMT
	Connection: close

Vulnerabilità	Identified Operating System Windows 7 or 8 via Packet Check #3
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	443/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and won't be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Windows 7 or 8

Vulnerabilità	SSL Client Information
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	443/tcp
SPID	58286
Impatto	The target web server do not support encryption Downgrade attack prevention. This might enable attackers to carry out other attacks.
Soluzione	It is recommended to disable SSLv3. Enable HTTP compression only for static content. Upgrade to the latest version of your web application.
Output della vulnerabilità / Evidenze	
	Android 4.2.2 TLSv1.0 ECDHE-RSA-AES256-SHA 521 bit EC DH (P-521)
	Android 4.2.2 TLSv1.0 ECDHE-RSA-AES256-SHA 521 bit EC DH (P-521)
	Android 4.4.2 TLSv1.2 ECDHE-RSA-AES128-SHA256 521 bit ECDH (P-521)
	Android 5.0.0 TLSv1.2 ECDHE-RSA-AES256-SHA 521 bit EC DH (P-521)

Android 6.0 TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit EC DH (P-384)

Android 7.0 TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit EC DH (P-384)

Android 8.1 (native) TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

Android 9.0 (native) TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

Chrome 65 Win 7 TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

Chrome 74 (Win 10) TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

Firefox 62 Win 7 TLSv1.2 ECDHE-RSA-AES256-SHA 521 bit ECDH (P-521)

Firefox 66 (Win 8.1/10) TLSv1.2 ECDHE-RSA-AES256-SHA 521 bit ECDH (P-521)

IE 6 XP No connection

IE 7 Vista TLSv1.0 ECDHE-RSA-AES256-SHA 521 bit ECDH (P-521)

IE 8 Win 7 TLSv1.0 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

IE 8 XP No connection

IE 11 Win 7 TLSv1.2 ECDHE-RSA-AES256-SHA384 384 bit ECDH (P-384)

IE 11 Win 8.1 TLSv1.2 ECDHE-RSA-AES256-SHA384 384 bit ECDH (P-384)

IE 11 Win Phone 8.1 TLSv1.2 ECDHE-RSA-AES128-SHA256 384 bit ECDH (P-384)

IE 11 Win 10 TLSv1.2 ECDHE-RSA-AES256-SHA384 384 bit ECDH (P-384)

Edge 15 Win 10 TLSv1.2 ECDHE-RSA-AES256-SHA384 384 bit ECDH (P-384)

Edge 17 (Win 10) TLSv1.2 ECDHE-RSA-AES256-SHA384 384 bit ECDH (P-384)

Opera 60 (Win 10) TLSv1.2 ECDHE-RSA-AES256-SHA 384 bit ECDH (P-384)

Safari 9 iOS 9 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Safari 9 OS X 10.11 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Safari 10 OS X 10.12 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Apple ATS 9 iOS 9 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Tor 17.0.9 Win 7 TLSv1.0 ECDHE-RSA-AES256-SHA 521 bit ECDH (P-521)

Java 6u45 TLSv1.0 AES128-SHA No FS

Java 7u25 TLSv1.0 ECDHE-RSA-AES128-SHA 521 bit ECDH (P-521)

Java 8u161 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Java 9.0.4 TLSv1.2 ECDHE-RSA-AES256-SHA384 521 bit ECDH (P-521)

Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Thu, 14 Sep 2023 13:58:59 GMT

Vulnerabilità	Remote system answers to PING command
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.2: icmp_seq=0 ttl=128 time=0.5 ms

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	01:03:06

Vulnerabilità	MAC Address e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 17:40:06

Vulnerabilità	Direct HTTP 334616 & HTTPS 1 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

Sistema Target: 192.168.0.3

Vulnerabilità	SCADA System RSH RUGGEDCOM RS910 Overflow
Livello rischio	Alto
Porta	514/tcp
SPID	58371
Impatto	The target service found running is subject to a remote buffer overflow vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as the identified daemon.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found software. And it is recommended to set firewall permissions so only trusted users can connect to the found IP address. Note if you are running another service on this port you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Backdoor WinRemoteShell / IBM Tivoli ODBC Command Execution
Livello rischio	Alto
Porta	2020/tcp
SPID	47177
Impatto	The identified service found on the remote server is subject to a command execution vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as of the identified service is running with. The commands are executed with the privileges of the user account that started the Manager service on the remote server. Backburner is designed to be used by administrators on a closed network, the applications that use Backburner require partial administrative permissions therefore the service runs with administrative privileges. A malicious attacker could leverage this functionality to gain remote administrative control over the host running the Backburner software
Soluzione	Please upgrade to the latest version of the identified software you are running with the found service.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	SSH Service Accessible
Livello rischio	Alto
Porta	22/tcp
SPID	2733
Impatto	The SSH service allows anyone to connect to it. This is a security risk because an attacker can issue a brute force attack and the service has a history of many dangerous vulnerabilities.
Soluzione	It is recommended to only allow trusted users to connect to it.
Output della vulnerabilità / Evidenze	

AttackOutput: SSH-2.0-OpenSSH_7.4

Vulnerabilità	zoom remote exploit Port Identified
Livello rischio	Alto
Porta	5480/tcp
SPID	72193
Impatto	Possible Backdoor has been found (This check is only looking for the presense of the port and may be a false positive if you are running something else on the identified port) has listening on the target system. This likely means that your system has been compromised and the Backdoor installed.
Soluzione	Please restore your system from backups and or call your local computer crime unit for further investigation. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58666
Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Frame-Options
---------------	---

Livello rischio	Medio
Porta	80/tcp
SPID	58663
Impatto	X-Frame-Options is used to communicate to the web browser if you want to allow your site to be framed or not. Preventing the web browser from framing your site to defend against attacks such as clickjacking. The X-Frame-Options header can be used to if a web browser is allowed to render a page in a <frame>, <object>, or <iframe>. It is recommended to enable this check in penetration testing process.
Soluzione	Fix by adding to your site: header("X-Frame-Options: SAMEORIGIN")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Xss-Protection HTTP
Livello rischio	Medio
Porta	80/tcp
SPID	58662
Impatto	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP.
Soluzione	To add the header please see: https://scotthelme.co.uk/hardening-your-http-response-headers/#x-xss-protection X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1 mode=block" FIX: header("X-Xss-Protection: 1 mode=block")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Jetty Web Server File Geronimo cal2.jsp Cross Site Scripting
Livello rischio	Medio
Porta	9084/tcp
SPID	13456
CVE	CVE-2006-0254
CVSS	CVE-2006-0254 - CVSS Score V2: 4.3
Impatto	The identified file found on the remote web server is subject to a remote Cross Site Scripting vulnerability. An attacker can exploit this vulnerability to steal cookie based authentication credentials from legitimate users of the system.
Soluzione	Please upgrade to the latest version of the identified software you are running with the identified software.
Output della vulnerabilità / Evidenze	
Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check. k. AttackString: HEAD / HTTP/1.0 AttackOutput: HTTP/1.1 404 Not Found Date: Thu, 14 Sep 2023 15:07:14 GMT Cache-Control: must-revalidate,no-cache,no-store	

Content-Type: text/html
charset=iso-8859-1
Content-Length: 317
Server: Jetty(9.4.20.v20190813)

Vulnerabilità Rsh service on TCP port 514	
Livello rischio	Medio
Porta	514/tcp
SPID	17
CVE	CVE-1999-0651
CVSS	CVE-1999-0651 - CVSS Score V2: 7.5
Impatto	The identified TCP port 514 has been found open on the target. The Rshd service runs on this port. Rshd does not provide any good means of identification it can be used by attackers to scan a third party host and or bypassing your firewall.
Soluzione	It is highly recommended to disable this service. UNIX: On a common unix system comment out the "rshd shell" line in /etc/inetd.conf and or block incoming TCP traffic to port 514. WINDOWS: Please enter Control-Panel->Administrative Tools->Service->And there you can disable it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità Syslog service found on UDP 514	
Livello rischio	Medio
Porta	514/tcp
SPID	2724
Impatto	The target port found is known house the Syslog logging service. It is known to be subject to remote attacks where an attacker can flood the service. By this they can make it waste space on the hard drive and in the length over-flood the system which can result in a crash.
Soluzione	It is recommended to block incoming traffic to the identified port at firewall level. If you need this service open to specific users it is recommended to only allow their IPs to be able to connect to it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Lightweight Directory Access Protocol (LDAP)
Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	389/tcp
SPID	8
Impatto	The identified Lightweight Directory Access Protocol can be used by an attacker to enumerate valid users on the target system if it is set with guest permissions.
Soluzione	Please block incoming TCP traffic to port 389 and or only allow trusted hosts to connect. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	HTTP only port without SSL found
Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	80/tcp, 9084/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.3:80/tcp matches http

Vulnerabilità	LDAP Service
Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	636/tcp
SPID	9
Impatto	it is possible to access TCP port 636. This port is known to run the LDAP service. In the future a security vulnerability can raise in this software.
Soluzione	Please block incoming TCP traffic to port 636 and or only allow trusted hosts to connect. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Web Server Path Disclosure
Livello rischio	☐ ☐ ☒ Basso
Porta	80/tcp
SPID	7782
Impatto	It is possible on the remote web server by requesting GET /cfdocs/expeval/ExprCalc.cfm?RequestTimeout=2000&OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprcalc.cfm HTTP/1.0 URL to make it reveal the physical path as of where the software is installed on the target system. An attacker can exploit this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the software with the identified file.
Output della vulnerabilità / Evidenze	
AttackString: HTTP GET /cfdocs/expeval/ExprCalc.cfm?RequestTimeout=2000 &OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprcalc.cfm HTTP/1 .0 AttackOutput: HTTP/1.1 301 Moved Permanently Date: Thu, 14 Sep 2023 14:57:31 GMT Location: https://virtualcenter.img.local/cfdocs/expeval/ExprCalc.cfm?Req uestTimeout=2000&OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprc alc.cfm Connection: close Content-Type: text/html Content-Length: 56 <HTML><BODY><H1>301 Moved Permanently</H1></B ODY></HTML>	

Vulnerabilità	Possible Service/Game: kerberos firewall off can leak operating system Identified
Livello rischio	☐ ☐ ☒ Basso
Porta	88/tcp
SPID	61516
Impatto	Time ms14-068 exploitThe identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If y ou run another service on the found port please mark this check as a false posit ive in the menu.	

Vulnerabilità	Possible Service/Game: OpenEye Server Identified
Livello rischio	☐ ☐ ☒ Basso
Porta	2014/tcp, 2015/tcp
SPID	61166
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If y ou run another service on the found port please mark this check as a false posit ive in the menu.	

Vulnerabilità	Possible Service/Game: X10 AirSight XX39A Identified
Livello rischio	Basso
Porta	2012/tcp
SPID	60977
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.3:22/tcp matches ssh
	Protocol on 192.168.0.3:22/tcp matches ssh-openssh
	Protocol on 192.168.0.3:80/tcp matches http
	Protocol on 192.168.0.3:9084/tcp matches http
	Protocol on 192.168.0.3:9443/tcp matches http
	Protocol on 192.168.0.3:9443/tcp matches ssl

Vulnerabilità	Interesting directory HTTP /vci/downloads/ Identified
Livello rischio	Informazione
Porta	9084/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /vci/downloads/ HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	Date: Thu, 14 Sep 2023 15:10:08 GMT
	Content-Type: text/html
	charset=utf-8
	Content-Length: 1074

```

Server: Jetty(9.4.20.v20190813)
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<link href="jetty-dir.css" rel="stylesheet" />
<title>Directory: /vci/downloads/</title>
</head>
<body>
<h1 class="title">Directory: /vci/downloads/</h1>
<table class="listing">
<thead>
<tr><th class="name"><a href="?C=N&
0=D">Name 
&#8679
</a></th><th class="lastmodified"><a href=?C=M&0=A">Last Modified</a></th><th class=?q
uot;size"><a href="?C=S&0=A">Size</a><
/th></tr>
</thead>
<tbody>
<tr><td class="name"><a href="/vci/downloads
/health.xml">health.xml 
</a></td><td class="lastmodified">Jul 5, 2022 5:
10:29 AM 
</td><td class="size">430 bytes 
</td></tr>
<tr><td class="name"><a href="/vci/downloads
/vumclient.zip">vumclient.zip 
</a></td><td class="lastmodified">Nov 19, 2019
12:01:57 AM 
</td><td class="size">4,664,608 bytes 
</td></tr>
<tr><td class="name"><a href="/vci/downloads
/vum-htmlclient.zip">vum-htmlclient.zip 
</a></td><td class="lastmodified">Nov 19, 2019
12:01:57 AM 
</td><td class="size">1,966,339 bytes 
</td></tr>
</tbody>
</table>
</body></html>

```

Vulnerabilità	Possible Web Server Application Firewall: The site http://192.168.0.3:9084 is behind a Secu relIS;
Livello rischio	Informazione
Porta	9084/tcp
SPID	13481
Impatto	The remote host reveals what type of Web Application Firewall it is running. This information is critical for an attacker because then the attacker can much better target the attacks.

Soluzione	It is recommended to set your software to not reveal its program name.
Output della vulnerabilità / Evidenze	
	AttackOutput: The site http://192.168.0.3:9084 is behind a SecureIIS

Vulnerabilità	MAC Address 00-0c-29-55-3a-09 VMware, Inc.
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 00-0c-29-55-3a-09 VMware, Inc.

Vulnerabilità	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	9443/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and won't be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Linux 2.2.x-3.x

Vulnerabilità	SSL Client Information
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	443/tcp, 9443/tcp
SPID	58286
Impatto	The target web server do not support encryption Downgrade attack prevention. This might enable attackers to carry out other attacks.
Soluzione	It is recommended to disable SSLv3. Enable HTTP compression only for static content. Upgrade to the latest version of your web application.
Output della vulnerabilità / Evidenze	
	Android 4.2.2 No connection
	Android 4.2.2 No connection
	Android 4.4.2 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)
	Android 5.0.0 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 256 bit ECDH (P-256)
	Android 6.0 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 256 bit ECDH (P-256)

Android 7.0 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Android 8.1 (native) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Android 9.0 (native) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Chrome 65 Win 7 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Chrome 74 (Win 10) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Firefox 62 Win 7 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Firefox 66 (Win 8.1/10) No connection

IE 6 XP No connection

IE 7 Vista No connection

IE 8 Win 7 No connection

IE 8 XP No connection

IE 11 Win 7 TLSv1.2 AES256-GCM-SHA384 No FS

IE 11 Win 8.1 TLSv1.2 AES256-GCM-SHA384 No FS

IE 11 Win Phone 8.1 TLSv1.2 ECDHE-RSA-AES256-SHA 256 bit ECDH (P-256)

IE 11 Win 10 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Edge 15 Win 10 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Edge 17 (Win 10) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Opera 60 (Win 10) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Safari 9 iOS 9 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Safari 9 OS X 10.11 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Safari 10 OS X 10.12 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Apple ATS 9 iOS 9 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Tor 17.0.9 Win 7 No connection

Java 6u45 No connection

Java 7u25 No connection

Java 8u161 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

Java 9.0.4 TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

OpenSSL 1.0.1l TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

OpenSSL 1.0.2e TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

OpenSSL 1.1.0j (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

OpenSSL 1.1.1b (Debian) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256 bit ECDH (P-256)

```
Thunderbird (60.6) TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 256
bit ECDH (P-256)
Done 2023-09-14 16:49:56 [ 24s] --> 192.168.0.3:443 (192.168.0.3) <
--
```

Vulnerabilità	SSL Certificate information
Livello rischio	Informazione
Porta	443/tcp, 9443/tcp
SPID	3702
Impatto	It is possible to retrieve the SSL certificate owner information from the target web server running. In this check please review the vulnerability information provided from the ssl certificate.
Soluzione	If all the information in the certificate output is the correct information and matches what it is supposed to please ignore this check.
Output della vulnerabilità / Evidenze	
	subject=/CN=virtualcenter.img.local/C=US issuer=/CN=CA/DC=vsphere/DC=local/C=US/ST=California/O=virtualcenter.im g.local/OU=VMware Engineering

Vulnerabilità	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 9443
Livello rischio	Informazione
Porta	9443/tcp
SPID	108204
Impatto	The target Port is blocking connections from the Scanner or speed was determined too slow to scan. It means the port is being skipped in critical checks for the Scanner not to hang. It is recommended to allow the Scanner full connection to the port. Otherwise crucial vulnerabilities on the identified port can be missed.
Soluzione	If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Scanner. It is recommended to white list the Scanner for the best result.
Output della vulnerabilità / Evidenze	
	Time: 2297

Vulnerabilità	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
Livello rischio	Informazione
Porta	443/tcp
SPID	108204
Impatto	The target Port is blocking connections from the Scanner or speed was determined too slow to scan. It means the port is being skipped in critical checks for the Scanner not to hang. It is recommended to allow the Scanner full connection to the port. Otherwise crucial vulnerabilities on the identified port can be missed.
Soluzione	If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Scanner. It is recommended to white list the Scanner for the best result.
Output della vulnerabilità / Evidenze	
	Time: 2297

Vulnerabilità	System time via remote Web Server
Livello rischio	Informazione
Porta	80/tcp, 9084/tcp, 9443/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Thu, 14 Sep 2023 14:29:19 GMT

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.3: icmp_seq=0 ttl=64 time=0.5 ms

Vulnerabilità	Direct HTTP 501636 & HTTPS 2 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

Sistema Target: 192.168.0.4

Vulnerabilità	Windows Terminal Services RDP
Livello rischio	Alto
Porta	3389/tcp
SPID	2390
CVE	CVE-2002-0444
CVE	CVE-2001-0860
CVSS	CVE-2002-0444 - CVSS Score V2: 7.5
CVSS	CVE-2001-0860 - CVSS Score V2: 7.5
Impatto	The Terminal Services has been found running. Terminal Services is used to remotely obtain a graphical login interface. If an attacker has gained a valid login and password the attacker can be able to use this service to gain further access on the remote system. The identified service is also known to a remote Denial of Service vulnerability.
Soluzione	Be sure to change the default port. Either disable the Terminal Services from Start->Control-Panel->Administrative Tools->Service and find it and set it to disable and or block incoming TCP traffic to the identified port. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits
Livello rischio	Alto
Porta	445/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening. There has been known exploits like WannaCry on this port and it is recommended to firewall of the port and only allow trusted users to connect to it.

Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	It is possible to obtain remote NetBIOS name table
Livello rischio	☐ ☐ ☒ ☐ Basso
SPID	1770
Impatto	Attackers can use this information to base other attacks on.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	Name Service Type ----- ARBITER Workstation Service WORKGROUP Domain Name ARBITER File Server Service

Vulnerabilità	MAC address obtained via NetBIOS
Livello rischio	☐ ☐ ☒ ☐ Basso
SPID	1771

Impatto	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	MAC Address: 00-50-56-8c-c3-03

Vulnerabilità	HTTP only port without SSL found
Livello rischio	Basso
Porta	5985/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.4:5985/tcp matches http-apache-2

Vulnerabilità	NetBIOS service listening 137 UDP
Livello rischio	Basso
Porta	137/udp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	

Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 139 TCP
Livello rischio	Basso
Porta	139/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.4:135/tcp matches netbios-session
	Protocol on 192.168.0.4:139/tcp matches netbios-session
	Protocol on 192.168.0.4:3389/tcp matches ssl
	Protocol on 192.168.0.4:5985/tcp matches http
	Protocol on 192.168.0.4:5985/tcp matches http-apache-2

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
---------------	--

Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 19:45:51

Vulnerabilità	MAC Address 00-50-56-8c-c3-03 VMware, Inc.
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 00-50-56-8c-c3-03 VMware, Inc.

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	

08:44:55

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
64 octets from 192.168.0.4: icmp_seq=0 ttl=128 time=0.4 ms	

Vulnerabilità	System time via remote Web Server
Livello rischio	Informazione
Porta	5985/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
AttackString: HEAD / HTTP/1.0	
AttackOutput: Thu, 14 Sep 2023 15:05:45 GMT	

Vulnerabilità	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
Livello rischio	Informazione
Porta	135/tcp
SPID	58

Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and won't be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Linux 2.2.x-3.x

Vulnerabilità	Identified Operating System Check #2 Microsoft Windows via Banner
Livello rischio	Informazione
Porta	5985/tcp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and won't be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the https Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0 AttackOutput: HTTP/1.1 404 Not Found Content-Length: 315 Content-Type: text/html charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 14 Sep 2023 15:14:16 GMT Connection: close

Vulnerabilità	Direct HTTP 167181 & HTTPS 0 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

Sistema Target: 192.168.0.13

Vulnerabilità	MAC Address 28-29-86-04-61-53 APC by Schneider Electric
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 28-29-86-04-61-53 APC by Schneider Electric

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.13: icmp_seq=0 ttl=255 time=3.5 ms

Vulnerabilità	Direct HTTP 0 & HTTPS 0 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

Vulnerabilità	File 80sec内部专用过世界杀软体积最小功能超强超猛宇宙第一.asp Information Disclosure webshell
Livello rischio	 Alto
Porta	443/tcp
SPID	84805
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file.
Output della vulnerabilità / Evidenze	
	AttackString: HTTPS GET /owa/auth/80sec内部专用过世界杀软体积最小功能超强超猛宇宙第一.asp HTTP/1.0 AttackOutput: HTTP/1.1 200 OK

Vulnerabilità	File Jspspy%20web~shell%20V1.0%20*MADE%20by%20孤水绕城%20QQ540410588.jsp Information Disclosure webshell
Livello rischio	 Alto
Porta	443/tcp
SPID	84956
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file.
Output della vulnerabilità / Evidenze	
	AttackString: HTTPS GET /owa/auth/Jspspy%20web~shell%20V1.0%20MADE%20by%20孤水绕城%20QQ540410588.jsp HTTP/1.0 AttackOutput: HTTP/1.1 200 OK

Vulnerabilità	File MYSQL%20Manager%20-Asp.net%20Silic%20Group%20Hacker%20Army专用版本.aspx Information Disclosure webshell
Livello rischio	 Alto
Porta	443/tcp
SPID	84972
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file.
Output della vulnerabilità / Evidenze	
	AttackString: HTTPS GET /owa/auth/MYSQL%20Manager%20-Asp.net%20Silic%20Group%20Hacker%20Army专用版本.aspx HTTP/1.0 AttackOutput: HTTP/1.1 200 OK

Vulnerabilità	File response_packet_from_icmpsh_slave_containing_output_of_command_whoami.png Information Disclosure webshell
Livello rischio	 Alto
Porta	443/tcp

SPID	85431
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file.
Output della vulnerabilità / Evidenze	
	AttackString: HTTPS GET /owa/auth/response_packet_from_icmpsh_slave_containing_output_of_command_whoami.png HTTP/1.0 AttackOutput: HTTP/1.1 200 OK

Vulnerabilità	File shell~ Information Disclosure webshell
Livello rischio	Medio
SPID	69829
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can u

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.17:80/tcp matches http Protocol on 192.168.0.17:443/tcp matches ssl Protocol on 192.168.0.17:4343/tcp matches ssl Protocol on 192.168.0.17:8080/tcp matches http Protocol on 192.168.0.17:8080/tcp matches http-apache-2 Protocol on 192.168.0.17:8081/tcp matches http

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 18:03:49

Vulnerabilità	MAC Address d0-15-a6-cc-28-64 Adapter manufacturer: UNKNOWN
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: d0-15-a6-cc-28-64 Adapter manufacturer: UNKNOWN

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefore recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	17:03:49

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simply move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.17: icmp_seq=0 ttl=64 time=0.6 ms

Vulnerabilità System time via remote Web Server	
Livello rischio	Informazione
Porta	80/tcp, 8080/tcp, 8081/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Thu, 14 Sep 2023 16:03:55 GMT

FRED FOR SECURITY DEMO

Sistema Target: 192.168.0.25

Vulnerabilità	SSH Service Accessible
Livello rischio	Alto
Porta	22/tcp
SPID	2733
Impatto	The SSH service allows anyone to connect to it. This is a security risk because an attacker can issue a brute force attack and the service has a history of many dangerous vulnerabilities.
Soluzione	It is recommended to only allow trusted users to connect to it.
Output della vulnerabilità / Evidenze	
	AttackOutput: SSH-2.0-dropbear

Vulnerabilità	DNS Recursion Allowed
Livello rischio	Medio
SPID	56963
Impatto	The target DNS service is subject to a remote DNS Recursion vulnerability. Attackers can exploit this in DDoS Attacks. Recursion is used to process a DNS request where the DNS server performs the request for the client. Recursion should only be allowed for trusted clients.
Soluzione	Set permissions so only trusted clients can do recursion requests or disable recursion. On Unix* You can edit /etc/bind/named.conf. allow-transfer {"none"} allow-recursion {"none"} recursion no On Windows please see: http://technet.microsoft.com/en-us/library/cc771738.aspx
Output della vulnerabilità / Evidenze	
	yahoo.com mail is handled by 1 mta6.am0.yahoodns.net.

Vulnerabilità	8081 Port Identification
Livello rischio	Medio
Porta	8081/tcp
SPID	58833
Impatto	The target service found running is subject to an information vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as the identified daemon.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found software. And it is recommended to set firewall permissions so only trusted users can connect to the found IP address. Note if you are running another service on this port you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	HTTP only port without SSL found
---------------	----------------------------------

Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	8083/tcp, 8084/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.25:8083/tcp matches http

Vulnerabilità	ASP.NET path disclosure
Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	8083/tcp, 8084/tcp
SPID	2190
Impatto	The remote ASP.NET system is vulnerable to a path disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the ASP.NET service from http://www.asp.net/download.aspx
Output della vulnerabilità / Evidenze	
	AttackString: GET /a%5c.aspx HTTP/1.0
	AttackOutput: HTTP/1.0 500 Internal Server Error
	Connection: close

Vulnerabilità	Possible Service/Game: directtv Identified
Livello rischio	☐ ☐ ☒ ☐ Basso
Porta	8082/tcp
SPID	61358
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Identified Operating System Check #2 Microsoft Windows via Banner
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	53/udp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.

Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Microsoft DNS 6.1.7601 (1DB15F75)

Vulnerabilità	All Protocols Tested
Livello rischio	 Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.25:22/tcp matches ssh
	Protocol on 192.168.0.25:80/tcp matches http
	Protocol on 192.168.0.25:8081/tcp matches http
	Protocol on 192.168.0.25:8082/tcp matches http
	Protocol on 192.168.0.25:8083/tcp matches http
	Protocol on 192.168.0.25:8084/tcp matches http

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	 Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 18:32:25

Vulnerabilità	MAC Address e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN
Livello rischio	 Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.

Output della vulnerabilità / Evidenze	
	AttackOutput: e0-23-ff-6e-03-df Adapter manufacturer: UNKNOWN

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	17:32:25

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.25: icmp_seq=0 ttl=64 time=0.5 ms

Vulnerabilità	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
Livello rischio	Informazione
Porta	8084/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	

Linux 2.2.x-3.x

Vulnerabilità	Direct HTTP 334382 & HTTPS 0 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

FRED FOR SECURITY DEMO

Sistema Target: 192.168.0.27

Vulnerabilità	Missing Web Security Header Tag X-Frame-Options
Livello rischio	Medio
Porta	80/tcp
SPID	58663
Impatto	X-Frame-Options is used to communicate to the web browser if you want to allow your site to be framed or not. Preventing the web browser from framing your site to defend against attacks such as clickjacking. The X-Frame-Options header can be used to if a web browser is allowed to render a page in a <frame>, <object>, or <iframe>. It is recommended to enable this check in penetration testing process.
Soluzione	Fix by adding to your site: header("X-Frame-Options: SAMEORIGIN")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Strict-Transport-Security
Livello rischio	Medio
Porta	80/tcp
SPID	58665
Impatto	The HTTP Web Security Header Strict Transport Security is a recommended feature to increase the security on your website and strengthens your implementation of TLS by forcing the User Agent to use HTTPS. It is often know as HSTS that forces the web site to make the web browsers know it should be accessed only by using HTTPS instead of the insecure HTTP.
Soluzione	Fix by adding to your site: header("Strict-Transport-Security: max-age=31536000 includeSubDomains")
Output della vulnerabilità / Evidenze	

Vulnerabilità	File /js/home.js Information Disclosure
Livello rischio	Medio
Porta	80/tcp
SPID	71828
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file. Or if the file is sensitive make it unavailable.
Output della vulnerabilità / Evidenze	
AttackString: HTTP GET /js/home.js HTTP/1.0	
AttackOutput: HTTP/1.1 200 OK	
Date: Thu, 14 Sep 2023 21:56:34 GMT	
Server: Hydra/0.1.8	
Accept-Ranges: bytes	
Connection: close	
Content-Length: 14718	
Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT	
Content-Type: text/plain	
var isSafari = (navigator.vendor && (navigator.vendor.toLowerCase().indexOf(apple) != -1)) ? true : false	

```

var isFF = (navigator.userAgent && (navigator.userAgent.toLowerCase().
indexOf(firefox) != -1) ) ? true : false
var isChrome = (navigator.userAgent && (navigator.userAgent.toLowerCase().indexOf(chrome) != -1) ) ? true : false
_top = self
_top.STYLING = {
afterPOST: "",
successMsg: "Success.",
successMsgNS: {
msgType: 1,
msgText: "Success. To permanently save the configuration, go to <a href='\"javascript:NavigateFromSuccessMessage()\"' class='\"onLig
ht\"></a> page or click Save icon.",
linkText: "Copy/Save Configuration",
linkFunc: function(){}
},
edtBtnNotSelect: "Edit: only selected entry could be processed.",
edtBtnNotSingle: "Edit: only single entry could be processed.",
delBtnNotSelect: "Delete: only selected entries could be processed."
,
separator: ":",
reqEmptyMsg: "The field cannot be empty.",
reqTooltip: "* = Required fields.",
emptyTbl: "0 results found.",
sessionId: Math.round(Math.random()*10000000000000000).toString(10),
alertBox:
title: "",
msg: "",
func: function(){} ,
severity: 0,
closeDialog: false,
hasCancel:true,
isNotify:false,
noConfirmFuncHash: {}
},
buttons:
getMinWidth: function() {return 18
},
getShortWidth: function() {return 80
},
getLongWidth: function() {return 160
navigator.sayswho= (function(){
var ua= navigator.userAgent,
N= navigator.appName, tem,
M= ua.match(/(opera|chrome|safari|firefox|msie|trident)\/?\s*([\\d\\.]+)/i) ||
[]
M= M[2]? [M[1], M[2]]:[N, navigator.appVersion, -?]
if(M && (tem= ua.match(/version\/([\\d\\.]+)/i))!= null) M[2]= tem[1]
]
return M.join( )

```

```

})();
function isBrowserOlderIE10() {
if (isIE()) {
var ver = navigator.sayswho.split(" ")[1]
var ver_major = ver.split(".")[0]
if (parseInt(v

```

Vulnerabilità	File /home.html Information Disclosure
Livello rischio	Medio
Porta	80/tcp
SPID	67577
Impatto	The identified file found on the remote web server is subject to a remote information disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found file. Or if the file is sensitive make it unavailable.
Output della vulnerabilità / Evidenze	
<pre> AttackString: HTTP GET /home.html HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Thu, 14 Sep 2023 21:53:38 GMT Server: Hydra/0.1.8 Accept-Ranges: bytes Connection: close Content-Length: 43002 Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT Content-Type: text/html <html> <head> <title></title> <meta http-equiv="Content-Type" content="text/html charset=utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=Emulat eIE10"> <meta name="csrf-token" content=""> <link href="images/favicon.gif" type="text/css" rel="s hortcut icon" > <!--[if lte IE 6]> <link type="text/css" href="css/styling_ie6.css" rel= "stylesheet"> <![endif]--> <script src="js/jquery-1_10_2_min.js" type="text/javascript"> </script> <script src="js/underscore-1_5_1_min.js" type="text/javascr ipt"></script> <script src="js/backbone-1_0_0_min.js" type="text/javascrip t"></script> <script src="js/fileload-1_0_0_6.js" type="text/javascript"> </script> <script type="text/javascript" src="../../js/crypt/jsbn.js"> </script> </pre>	

```

<script type="text/javascript" src="../../js/crypt/prng4.js">
</script>
<script type="text/javascript" src="../../js/crypt/rng.js">
</script>
<script type="text/javascript" src="../../js/crypt/rsa.js">
</script>
<script type="text/javascript" src="../../js/crypt/base64.js">
</script>
<script>
var RootFrame = true
var MockupMode = false
var DebugMode = false
var fileVer = 1.1.4.8
var deviceId = null
var country = null
var devPortNum = 0
var devPoePortNum = 0
var defPage = null
var defHelp = null
var data
var infoMsg

```

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")
Output della vulnerabilità / Evidenze	

Vulnerabilità	SSL PFS Forward Secrecy Check
Livello rischio	Medio
Porta	443/tcp
SPID	58291
Impatto	The remote target SSL server do not offer PFS Forward Secrecy. It is recommended to enable it or it can render the server vulnerable to Man in the Middle attacks.
Soluzione	It is recommended to disable SSLv3. Enable HTTP compression only for static content. Upgrade to the latest version of your web application.
Output della vulnerabilità / Evidenze	
	No ciphers supporting Forward Secrecy offered

Vulnerabilità	Missing Web Security Header Tag Content-Security-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58667
Impatto	The Content Security Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Content-Security-Policy: block-all-mixed-content script-src 'self' www.youriste.com ")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Xss-Protection HTTP
Livello rischio	Medio
Porta	80/tcp
SPID	58662
Impatto	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP.
Soluzione	To add the header please see: https://scotthelme.co.uk/hardening-your-http-response-headers/#x-xss-protection X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1 mode=block" FIX: header("X-Xss-Protection: 1 mode=block")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	Medio
Porta	80/tcp
SPID	58666
Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Content-Type-Options
Livello rischio	Medio
Porta	80/tcp
SPID	58664

Impatto	X-Content-Type-Options Security Header is used to prevent a browser from trying to MIME sniff the sensitive content type & forces the browser to use the declared content-type. The HTTP Security header is used by the server to indicate the MIME types advertised in the Content-Type headers to not be changed. This can prevent MIME type sniffing. The header was first introduced by Microsoft in Internet Explorer IE 8 to allow webmasters block content sniffing that could transform non-executable MIME types into executable MIME type. Other web browsers have introduced it as well. It is recommended by penetration testing process to expect this header to be set. The only valid value you can set for this header is nosniff.
Soluzione	Fix by adding to your site: header("X-Content-Type-Options: nosniff")
Output della vulnerabilità / Evidenze	

Vulnerabilità	HTTP only port without SSL found
Livello rischio	 Basso
Porta	80/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
AttackOutput: Protocol on 192.168.0.27:80/tcp matches http	

Vulnerabilità	Interesting directory HTTP /help/ Identified
Livello rischio	 Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
AttackString: GET /help/ HTTP/1.0	
AttackOutput: HTTP/1.1 200 OK	
Date: Thu, 14 Sep 2023 20:56:50 GMT	
Server: Hydra/0.1.8	
Accept-Ranges: bytes	
Connection: close	
Content-Length: 211560	
Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT	
Content-Type: text/html	

Vulnerabilità	Interesting directory HTTP ././ Identified
Livello rischio	 Informazione
Porta	80/tcp
SPID	56003

Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
AttackString: GET ../../ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Thu, 14 Sep 2023 20:39:24 GMT Server: Hydra/0.1.8 Accept-Ranges: bytes Connection: close Content-Length: 225 Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT Content-Type: text/html <html> <head> <script type="text/javascript"> function gotoLogin() var fileVer = (new Date().getTime()) window.location.href="login.html?ver="+fileVer </script> </head> <body onload="gotoLogin()"> "> </body> </html>	

Vulnerabilità	Interesting directory HTTP /%00/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
AttackString: GET /%00/ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Thu, 14 Sep 2023 20:39:22 GMT Server: Hydra/0.1.8 Accept-Ranges: bytes Connection: close Content-Length: 225 Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT Content-Type: text/html <html>	

```

<head>
<script type="text/javascript">
function gotoLogin()
var fileVer = (new Date()).getTime()
window.location.href="login.html?ver="+fileVer
</script>
</head>
<body onload="gotoLogin()"
">
</body>
</html>

```

Vulnerabilità	Interesting directory HTTP /%00/interact.sh/ Identified
Livello rischio	Informazione
Porta	80/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .

Output della vulnerabilità / Evidenze

```

AttackString: GET /%00/interact.sh/ HTTP/1.0
AttackOutput: HTTP/1.1 200 OK
Date: Thu, 14 Sep 2023 20:37:28 GMT
Server: Hydra/0.1.8
Accept-Ranges: bytes
Connection: close
Content-Length: 225
Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT
Content-Type: text/html
<html>
<head>
<script type="text/javascript">
function gotoLogin()
var fileVer = (new Date()).getTime()
window.location.href="login.html?ver="+fileVer
</script>
</head>
<body onload="gotoLogin()"
">
</body>
</html>

```

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione

SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.27:22/tcp matches ssh
	Protocol on 192.168.0.27:22/tcp matches ssh-openssh
	Protocol on 192.168.0.27:80/tcp matches http

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 21:59:06

Vulnerabilità	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
Livello rischio	Informazione
Porta	443/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Linux 2.2.x-3.x

Vulnerabilità	SSL Client Information
Livello rischio	Informazione
Porta	443/tcp
SPID	58286

Impatto	The target web server do not support encryption Downgrade attack prevention. This might enable attackers to carry out other attacks.
Soluzione	It is recommended to disable SSLv3. Enable HTTP compression only for static content. Upgrade to the latest version of your web application.
Output della vulnerabilità / Evidenze	
	Android 4.2.2 No connection
	Android 4.2.2 No connection
	Android 4.4.2 TLSv1.2 AES256-GCM-SHA384 No FS
	Android 5.0.0 TLSv1.2 AES256-SHA No FS
	Android 6.0 TLSv1.2 AES128-GCM-SHA256 No FS
	Android 7.0 TLSv1.2 AES128-GCM-SHA256 No FS
	Android 8.1 (native) TLSv1.2 AES128-GCM-SHA256 No FS
	Android 9.0 (native) TLSv1.2 AES128-GCM-SHA256 No FS
	Chrome 65 Win 7 TLSv1.2 AES128-GCM-SHA256 No FS
	Chrome 74 (Win 10) TLSv1.2 AES128-GCM-SHA256 No FS
	Firefox 62 Win 7 TLSv1.2 AES128-SHA No FS
	Firefox 66 (Win 8.1/10) No connection
	IE 6 XP No connection
	IE 7 Vista No connection
	IE 8 Win 7 No connection
	IE 8 XP No connection
	IE 11 Win 7 TLSv1.2 AES256-GCM-SHA384 No FS
	IE 11 Win 8.1 TLSv1.2 AES256-GCM-SHA384 No FS
	IE 11 Win Phone 8.1 TLSv1.2 AES128-SHA256 No FS
	IE 11 Win 10 TLSv1.2 AES256-GCM-SHA384 No FS
	Edge 15 Win 10 TLSv1.2 AES256-GCM-SHA384 No FS
	Edge 17 (Win 10) TLSv1.2 AES256-GCM-SHA384 No FS
	Opera 60 (Win 10) TLSv1.2 AES128-GCM-SHA256 No FS
	Safari 9 iOS 9 TLSv1.2 AES256-GCM-SHA384 No FS
	Safari 9 OS X 10.11 TLSv1.2 AES256-GCM-SHA384 No FS
	Safari 10 OS X 10.12 TLSv1.2 AES256-GCM-SHA384 No FS
	Apple ATS 9 iOS 9 No connection
	Tor 17.0.9 Win 7 No connection
	Java 6u45 No connection
	Java 7u25 No connection
	Java 8u161 TLSv1.2 AES256-SHA256 No FS
	Java 9.0.4 TLSv1.2 AES256-GCM-SHA384 No FS
	OpenSSL 1.0.1l TLSv1.2 AES256-GCM-SHA384 No FS
	OpenSSL 1.0.2e TLSv1.2 AES256-GCM-SHA384 No FS
	OpenSSL 1.1.0j (Debian) TLSv1.2 AES256-GCM-SHA384 No FS
	OpenSSL 1.1.1b (Debian) TLSv1.2 AES256-GCM-SHA384 No FS
	Thunderbird (60.6) TLSv1.2 AES128-SHA No FS
	Done 2023-09-14 22:22:38 [39s] --> 192.168.0.27:443 (192.168.0.27) <<--

Vulnerabilità	SSL Certificate information
Livello rischio	Informazione
Porta	443/tcp

SPID	3702
Impatto	It is possible to retrieve the SSL certificate owner information from the target web server running. In this check please review the vulnerability information provided from the ssl certificate.
Soluzione	If all the information in the certificate output is the correct information and matches what it is supposed to please ignore this check.
Output della vulnerabilità / Evidenze	
	subject=/CN=My Name/OU=My Organization
	issuer=/CN=My Name/OU=My Organization

Vulnerabilità	Target port found slow to scan or scanner is being blocked by firewall/ips system Port: 443
Livello rischio	Informazione
Porta	443/tcp
SPID	108204
Impatto	The target Port is blocking connections from the Scanner or speed was determined too slow to scan. It means the port is being skipped in critical checks for the Scanner not to hang. It is recommended to allow the Scanner full connection to the port. Otherwise crucial vulnerabilities on the identified port can be missed.
Soluzione	If the speed is slow there might be a connection problem or a firewall/ips/shunning system blocking the Scanner. It is recommended to white list the Scanner for the best result.
Output della vulnerabilità / Evidenze	
	Time: 1683

Vulnerabilità	System time via remote Web Server
Livello rischio	Informazione
Porta	80/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Thu, 14 Sep 2023 19:59:11 GMT

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.27: icmp_seq=0 ttl=64 time=0.5 ms

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	20:59:06

Vulnerabilità	MAC Address b0-7d-47-37-98-d4 Cisco Systems, Inc
Livello rischio	Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: b0-7d-47-37-98-d4 Cisco Systems, Inc

Vulnerabilità	File /login.html admin interface identified
Livello rischio	Informazione

Porta	80/tcp
SPID	59062
Impatto	A possible administration interface identified. An attacker can use this information to base other attacks on.
Soluzione	It is recommended to keep the system up to date.
Output della vulnerabilità / Evidenze	
	<pre> AttackString: HTTP GET /login.html HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Thu, 14 Sep 2023 21:58:06 GMT Server: Hydra/0.1.8 Accept-Ranges: bytes Connection: close Content-Length: 22770 Last-Modified: Mon, 01 Jan 2019 00:00:00 GMT Content-Type: text/html <html> <head> <title></title> <meta http-equiv="Content-Type" content="text/html charset=utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=Emulat eIE10"> <link href="images/favicon.gif" type="text/css" rel="& quot;shortcut icon" > <!--[if lte IE 6]> <link type="text/css" href="css/styling_ie6.css" rel= "stylesheet"> <![endif]--> <script src="js/jquery-1_10_2_min.js" type="text/javascript& quot;></script> <script src="js/underscore-1_5_1_min.js" type="text/javascr ipt"></script> <script src="js/backbone-1_0_0_min.js" type="text/javascrip t"></script> <script src="js/fileload-1_0_0_6.js" type="text/javascript&qu ot;></script> <script type="text/javascript" src="js/crypt/jsbn.js"> </script> <script type="text/javascript" src="js/crypt/prng4.js"> </script> <script type="text/javascript" src="js/crypt/rng.js"> </script> <script type="text/javascript" src="js/crypt/rsa.js"> </script> <script type="text/javascript" src="js/crypt/base64.js" ></script> <style type="text/css"> .titleciscolog font-family: Arial, sans-serif font-size: 22px color: #ffffff </pre>

```
.titleciscouser  
font-family: Arial, sans-serif  
font-size: 12px  
color: #ffffff  
.titlecisco3log  
font-family: Arial, sans-serif  
font-size: 12px  
color: #ffffff  
#cellMessage span.inv
```

FRED FOR SECURITY DEMO

Sistema Target: 192.168.0.29

Vulnerabilità	Apple RTSP quicktime Remote Preauth Code Execution
Livello rischio	Alto
Porta	554/tcp
SPID	4773
Impatto	The identified port found open on the target system with the found service is known to be subject to a remote buffer execution Overflow that an attacker can exploit to execute arbitrary code on the target system.
Soluzione	It is recommended to block incoming traffic to the identified port and or only allow trusted users to connect to it and further more make sure you have the latest version of the service.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	X Font Service found on the remote system
Livello rischio	Alto
Porta	7100/tcp
SPID	3298
CVE	CVE-2002-1317
CVSS	CVE-2002-1317 - CVSS Score V2: 7.5
Impatto	The identified system was found running the X Font Service. The X Font service has a history of vulnerabilities where it can be possible for a remote attacker to gain root access on the remote system.
Soluzione	It is highly recommended to block incoming traffic to the found port at firewall level. Further more make sure you are running the latest X Font service for your system. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	Microsoft(R) Biztalk Server Vulnerability
Livello rischio	Alto
Porta	82/tcp, 30001/tcp
SPID	3719
CVE	CVE-2003-0117
CVE	CVE-2003-0118
CVSS	CVE-2003-0117 - CVSS Score V2: 7.5
CVSS	CVE-2003-0118 - CVSS Score V2: 7.5

Impatto	The target system is running the Microsoft BizTalk service. Found file biztalkhttpreceive.dll on the remote web server. It is subject to several vulnerabilities where it is possible for an attacker to cause an SQL insertion attacker and or execute arbitrary code on the system This can lead to the compromise of the service.
Soluzione	Please issue the patch from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-016.asp NOTE: If you already applied the patch please ignore this check.

Output della vulnerabilità / Evidenze

AttackString: GET /cgi-bin/biztalkhttpreceive.dll HTTP/1.0
Content-Length: 7
UNKNOWN
AttackOutput: HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml
charset=utf-8
Content-Length: 2836
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ; xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tnsl="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" ; xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd/Analytics/wsd" xmlns:tds="http://www.onvif.org/ver10/device/wsd" ; xmlns:tes-cppb="http://www.onvif.org/ver10/events/wsd/CreatePullPointBinding" xmlns:tes-e="http://www.onvif.org/ver10/events/wsd/EventBinding" xmlns:tes-nc="http://www.onvif.org/ver10/events/wsd/NotificationConsumerBinding" xmlns:tes-np="http://www.onvif.org/ver10/events/wsd/NotificationProducerBinding" xmlns:tes-ppb="http://www.onvif.org/ver10/events/wsd/PullPointBinding" xmlns:tes-pps="http://www.onvif.org/ver10/events/wsd/PullPointSubscriptionBinding" xmlns:tev="http://www.onvif.org/ver10/events/wsd" xmlns:tes-psmb="http://www.onvif.org/ver10/events/wsd" />

Vulnerabilità	ctf australia 2014 / SCADA PLC RUGGEDCOM DNP3 System Identified
Livello rischio	Medio
Porta	20000/tcp
SPID	58573

Impatto	SCADA PLC RUGGEDCOM DNP3 port /DNP3 DNP3 Master device DNP3 (Port 20000) The Distributed Network Protocol (DNP3) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies; usage in other industries is not common. As it was developed for communications between various types of data acquisition and control equipment, this protocol plays a crucial role in SCADA/control systems, where it is used by SCADA master stations, Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter-Control Center Communications Protocol (a part of the IEC 60870-6 protocol), is used for inter-master station communications. The target service found running can be subject to a remote buffer overflow vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as the identified daemon.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found software. And it is recommended to set firewall permissions so only trusted users can connect to the found IP address. Note if you are running another service on this port you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Missing Web Security Header Tag X-Content-Type-Options
Livello rischio	☒ ☐ ☐ ☐ Medio
Porta	30000/tcp
SPID	58664
Impatto	X-Content-Type-Options Security Header is used to prevent a browser from trying to MIME sniff the sensitive content type & forces the browser to use the declared content-type. The HTTP Security header is used by the server to indicate the MIME types advertised in the Content-Type headers to not be changed. This can prevent MIME type sniffing. The header was first introduced by Microsoft in Internet Explorer IE 8 to allow webmasters block content sniffing that could transform non-executable MIME types into executable MIME type. Other web browsers have introduced it as well. It is recommended by penetration testing process to expect this header to be set. The only valid value you can set for this header is nosniff.
Soluzione	Fix by adding to your site: header("X-Content-Type-Options: nosniff")
Output della vulnerabilità / Evidenze	

Vulnerabilità	uTorrent Peer to Peer Web Server
Livello rischio	☒ ☐ ☐ ☐ Medio
Porta	20000/tcp
SPID	5333
Impatto	The identified uTorrent Peer to Peer web server found running indicated that a P2P Web server is active in your network. This can be abused to share illegal files and copyrighted materials on the target system.
Soluzione	Please upgrade to the latest version from of the software and or remove the system from the network if your policy forbids it.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Web Server Authentication Method NTLM Disclosure
Livello rischio	Medio
Porta	82/tcp
SPID	1640
CVE	CVE-2002-0419
CVSS	CVE-2002-0419 - CVSS Score V2: 5
Impatto	The identified IIS running could be identified to run the Basic authentication. An attacker can misuse this to do a specific based brute force attack against the remote host.
Soluzione	Please issue the patch from Microsoft(R) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/wsrsvsec.asp

Output della vulnerabilità / Evidenze

```

AttackString: GET / HTTP/1.1
Host: iis-server
Authorization: Negotiate TlRMTVNTUAABAAAAB4IAoAAAAAAAAAAAAAAAAAAAAA=
AttackOutput: HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml
charset=utf-8
Content-Length: 2836
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tns1="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd" xmlns:tds="h

```

Vulnerabilità	Missing Web Security Header Tag Strict-Transport-Security
Livello rischio	Medio
Porta	80/tcp, 30000/tcp
SPID	58665

Impatto	The HTTP Web Security Header Strict Transport Security is a recommended feature to increase the security on your website and strengthens your implementation of TLS by forcing the User Agent to use HTTPS. It is often know as HSTS that forces the web site to make the web browsers know it should be accessed only by using HTTPS instead of the insecure HTTP.
Soluzione	Fix by adding to your site: header("Strict-Transport-Security: max-age=31536000 includeSubDomains")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	 Medio
Porta	80/tcp, 30000/tcp
SPID	58666
Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Content-Security-Policy
Livello rischio	 Medio
Porta	80/tcp, 30000/tcp
SPID	58667
Impatto	The Content Security Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Content-Security-Policy: block-all-mixed-content script-src 'self' www.youriste.com ")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	 Medio
Porta	80/tcp, 30000/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Web Server Authentication Method Basic Disclosure
Livello rischio	 Medio

Porta	82/tcp
SPID	2103
CVE	CVE-2002-0419
CVSS	CVE-2002-0419 - CVSS Score V2: 5
Impatto	The identified IIS running could be identified to run the Basic authentication. An attacker can misuse this to do a specific based brute force attack against the remote host.
Soluzione	Please issue the patch from Microsoft(R) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/wsrsvsec.asp

Output della vulnerabilità / Evidenze

AttackString: GET / HTTP/1.1
Host: iis-server
Authorization: Basic cTFraTk6ZDA5a2xt
AttackOutput: HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml
charset=utf-8
Content-Length: 2836
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tnsl="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd" xmlns:tds="h

Vulnerabilità	Missing Web Security Header Tag X-Xss-Protection HTTP
Livello rischio	Medio
Porta	30000/tcp
SPID	58662
Impatto	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks. Although these protections are largely unnecessary in modern browsers when sites implement a strong Content-Security-Policy that disables the use of inline JavaScript ('unsafe-inline'), they can still provide protections for users of older web browsers that don't yet support CSP.

Soluzione	To add the header please see: https://scotthelme.co.uk/hardening-your-http-response-headers/#x-xss-protection X-XSS-Protection sets the configuration for the cross-site scripting filter built into most browsers. Recommended value "X-XSS-Protection: 1 mode=block" FIX: header("X-Xss-Protection: 1 mode=block")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Sage Content Management System Cross Site Scripting
Livello rischio	Medio
Porta	30000/tcp
SPID	3526
Impatto	The identified Sage Content Management System found running on the remote web server is subject to a Cross Site Scripting Vulnerability. This can allow an attacker to steal cookie-based authentication credentials from legitimate users of the system. This can lead to some part compromise.
Soluzione	Please upgrade to the latest version of the software you are running.
Output della vulnerabilità / Evidenze	
	AttackString: GET /?mod=<script>alert(document.cookie)</script>&gt; ;&op=browse HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Content-Type:text/html X-Frame-Options: SAMEORIGIN <!DOCTYPE html><html><head><title></title><META http-equiv="Content-Type" content="text/html charset=utf-8"><META http-equiv="Pragma" content="no-cache"><META http-equiv="Cache-Control" content="no-cache"><META http-equiv="Expires" content="0"><style type="text/css">html, body{height: 100% margin: 0px overflow: hidden }</style><script type="text/javascript">function release(){document.frames[banner].release()}</script></head><body><iframe name="banner"&quot; id="banner" hideFocus="hideFocus" marginwidth="0" marginheight="0" src=" ../index.htm?client IpAddr=172.16.0.1&IsRemote=0&mod=&ltscript&gtalert(document.cookie)&lt/script&gt&op=browse" frameborder="&quot; 0" width="100%" height="100%"></iframe&gt;</body></html>

Vulnerabilità	Oracle 9iAS Access of SOAP documentation
Livello rischio	Basso
Porta	82/tcp, 30001/tcp
SPID	2053
Impatto	It is possible on the remote system to access the SOAP documentation. Those files can be used by an attacker to determine what kind of system is running on the target system.

Soluzione	From http://www.oracle.com/appserver/ click on download to enter download section. From there choose oracle application server NOTE* You will need a USERNAME and PASSWORD in order to download the latest version. For more information please see http://otn.oracle.com/deploy/security/pdf/ias_soap_alert.pdf And or Remove the soapdocs alias from the Oracle 9iAS http.conf: Alias /soapdocs/ \$ORACLE_HOME/soap/docs/
------------------	---

Output della vulnerabilità / Evidenze

AttackString: GET /ReleaseNotes.html HTTP/1.0
AttackOutput: HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml
charset=utf-8
Content-Length: 2836
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tns1="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd/" xmlns:tds="http://www.onvif.org/ver10/device/wsd/" xmlns:tes-cppb="http://www.onvif.org/ver10/events/wsd/CreatePullPointBinding" xmlns:tes-e="http://www.onvif.org/ver10/events/wsd/EventBinding" xmlns:tes-nc="http://www.onvif.org/ver10/events/wsd/NotificationConsumerBinding" xmlns:tes-np="http://www.onvif.org/ver10/events/wsd/NotificationProducerBinding" xmlns:tes-ppb="http://www.onvif.org/ver10/events/wsd/PullPointBinding" xmlns:tes-pps="http://www.onvif.org/ver10/events/wsd/PullPointSubscriptionBinding" xmlns:tev="http://www.onvif.org/ver10/events/wsd/" xmlns:tes-psmb="http://www.onvif.org/ver10/events/wsd/"

Vulnerabilità	File userslist.asp Path Disclosure
Livello rischio	☐ ☐ ☒ Basso
Porta	82/tcp, 30001/tcp
SPID	6637
Impatto	The identified userslist.asp file found on the remote web server is subject to a remote path disclosure vulnerability. An attacker can exploit this information to base other attacks on.
Soluzione	Please upgrade to the latest version from http://www.persianblog.com
Output della vulnerabilità / Evidenze	
AttackString: GET /userslist.asp?page=2&catid=16 HTTP/1.0	

```

AttackOutput: HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml
charset=utf-8
Content-Length: 2836
Connection: close
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tnsl="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd" xmlns:tds="h

```

Vulnerabilità	ASP.NET path disclosure
Livello rischio	Basso
Porta	82/tcp, 30001/tcp, 49152/tcp
SPID	2190
Impatto	The remote ASP.NET system is vulnerable to a path disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the ASP.NET service from http://www.asp.net/download.aspx
Output della vulnerabilità / Evidenze	
<pre> AttackString: GET /a%5c.aspx HTTP/1.0 AttackOutput: HTTP/1.1 500 Internal Server Error Server: gSOAP/2.7 Content-Type: text/xml charset=utf-8 Content-Length: 2836 Connection: close <?xml version="1.0" encoding="UTF-8"?> </pre>	

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ; xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tns1="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" ; xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tp1="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd/" xmlns:tds="http://www.onvif.org/ver10/device/wsd/" ; xmlns:tes-cppb="http://www.onvif.org/ver10/events/wsd/CreatePullPointBinding" xmlns:tes-e="http://www.onvif.org/ver10/events/wsd/EventBinding" xmlns:tes-nc="http://www.onvif.org/ver10/events/wsd/NotificationConsumerBinding" xmlns:tes-np="http://www.onvif.org/ver10/events/wsd/NotificationProducerBinding" xmlns:tes-ppb="http://www.onvif.org/ver10/events/wsd/PullPointBinding" xmlns:tes-ps="http://www.onvif.org/ver10/events/wsd/PullPointSubscriptionBinding" xmlns:tev="http://www.onvif.org/ver10/events/wsd/" xmlns:tes-psmb="http://www.onvif.org/ver10/events/wsd/"
```

Vulnerabilità	Possible Service/Game: Star Wars Identified
Livello rischio	☐ ☒ ☐ Basso
Porta	7070/tcp
SPID	61064
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Possible Service/Game: freephoneline Identified
Livello rischio	☐ ☒ ☐ Basso
Porta	6060/tcp
SPID	61289
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.

Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	HTTP only port without SSL found
Livello rischio	 Basso
Porta	80/tcp, 82/tcp, 30000/tcp, 30001/tcp, 49152/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.29:80/tcp matches http

Vulnerabilità	Lethal Attack 1 HTTP Possible CGI
Livello rischio	 Basso
Porta	80/tcp
SPID	62585
Impatto	The identified files found in the VULNOUTPUT section reveals sensitive error information. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the identified file and or if you coded it your self please make input tests on it.
Output della vulnerabilità / Evidenze	
	Lethal Attack Crawler Possible CGI: (GET http://192.168.0.29/cgi-bin/main-cgi)

Vulnerabilità	Identified Operating System Check #2 Linux via Banner
Livello rischio	 Informazione
Porta	49152/tcp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the https Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0 AttackOutput: HTTP/1.0 500 Internal Server Error

SERVER: Linux/3.18.20, UPnP/1.0, Portable SDK for UPnP devices/1.6.22
CONTENT-LENGTH: 60
CONTENT-TYPE: text/html
<html><body> 500 Internal Server Error </body></html>

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.29:80/tcp matches http
	Protocol on 192.168.0.29:82/tcp matches http
	Protocol on 192.168.0.29:554/tcp matches streaming-server
	Protocol on 192.168.0.29:30000/tcp matches http
	Protocol on 192.168.0.29:30001/tcp matches http
	Protocol on 192.168.0.29:49152/tcp matches http

Vulnerabilità	Interesting directory HTTP ../ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET ../ HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	Date: Tue, 19 Sep 2023 09:16:13 GMT
	Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT
	Etag: "5f2cbf8e.10699"
	Content-Type: text/html
	Content-Length: 10699
	Connection: close
	Accept-Ranges: bytes
	X-Content-Type-Options: nosniff
	X-Frame-Options: SAMEORIGIN
	x-xss-protection: 1
	mode=block
	<!DOCTYPE html>
	<html>
	<head>
	<script>

```

/**
 * 防止浏览器缓存导致登录页的js文件加载失败
 * 如果url中没有参数则为url加上一个随机数重新加载，需要过滤cloud方式登录
 * @return {[type]} [description]
 */
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(=) && -1 === href.indexOf(/{)){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&
quot; />
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Vulnerabilità	Identified Operating System Check #2 Linux via Banner
Livello rischio	Informazione
Porta	82/tcp
SPID	58296

Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible. Vulnerability found: NAME: Information: Identified Operating System Check #2 Element OS Linux via Banner RISK: Low SPID: 58296 IMPACT: Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched. RECOMMENDED SOLUTION: It is recommended to clean the identified version banner so it reveals as less information as possible.

Output della vulnerabilità / Evidenze

Please note in this check it only relied on the https Version check. So if you have a vulnerable version with custom patches you might look away from this check. AttackString: HEAD / HTTP/1.0

AttackOutput: HTTP/1.1 500 Internal Server Error

Server: gSOAP/2.7

Content-Type: text/xml

charset=utf-8

Content-Length: 2837

Connection: close

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/tns.xsd" xmlns:tns1="http://www.onvif.org/ver10/topics" xmlns:c14n="http://www.w3.org/2001/10/xml-exc-c14n#" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:xmime5="http://tempuri.org/xmime5.xsd" xmlns:xop="http://www.w3.org/2004/08/xop/include" xmlns:tplt="http://www.onvif.org/ver10/plus/schema" xmlns:tt="http://www.onvif.org/ver10/schema" xmlns:wstop="http://docs.oasis-open.org/wsn/t-1" xmlns:wsrfr="http://docs.oasis-open.org/wsrfr/r-2" xmlns:wsrfrbf="http://docs.oasis-open.org/wsrfr/bf-2" xmlns:tanae="http://www.onvif.org/ver20/analytics/wsd/AnalyticsEngineBinding" xmlns:tanre="http://www.onvif.org/ver20/analytics/wsd/RuleEngineBinding" xmlns:tan="http://www.onvif.org/ver20/analytics/wsd/Analytics" xmlns:tds="http://www.onvif.org/ver10/device/wsd" xmlns:tes-cppb="http://www.onvif.org/ver10/events/wsd/CreatePullPointBinding" xmlns:tes-e="http://www.onvif.org/ver10/events/wsd/EventBinding" xmlns:tes-nc="http://www.onvif.org/ver10/events/wsd/NotificationConsumerBinding" xmlns:tes-np="http://www.onvif.org/ver10/events/wsd/NotificationProducerBinding" xmlns:tes-ppb="http://www.onvif.org/ver10/events/wsd/PullPointBinding" xmlns:tes-pps="http://www.onvif.org/ver10/events/wsd/PullPointSubscriptionBinding" xmlns:tev="http://www.onvif.org/ver10/events/wsd" xmlns:tes-psmb="http://www.onvif.org/ver10/events/wsd"/>
```

Vulnerabilità	MAC Address 48-ea-63-bb-4f-55 Zhejiang Uniview Technologies Co., Ltd.
Livello rischio	Informazione

SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 48-ea-63-bb-4f-55 Zhejiang Uniview Technologies Co., Ltd.

Vulnerabilità	Interesting directory HTTP /.../.../ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /.../.../.../ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Tue, 19 Sep 2023 09:16:13 GMT Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT Etag: "5f2cbf8e.10699" Content-Type: text/html Content-Length: 10699 Connection: close Accept-Ranges: bytes X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN x-xss-protection: 1 mode=block <!DOCTYPE html> <html> <head> <script> /** * 防止浏览器缓存导致登录页的js文件加载失败 * 如果url中没有参数则为url上加上一个随机数重新加载，需要过滤cloud方式登录 * @return {[type]} [description] */ (function(){ var href = window.location.href var ran = Math.round(Math.random() * 10000000000000) if (-1 === href.indexOf(?)){ window.location.href = href + ?_ = + ran } else if (-1 === href.indexOf(=) && -1 === href.indexOf((/?)){

```

window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&
quot; />
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Vulnerabilità	Interesting directory HTTP /...../ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
	AttackString: GET /...../ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Tue, 19 Sep 2023 09:16:13 GMT Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT Etag: "5f2cbf8e.10699" Content-Type: text/html Content-Length: 10699

```
Connection: close
Accept-Ranges: bytes
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
x-xss-protection: 1
mode=block
<!DOCTYPE html>
<html>
<head>
<script>
/**
 * 防止浏览器缓存导致登录页的js文件加载失败
 * 如果url中没有参数则为url上加上一个随机数重新加载，需要过滤cloud方式登录
 * @return {[type]} [description]
 */
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(=) && -1 === href.indexOf(/{))){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&quot; />
<meta http-equiv="Content-Type" content="text/html charset=utf-8" />
<meta content="favicon.ico" itemprop="image" />
<link rel="stylesheet" href="/style/plugins/jquery-ui.min_6389365.css" type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css" />
<link rel="stylesheet" href="style/color.css" />
<title data-text="Text.VideoManageSystem"></title>
</head>
<body id="login_body" class="login_min_height_width">
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionTip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
```

```
</div>
<div class="login_f
```

Vulnerabilità	Interesting directory HTTP /...../ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
<pre> AttackString: GET /...../ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Tue, 19 Sep 2023 09:16:13 GMT Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT Etag: "5f2cbf8e.10699" Content-Type: text/html Content-Length: 10699 Connection: close Accept-Ranges: bytes X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN x-xss-protection: 1 mode=block <!DOCTYPE html> <html> <head> <script> /** * 防止浏览器缓存导致登录页的js文件加载失败 * 如果url中没有参数则为url上加上一个随机数重新加载，需要过滤cloud方式登录 * @return {[type]} [description] */ (function(){ var href = window.location.href var ran = Math.round(Math.random() * 1000000000000) if (-1 === href.indexOf(?)){ window.location.href = href + ?_ = + ran } else if (-1 === href.indexOf(=) && -1 === href.indexOf(/{))){ window.location.href = href + &_ = + ran } })(); </script> <meta http-equiv="X-UA-Compatible" content="edge& quot; /> </pre>	

```
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f
```

Vulnerabilità	Interesting directory HTTP /...../ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/.
Output della vulnerabilità / Evidenze	
AttackString: GET /...../ HTTP/1.0	
AttackOutput: HTTP/1.1 200 OK	
Date: Tue, 19 Sep 2023 09:16:13 GMT	
Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT	
Etag: "5f2cbf8e.10699"	
Content-Type: text/html	
Content-Length: 10699	
Connection: close	
Accept-Ranges: bytes	
X-Content-Type-Options: nosniff	
X-Frame-Options: SAMEORIGIN	
x-xss-protection: 1	
mode=block	

```

<!DOCTYPE html>
<html>
<head>
<script>
/**
 * 防止浏览器缓存导致登录页的js文件加载失败
 * 如果url中没有参数则为url上加上一个随机数重新加载，需要过滤cloud方式登录
 * @return {[type]} [description]
 */
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(=) && -1 === href.indexOf(/?)){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&
quot; />
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /admin/ .
Output della vulnerabilità / Evidenze	
<pre> AttackString: GET ../../ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Tue, 19 Sep 2023 09:16:13 GMT Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT Etag: "5f2cbf8e.10699" Content-Type: text/html Content-Length: 10699 Connection: close Accept-Ranges: bytes X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN x-xss-protection: 1 mode=block <!DOCTYPE html> <html> <head> <script> /** * 防止浏览器缓存导致登录页的js文件加载失败 * 如果url中没有参数则为url上加上一个随机数重新加载，需要过滤cloud方式登录 * @return {[type]} [description] */ (function(){ var href = window.location.href var ran = Math.round(Math.random() * 1000000000000) if (-1 === href.indexOf(?)){ window.location.href = href + ?_ = + ran } else if (-1 === href.indexOf(=) && -1 === href.indexOf(/{ (/?)){ window.location.href = href + &_ = + ran } })() </script> <meta http-equiv="X-UA-Compatible" content="edge& quot; /> <meta http-equiv="Content-Type" content="text/html charset=utf-8" /> <meta content="favicon.ico" itemprop="image" /> <link rel="stylesheet" href="/style/plugins/jquery-ui .min_6389365.css" </pre>	

```

type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Vulnerabilità	Interesting directory HTTP /..%00/ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
Output della vulnerabilità / Evidenze	
AttackString: GET /..%00/ HTTP/1.0 AttackOutput: HTTP/1.1 200 OK Date: Tue, 19 Sep 2023 09:16:13 GMT Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT Etag: "5f2cbf8e.10699" Content-Type: text/html Content-Length: 10699 Connection: close Accept-Ranges: bytes X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN x-xss-protection: 1 mode=block <!DOCTYPE html> <html> <head> <script> /** * 防止浏览器缓存导致登录页的js文件加载失败	

```

* 如果url中没有参数则为url加上一个随机数重新加载，需要过滤cloud方式登录
* @return {[type]} [description]
*/
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(_=) && -1 === href.indexOf(/{?){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&
quot; />
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title&gt
;
</head>
<body id="login_body" class="login_min_height_width&q
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Vulnerabilità	Interesting directory HTTP /.%00 Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.

Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .
------------------	--

Output della vulnerabilità / Evidenze

```

AttackString: GET /..%00 HTTP/1.0
AttackOutput: HTTP/1.1 200 OK
Date: Tue, 19 Sep 2023 09:16:13 GMT
Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT
Etag: "5f2cbf8e.10699"
Content-Type: text/html
Content-Length: 10699
Connection: close
Accept-Ranges: bytes
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
x-xss-protection: 1
mode=block
<!DOCTYPE html>
<html>
<head>
<script>
/**
 * 防止浏览器缓存导致登录页的js文件加载失败
 * 如果url中没有参数则为url加上一个随机数重新加载，需要过滤cloud方式登录
 * @return {[type]} [description]
 */
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(=) && -1 === href.indexOf(/{))){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&
quot; />
<meta http-equiv="Content-Type" content="text/html
charset=utf-8" />
<meta content="favicon.ico" itemprop="image"
/>
<link rel="stylesheet" href="/style/plugins/jquery-ui
.min_6389365.css"
type="text/css" />
<link rel="stylesheet" href="/style/index_

```

Vulnerabilità	Interesting directory HTTP /%00/ Identified
----------------------	--


```

type="text/css" />
<link rel="stylesheet" href="/style/index_815c31a.css
" />
<link rel="stylesheet" href="style/color.css" />
;
<title data-text="Text.VideoManageSystem"></title>
;
</head>
<body id="login_body" class="login_min_height_width&
uot;>
<div class="pluginTip" id="pluginTip">
<div class="pluginVersionTip" id="pluginVersionT
ip" data-title="Text.TipDbClickClose3"></div>
</div>
<div class="login_fullPage login_min_height_width">
<div class="login_placeHolder">
<div class="login_minHeight"></div>
</div>
<div class="login_f

```

Vulnerabilità	Interesting directory HTTP /%00/interact.sh/ Identified
Livello rischio	Informazione
Porta	80/tcp, 30000/tcp
SPID	56003
Impatto	The Interesting directory HTTP has been found to be existing. This might need to be investigated. An attacker can use this information to guess more information about the system and properly base other attacks on.
Soluzione	It is recommended to rename the directories to names that are hard to guess. Example if a directory is called /admin/ call it /addmin/ .

Output della vulnerabilità / Evidenze

```

AttackString: GET /%00/interact.sh/ HTTP/1.0
AttackOutput: HTTP/1.1 200 OK
Date: Tue, 19 Sep 2023 09:16:09 GMT
Last-Modified: Fri, 07 Aug 2020 02:42:22 GMT
Etag: "5f2cbf8e.10699"
Content-Type: text/html
Content-Length: 10699
Connection: close
Accept-Ranges: bytes
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
x-xss-protection: 1
mode=block
<!DOCTYPE html>
<html>
<head>
<script>
/**
* 防止浏览器缓存导致登录页的js文件加载失败

```

```

* 如果url中没有参数则为url加上一个随机数重新加载，需要过滤cloud方式登录
* @return {[type]} [description]
*/
(function(){
var href = window.location.href
var ran = Math.round(Math.random() * 1000000000000)
if (-1 === href.indexOf(?)){
window.location.href = href + ?_ = + ran
} else if (-1 === href.indexOf(_=) && -1 === href.indexOf(/{?){
window.location.href = href + &_ = + ran
}
})();
</script>
<meta http-equiv="X-UA-Compatible" content="edge&quot; />
<meta http-equiv="Content-Type" content="text/html charset=utf-8" />
<meta content="favicon.ico" itemprop="image" />
<link rel="stylesheet" href="/style/plugins/jquery-ui.min_6389365.css" type="text/css" />
<link rel="stylesheet" href="/style/index_

```

Vulnerabilità	System time via remote Web Server
Livello rischio	Informazione
Porta	80/tcp, 82/tcp, 30000/tcp, 30001/tcp, 49152/tcp
SPID	1745
Impatto	It is possible to connect to the remote web server and issue a HEAD / HTTP/1.0 which revealed the system time on the target. Attackers can use this knowledge to bypass possible time-based intrusion detection. *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	Since this is a default option in most web servers, it has to be reconfigured without the Date function. Apache: It is very easy. First you have to RE compile apache from source. Before recompiling find the file /apache_x_x/src/main/http_protocol.c where x_x is version number. Now in that file locate the line ap_send_header_field(r, "Date", ap_gm_timestr_822(r->pool, r->request_time)) and UN Comment the line by setting a // in-front of the line. After that find the line ap_table_unset(r->headers_out, "Date") and put a // in-front of that line as well. Now recompile apache. IIS This is not directly possible here and has to be done on firewall level or by applying thrid party software. IIS WINDOWS This is an option that can be very hard to accomplish since this is not a default feature at the current time of the iis web server. So either block this at firewall level or put this in your security policy so that you are aware of it.
Output della vulnerabilità / Evidenze	
	AttackString: HEAD / HTTP/1.0
	AttackOutput: Tue, 19 Sep 2023 09:07:41 GMT

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.29: icmp_seq=0 ttl=64 time=0.9 ms

Vulnerabilità	Direct HTTP 784276 & HTTPS 0 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

FRED FOR SECURITY DEMO

Sistema Target: 192.168.0.30

Vulnerabilità	SSH Service Accessible
Livello rischio	Alto
Porta	22/tcp
SPID	2733
Impatto	The SSH service allows anyone to connect to it. This is a security risk because an attacker can issue a brute force attack and the service has a history of many dangerous vulnerabilities.
Soluzione	It is recommended to only allow trusted users to connect to it.
Output della vulnerabilità / Evidenze	
AttackOutput: SSH-2.0-Mocana SSH 6.3	

Vulnerabilità	Target ip address system reverses traffic
Livello rischio	Medio
SPID	3685
Impatto	The target system reverses a source route when responding to a source routed packet. This can allow an attacker to spoof a packet as coming from a trusted IP address that just happens to be source routed through an IP address that the attacker can sniff on. The victim ip address would then send return traffic to the spoofed source.
Soluzione	It is recommended to reconfigure the network device you have running on the target system and set the sourceroute option to zero

Vulnerabilità	Telnet Service
Livello rischio	Medio
Porta	23/tcp
SPID	29
CVE	CVE-1999-0619
CVSS	
Impatto	The telnet service has been found on TCP port 23. This service is used for remote administration. Telnet sends all usernames,passwords and data unencrypted.
Soluzione	UNIX: Disable the Telnet service by uncommenting the telnet line in /etc/inetd.conf on UNIX systems. WINDOWS: Systems enter Control-Panel->Administrative Tools->Services and put the telnet service on Disable. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.	

Vulnerabilità	HTTP only port without SSL found
---------------	----------------------------------

Livello rischio	Basso
Porta	80/tcp, 1513/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.30:80/tcp matches http

Vulnerabilità	SNMP service detected on udp
Livello rischio	Basso
Porta	161/udp
SPID	2295
Impatto	The snmp service has been detected. It is normally used to control routers and to get information from routers and other network equipment. It is known to have contained several vulnerabilities in the past.
Soluzione	It is recommended to either disable the snmp service or block incoming traffic to the identified port. If you NEED this service make sure that ONLY trusted ips are allowed to connect to it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	All Protocols Tested
Livello rischio	Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.30:22/tcp matches ssh
	Protocol on 192.168.0.30:23/tcp matches telnet
	Protocol on 192.168.0.30:80/tcp matches http
	Protocol on 192.168.0.30:1506/tcp matches telnet
	Protocol on 192.168.0.30:1513/tcp matches http

Vulnerabilità	MAC Address 20-67-7c-9f-33-80 Hewlett Packard Enterprise
Livello rischio	Informazione
SPID	12167

Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: 20-67-7c-9f-33-80 Hewlett Packard Enterprise

Vulnerabilità	Remote system answers to PING command
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.30: icmp_seq=0 ttl=255 time=0.9 ms

Vulnerabilità	Identified Operating System Windows XP via Packet Check #3
Livello rischio	☐ ☐ ☐ ☒ Informazione
Porta	1513/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Windows XP

Vulnerabilità	Direct HTTP 5805 & HTTPS 0 Connections
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

Sistema Target: 192.168.0.34

Vulnerabilità	SSH Service Accessible
Livello rischio	Alto
Porta	22/tcp
SPID	2733
Impatto	The SSH service allows anyone to connect to it. This is a security risk because an attacker can issue a brute force attack and the service has a history of many dangerous vulnerabilities.
Soluzione	It is recommended to only allow trusted users to connect to it.
Output della vulnerabilità / Evidenze	
	AttackOutput: SSH-2.0-dropbear

Vulnerabilità	DNS Recursion Allowed
Livello rischio	Medio
SPID	56963
Impatto	The target DNS service is subject to a remote DNS Recursion vulnerability. Attackers can exploit this in DDoS Attacks. Recursion is used to process a DNS request where the DNS server performs the request for the client. Recursion should only be allowed for trusted clients.
Soluzione	Set permissions so only trusted clients can do recursion requests or disable recursion. On Unix* You can edit /etc/bind/named.conf. allow-transfer {"none"} allow-recursion {"none"} recursion no On Windows please see: http://technet.microsoft.com/en-us/library/cc771738.aspx
Output della vulnerabilità / Evidenze	
	yahoo.com mail is handled by 1 mta7.am0.yahoodns.net.

Vulnerabilità	8081 Port Identification
Livello rischio	Medio
Porta	8081/tcp
SPID	58833
Impatto	The target service found running is subject to an information vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the target system with the same permissions as the identified daemon.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found software. And it is recommended to set firewall permissions so only trusted users can connect to the found IP address. Note if you are running another service on this port you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	HTTP only port without SSL found
---------------	----------------------------------

Livello rischio	Basso
Porta	8083/tcp, 8084/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.34:8083/tcp matches http

Vulnerabilità	ASP.NET path disclosure
Livello rischio	Basso
Porta	8083/tcp, 8084/tcp
SPID	2190
Impatto	The remote ASP.NET system is vulnerable to a path disclosure vulnerability. An attacker can use this information to base other attacks on.
Soluzione	Please upgrade to the latest version of the ASP.NET service from http://www.asp.net/download.aspx
Output della vulnerabilità / Evidenze	
	AttackString: GET /a%5c.aspx HTTP/1.0
	AttackOutput: HTTP/1.0 500 Internal Server Error
	Connection: close

Vulnerabilità	Possible Service/Game: directtv Identified
Livello rischio	Basso
Porta	8082/tcp
SPID	61358
Impatto	The identified port found open on the target system is subject to a remote attack factor. An attacker can exploit this vulnerability to crash the target program or base other attacks on it.
Soluzione	Please upgrade to the latest version of the program. It is recommended to firewall off the port. If it is already secure and updated to the latest version you can ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Identified Operating System Check #2 Microsoft Windows via Banner
Livello rischio	Informazione
Porta	53/udp
SPID	58296
Impatto	Via the identified banner on the found service port it reveals sensitive information about which Operating System Check is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.

Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	
	Microsoft DNS 6.1.7601 (1DB15F75)

Vulnerabilità	All Protocols Tested
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	8311
Impatto	This check probes all ports for their real protocols. If all matches as it should be please ignore this check.
Soluzione	If there is found known services on unknown ports it is recommended to properly test those ports.
Output della vulnerabilità / Evidenze	
	Protocol on 192.168.0.34:22/tcp matches ssh
	Protocol on 192.168.0.34:80/tcp matches http
	Protocol on 192.168.0.34:8081/tcp matches http
	Protocol on 192.168.0.34:8082/tcp matches http
	Protocol on 192.168.0.34:8083/tcp matches http
	Protocol on 192.168.0.34:8084/tcp matches http

Vulnerabilità	System Time Revealed via. ICMP TimeStamp Request
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is identified. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level.
Output della vulnerabilità / Evidenze	
	AttackOutput: 11:41:26

Vulnerabilità	MAC Address ac-86-74-6f-8f-c0 Open Mesh, Inc.
Livello rischio	☐ ☐ ☐ ☒ Informazione
SPID	12167
Impatto	In this check we are guessing the type of system device by tracing the MAC address of the network interface card. This can reveal sensitive information such as firewall manufacturers or other details. An attacker can use this data to base other attacks on. A MAC Address is a 24 bit Organizationally Unique Identifier (OUI). Please note the MAC Address can easily be spoofed on a device.
Soluzione	It is recommended to have a firewall device up in front of your servers that will give a fake identification of your network card. If you have already done this you can ignore this check.

Output della vulnerabilità / Evidenze	
	AttackOutput: ac-86-74-6f-8f-c0 Open Mesh, Inc.

Vulnerabilità	System Time Revealed ICMP TimeStamp
Livello rischio	Informazione
SPID	1746
CVE	CVE-1999-0524
CVSS	CVE-1999-0524 - CVSS Score V2: 2.1
Impatto	By sending an ICMP TIMESTAMP REQUEST packet (ICMP type 13), the system time of the target host is ascertained to be. Information such as this can be used in extreme cases to bypass time-based Intrusion Detection Systems (IDS). *NOTE* This vulnerability can be ignored because it is a Low risk and if it is very difficult in your setup to change the required settings to block the timestamp requests.
Soluzione	At network-level this traffic should be rejected both inbound and outbound. UNIX: ICMP type 13 packets should be dropped inbound, and ICMP type 14 packets should be dropped outbound. Other ICMP packet types can be allowed into and out of your network space, and it is recommended that these are assessed and filtered accordingly. WINDOWS: This can be a hard option to set at the current time and it is therefor recommended to apply at firewall level. On a Cisco device it can be blocked by setting the rules access-list 101 deny icmp any any 13 ! timestamp request.
Output della vulnerabilità / Evidenze	
	10:41:26

Vulnerabilità	Remote system answers to PING command
Livello rischio	Informazione
SPID	2853
Impatto	The remote system answers to the PING command. The PING command is used to see if a system is "Alive" on the Internet. By this an attacker can easily determine if the system is running to the INTERNET and base other attacks on this.
Soluzione	It is recommended to block at firewall level so that the system do not respond to PING queries. By "Cloaking" the system to the INTERNET unskilled attackers can think there is no system on the IP address and simple move on the next IP address. This can be blocked by Block incoming icmp-type 13 and block outgoing icmp-type 14 .
Output della vulnerabilità / Evidenze	
	64 octets from 192.168.0.34: icmp_seq=0 ttl=64 time=0.6 ms

Vulnerabilità	Identified Operating System Linux 2.2.x-3.x via Packet Check #3
Livello rischio	Informazione
Porta	8084/tcp
SPID	58
Impatto	This can also identify wrong example if a Windows based system running but identified as Linux it can be because a Linux based firewall is running in front. Via the identified banner on the found service port it reveals sensitive information about which operating system is running. This is very dangerous since attackers can base other attacks on this information. It can even reveal if the operating system is end of life and wide open to attacks and wont be patched.
Soluzione	It is recommended to clean the identified version banner so it reveals as less information as possible.
Output della vulnerabilità / Evidenze	

Linux 2.2.x-3.x

Vulnerabilità	Direct HTTP 335610 & HTTPS 0 Connections
Livello rischio	Informazione
SPID	6175
Impatto	The Penetrator uses different techniques for connection. Here is the list of Direct HTTP and HTTPS Connections without the counting from crawlers and external tools.
Soluzione	Information check only

FRED FOR SECURITY DEMO

Sistema Target: 192.168.0.37

Vulnerabilità NetBIOS service listening 445 TCP Possible Vulnerable Remote Exploits	
Livello rischio	Alto
Porta	445/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening. There has been known exploits like WannaCry on this port and it is recommended to firewall of the port and only allow trusted users to connect to it.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. Further more to stop the listening on TCP and UDP port 445 in Regedit please goto: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters And in the TransportBindName remove the "\Device\" value. It can also be done by opening the Network and Dial-Up Connections applet and there select Advanced and Advanced Settings. There deselecting File And Printer Sharing for Microsoft Networks. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità Missing Web Security Header Tag Strict-Transport-Security	
Livello rischio	Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58665
Impatto	The HTTP Web Security Header Strict Transport Security is a recommended feature to increase the security on your website and strengthens your implementation of TLS by forcing the User Agent to use HTTPS. It is often know as HSTS that forces the web site to make the web browsers know it should be accessed only by using HTTPS instead of the insecure HTTP.
Soluzione	Fix by adding to your site: header("Strict-Transport-Security: max-age=31536000 includeSubDomains")
Output della vulnerabilità / Evidenze	

Vulnerabilità DeleGate Web Server Denial of Service	
---	--

Livello rischio	Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	7770
Impatto	The identified web server found running on the target system is subject to a remote Denial of Service vulnerability. An attacker can exploit this vulnerability to crash the target service.
Soluzione	Please upgrade to the latest version from http://www.delegate.org/
Output della vulnerabilità / Evidenze	
	Please note in this check it only relied on the HTTP Version check. So if you have a vulnerable version with custom patches you might look away from this check.
	k. AttackString: HEAD / HTTP/1.0
	AttackOutput: HTTP/1.1 200 OK
	Date: Tue, 19 Sep 2023 13:43:56 GMT
	Server: Apache
	X-Frame-Options: SAMEORIGIN
	Set-Cookie: Session=192.168.0.51.0ad8222a66945356ffba78bc8b7ebe12
	path=/
	Set-Cookie: Locale=en-US
	path=/
	Cache-Control: no-cache,no-store,must-revalidate
	Accept-Ranges: bytes
	Content-Length: 4564
	Pragma: no-cache
	X-XSS-Protection: 1
	mode=block
	X-Frame-Options: SAMEORIGIN
	Connection: close
	Content-Type: text/html
	charset=UTF-8

Vulnerabilità	vsftpd DoS
Livello rischio	Medio
Porta	21/tcp
SPID	48948
CVE	CVE-2011-0762
CVE	CVE-2010-2632
CVSS	CVE-2011-0762 - CVSS Score V2: 4
CVSS	CVE-2010-2632 - CVSS Score V2: 7.8
USN	1098-1
Impatto	The identified FTP server found running is subject to a remote Denial of Service vulnerability. An attacker can exploit this vulnerability to crash the ftp server.
Soluzione	Please upgrade to the latest version of the identified ftp server.
Output della vulnerabilità / Evidenze	
	AttackOutput: 220 (vsFTPd 2.2.2)

Vulnerabilità	VMware ESXI / Possible Novell Client running Port 427 TCP
----------------------	--

Livello rischio	Medio
Porta	427/tcp
SPID	40
Impatto	tcp port 427 is known to be the port of Novell Client. Versions 3.0 and 3.01 of the Novell client are known to be vulnerable to Denial of Service attacks.
Soluzione	If you are running the vulnerable client Please upgrade to the latest from http://download.novell.com/ NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Missing Web Security Header Tag Permissions-Policy
Livello rischio	Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58860
Impatto	The Permissions-Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: <code>header("Permissions-Policy: accelerometer=(), camera=(), document-domain=(), encrypted-media=(), geolocation=(), gyroscope=(), magnetometer=(), midi=(), payment=(), publickey-credentials-get=(), usb=(), xr-spatial-tracking=(), fullscreen=(self), autoplay=(self), microphone=(self), picture-in-picture=(), sync-xhr=(self)")</code>
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Content-Security-Policy
Livello rischio	Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58667
Impatto	The Content Security Policy Security Header can help secure your website from XSS attacks. Whitelist sources of approved content you can this way prevent the browser from loading malicious content. The Security Header allows website security administrator to control resources the user agent can be allowed to load on a given page. This can help protect against Cross Site Scripting attacks XSS.
Soluzione	Fix by adding to your site: <code>header("Content-Security-Policy: block-all-mixed-content script-src 'self' www.youriste.com ")</code>
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag Referrer-Policy
Livello rischio	Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58666

Impatto	The Referrer Policy is a newer security header that allows a website to control the amount of information the web browser is sending with navigation away from a document. It is recommended and should be set by all sites. The header protects which referrer information sent in Referer requests made.
Soluzione	Fix by adding to your site: header("Referrer-Policy: no-referrer,strict-origin-when-cross-origin")
Output della vulnerabilità / Evidenze	

Vulnerabilità	Missing Web Security Header Tag X-Content-Type-Options
Livello rischio	 Medio
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58664
Impatto	X-Content-Type-Options Security Header is used to prevent a browser from trying to MIME sniff the sensitive content type & forces the browser to use the declared content-type. The HTTP Security header is used by the server to indicate the MIME types advertised in the Content-Type headers to not be changed. This can prevent MIME type sniffing. The header was first introduced by Microsoft in Internet Explorer IE 8 to allow webmasters block content sniffing that could transform non-executable MIME types into executable MIME type. Other web browsers have introduced it as well. It is recommended by penetration testing process to expect this header to be set. The only valid value you can set for this header is nosniff.
Soluzione	Fix by adding to your site: header("X-Content-Type-Options: nosniff")
Output della vulnerabilità / Evidenze	

Vulnerabilità	NetBIOS User Name Retrieval #1
Livello rischio	 Medio
SPID	1772
Impatto	It is possible to query NetBIOS Windows file sharing services running on The identified TCP port to gain a list of and other NetBIOS information. Determined attackers can use this information to launch effective brute-force attacks against shared resources.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via the identified TCP port. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
AttackOutput: : 28 > 24	

Vulnerabilità	Open Netbios Shares Without Username and Password
Livello rischio	 Medio
Porta	139/tcp
SPID	58209
Impatto	Anyone could access, list or even modify files in open non-protected shares. This can lead to leak of sensitive information.

Soluzione

RECOMMENDED SOLUTION: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use.

If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken -

Click through Start-> Settings-> Network and Dial-up Connection

Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.

Output della vulnerabilità / Evidenze

Sharename	Type	Comment
-----	-----	-----
FILE_SHARE	Disk	
PS3_driver	Disk	
UNIV_driver	Disk	
XPS_driver	Disk	
IPC\$	IPC	IPC Service (SMB Server)
Server	Comment	
-----	-----	-----
MFP12172073	SMB Server	
Workgroup	Master	
-----	-----	-----
WORKGROUP	LAPTOP-0CIKA39T	
found		
PS3_driver		
. DH 0	Mon Sep 18 17:38:06 2023	
.. DH 0	Thu Mar 22 23:11:03 2018	
eSPDPS.msi	AH 1725952 Mon Oct 23 14:11:56 2017	
0x0407.ini	AH 24670 Thu Apr 14 13:10:34 2011	
0x0411.ini	AH 14350 Thu Apr 14 13:10:34 2011	
0x0404.ini	AH 10258 Thu Apr 14 13:10:34 2011	
0x040a.ini	AH 24024 Thu Apr 14 13:10:34 2011	
1034.mst	AH 196608 Tue Sep 5 15:00:48 2017	
0x0406.ini	AH 22770 Thu Apr 14 13:10:34 2011	
0x0804.ini	AH 10324 Thu Apr 14 13:10:34 2011	
1053.mst	AH 143360 Tue Sep 5 15:00:48 2017	
1055.mst	AH 102400 Tue Sep 5 15:00:48 2017	
Discover	DH 0 Thu Mar 22 23:11:00 2018	
1045.mst	AH 151552 Tue Sep 5 15:00:48 2017	
1035.mst	AH 147456 Tue Sep 5 15:00:48 2017	
0x041d.ini	AH 22224 Thu Apr 14 13:10:34 2011	
1040.mst	AH 155648 Tue Sep 5 15:00:48 2017	
0x0414.ini	AH 22816 Thu Apr 14 13:10:34 2011	
0x0415.ini	AH 23108 Thu Apr 14 13:10:34 2011	
32bit	DH 0 Thu Mar 22 23:10:59 2018	
1049.mst	AH 147456 Tue Sep 5 15:00:48 2017	
1044.mst	AH 143360 Tue Sep 5 15:00:48 2017	
0x040c.ini	AH 24944 Thu Apr 14 13:10:34 2011	
STRINGS	DH 0 Mon Oct 23 12:42:10 2017	
0x040b.ini	AH 21602 Thu Apr 14 13:10:34 2011	

```

1028.mst AH 122880 Tue Sep 5 15:00:48 2017
Setup.ini AH 5290 Mon Oct 23 12:42:08 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017
0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017
essetup.exe A 1646048 Mon Oct 23 14:10:42 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
eSPDPS.exe AH 370176 Tue Sep 5 15:18:22 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:00 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
eSPDPS.cfg H 228 Mon Sep 18 17:38:06 2023
64bit DH 0 Thu Mar 22 23:10:59 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available
found
FILE_SHARE
. D 0 Thu Mar 22 22:02:44 2018
.. D 0 Mon Feb 1 09:06:58 2021
123804964 blocks of size 1024. 117431880 blocks available
found
XPS_driver
. DH 0 Mon Sep 18 17:38:06 2023
.. DH 0 Thu Mar 22 23:11:03 2018
0x0407.ini AH 24670 Thu Apr 14 13:10:34 2011
0x0411.ini AH 14350 Thu Apr 14 13:10:34 2011
0x0404.ini AH 10258 Thu Apr 14 13:10:34 2011
0x040a.ini AH 24024 Thu Apr 14 13:10:34 2011
1034.mst AH 196608 Tue Sep 5 15:00:48 2017
0x0406.ini AH 22770 Thu Apr 14 13:10:34 2011
0x0804.ini AH 10324 Thu Apr 14 13:10:34 2011
1053.mst AH 143360 Tue Sep 5 15:00:48 2017
1055.mst AH 102400 Tue Sep 5 15:00:48 2017
Discover DH 0 Thu Mar 22 23:11:06 2018
1045.mst AH 151552 Tue Sep 5 15:00:48 2017
1035.mst AH 147456 Tue Sep 5 15:00:48 2017
0x041d.ini AH 22224 Thu Apr 14 13:10:34 2011
1040.mst AH 155648 Tue Sep 5 15:00:48 2017
0x0414.ini AH 22816 Thu Apr 14 13:10:34 2011
0x0415.ini AH 23108 Thu Apr 14 13:10:34 2011
32bit DH 0 Thu Mar 22 23:11:05 2018

```

```

eSPDXPS.cfg H 228 Mon Sep 18 17:38:06 2023
1049.mst AH 147456 Tue Sep 5 15:00:48 2017
1044.mst AH 143360 Tue Sep 5 15:00:48 2017
0x040c.ini AH 24944 Thu Apr 14 13:10:34 2011
STRINGS DH 0 Mon Oct 23 12:42:10 2017
0x040b.ini AH 21602 Thu Apr 14 13:10:34 2011
1028.mst AH 122880 Tue Sep 5 15:00:48 2017
Setup.ini AH 5296 Mon Oct 23 12:42:10 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017
0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
eSPDXPS.msi AH 1725952 Mon Oct 23 14:12:06 2017
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017
esetup.exe A 1646048 Mon Oct 23 14:10:48 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:06 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
64bit DH 0 Thu Mar 22 23:11:06 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
eSPDXPS.exe AH 370176 Tue Sep 5 15:18:22 2017
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available
found
UNIV_driver
. DH 0 Mon Sep 18 17:38:07 2023
.. DH 0 Thu Mar 22 23:11:03 2018
0x0407.ini AH 24670 Thu Apr 14 13:10:34 2011
0x0411.ini AH 14350 Thu Apr 14 13:10:34 2011
0x0404.ini AH 10258 Thu Apr 14 13:10:34 2011
0x040a.ini AH 24024 Thu Apr 14 13:10:34 2011
1034.mst AH 196608 Tue Sep 5 15:00:48 2017
0x0406.ini AH 22770 Thu Apr 14 13:10:34 2011
0x0804.ini AH 10324 Thu Apr 14 13:10:34 2011
1053.mst AH 143360 Tue Sep 5 15:00:48 2017
1055.mst AH 102400 Tue Sep 5 15:00:48 2017
Discover DH 0 Thu Mar 22 23:11:03 2018
1045.mst AH 151552 Tue Sep 5 15:00:48 2017
1035.mst AH 147456 Tue Sep 5 15:00:48 2017
0x041d.ini AH 22224 Thu Apr 14 13:10:34 2011
1040.mst AH 155648 Tue Sep 5 15:00:48 2017
eSPDUNI.cfg H 229 Mon Sep 18 17:38:07 2023
eSPDUNI.exe AH 370176 Tue Sep 5 15:18:22 2017

```

```

0x0414.ini AH 22816 Thu Apr 14 13:10:34 2011
0x0415.ini AH 23108 Thu Apr 14 13:10:34 2011
eSPDUNI.msi AH 1725952 Mon Oct 23 14:11:40 2017
32bit DH 0 Thu Mar 22 23:11:02 2018
1049.mst AH 147456 Tue Sep 5 15:00:48 2017
1044.mst AH 143360 Tue Sep 5 15:00:48 2017
0x040c.ini AH 24944 Thu Apr 14 13:10:34 2011
STRINGS DH 0 Mon Oct 23 12:42:08 2017
0x040b.ini AH 21602 Thu Apr 14 13:10:34 2011
1028.mst AH 122880 Tue Sep 5 15:00:48 2017
Setup.ini AH 5308 Mon Oct 23 12:42:08 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017
0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017
essetup.exe A 1646048 Mon Oct 23 14:10:38 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:03 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
64bit DH 0 Thu Mar 22 23:11:03 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available

```

Vulnerabilità	Open Netbios Shares
Livello rischio	Medio
Porta	139/tcp
SPID	47039
Impatto	Anyone could access, list or even modify files in open non-protected shares. This can lead to leak of sensitive information.
Soluzione	RECOMMENDED SOLUTION: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	Sharename Type Comment

```

-----
FILE_SHARE Disk
PS3_driver Disk
UNIV_driver Disk
XPS_driver Disk
IPC$ IPC IPC Service (SMB Server)
Server Comment
-----
MFP12172073 SMB Server
Workgroup Master
-----
WORKGROUP LAPTOP-0CIKA39T
found
PS3_driver
. DH 0 Mon Sep 18 17:38:06 2023
.. DH 0 Thu Mar 22 23:11:03 2018
eSPDPS.msi AH 1725952 Mon Oct 23 14:11:56 2017
0x0407.ini AH 24670 Thu Apr 14 13:10:34 2011
0x0411.ini AH 14350 Thu Apr 14 13:10:34 2011
0x0404.ini AH 10258 Thu Apr 14 13:10:34 2011
0x040a.ini AH 24024 Thu Apr 14 13:10:34 2011
1034.mst AH 196608 Tue Sep 5 15:00:48 2017
0x0406.ini AH 22770 Thu Apr 14 13:10:34 2011
0x0804.ini AH 10324 Thu Apr 14 13:10:34 2011
1053.mst AH 143360 Tue Sep 5 15:00:48 2017
1055.mst AH 102400 Tue Sep 5 15:00:48 2017
Discover DH 0 Thu Mar 22 23:11:00 2018
1045.mst AH 151552 Tue Sep 5 15:00:48 2017
1035.mst AH 147456 Tue Sep 5 15:00:48 2017
0x041d.ini AH 22224 Thu Apr 14 13:10:34 2011
1040.mst AH 155648 Tue Sep 5 15:00:48 2017
0x0414.ini AH 22816 Thu Apr 14 13:10:34 2011
0x0415.ini AH 23108 Thu Apr 14 13:10:34 2011
32bit DH 0 Thu Mar 22 23:10:59 2018
1049.mst AH 147456 Tue Sep 5 15:00:48 2017
1044.mst AH 143360 Tue Sep 5 15:00:48 2017
0x040c.ini AH 24944 Thu Apr 14 13:10:34 2011
STRINGS DH 0 Mon Oct 23 12:42:10 2017
0x040b.ini AH 21602 Thu Apr 14 13:10:34 2011
1028.mst AH 122880 Tue Sep 5 15:00:48 2017
Setup.ini AH 5290 Mon Oct 23 12:42:08 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017
0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017

```

```

essetup.exe A 1646048 Mon Oct 23 14:10:42 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
eSPDPS.exe AH 370176 Tue Sep 5 15:18:22 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:00 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
eSPDPS.cfg H 228 Mon Sep 18 17:38:06 2023
64bit DH 0 Thu Mar 22 23:10:59 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available
found
FILE_SHARE
. D 0 Thu Mar 22 22:02:44 2018
.. D 0 Mon Feb 1 09:06:58 2021
123804964 blocks of size 1024. 117431880 blocks available
found
XPS_driver
. DH 0 Mon Sep 18 17:38:06 2023
.. DH 0 Thu Mar 22 23:11:03 2018
0x0407.ini AH 24670 Thu Apr 14 13:10:34 2011
0x0411.ini AH 14350 Thu Apr 14 13:10:34 2011
0x0404.ini AH 10258 Thu Apr 14 13:10:34 2011
0x040a.ini AH 24024 Thu Apr 14 13:10:34 2011
1034.mst AH 196608 Tue Sep 5 15:00:48 2017
0x0406.ini AH 22770 Thu Apr 14 13:10:34 2011
0x0804.ini AH 10324 Thu Apr 14 13:10:34 2011
1053.mst AH 143360 Tue Sep 5 15:00:48 2017
1055.mst AH 102400 Tue Sep 5 15:00:48 2017
Discover DH 0 Thu Mar 22 23:11:06 2018
1045.mst AH 151552 Tue Sep 5 15:00:48 2017
1035.mst AH 147456 Tue Sep 5 15:00:48 2017
0x041d.ini AH 22224 Thu Apr 14 13:10:34 2011
1040.mst AH 155648 Tue Sep 5 15:00:48 2017
0x0414.ini AH 22816 Thu Apr 14 13:10:34 2011
0x0415.ini AH 23108 Thu Apr 14 13:10:34 2011
32bit DH 0 Thu Mar 22 23:11:05 2018
eSPDXPS.cfg H 228 Mon Sep 18 17:38:06 2023
1049.mst AH 147456 Tue Sep 5 15:00:48 2017
1044.mst AH 143360 Tue Sep 5 15:00:48 2017
0x040c.ini AH 24944 Thu Apr 14 13:10:34 2011
STRINGS DH 0 Mon Oct 23 12:42:10 2017
0x040b.ini AH 21602 Thu Apr 14 13:10:34 2011
1028.mst AH 122880 Tue Sep 5 15:00:48 2017
Setup.ini AH 5296 Mon Oct 23 12:42:10 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017

```

```

0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
eSPDXPS.msi AH 1725952 Mon Oct 23 14:12:06 2017
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017
esetup.exe A 1646048 Mon Oct 23 14:10:48 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:06 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
64bit DH 0 Thu Mar 22 23:11:06 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
eSPDXPS.exe AH 370176 Tue Sep 5 15:18:22 2017
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available
found
UNIV_driver
. DH 0 Mon Sep 18 17:38:07 2023
.. DH 0 Thu Mar 22 23:11:03 2018
0x0407.ini AH 24670 Thu Apr 14 13:10:34 2011
0x0411.ini AH 14350 Thu Apr 14 13:10:34 2011
0x0404.ini AH 10258 Thu Apr 14 13:10:34 2011
0x040a.ini AH 24024 Thu Apr 14 13:10:34 2011
1034.mst AH 196608 Tue Sep 5 15:00:48 2017
0x0406.ini AH 22770 Thu Apr 14 13:10:34 2011
0x0804.ini AH 10324 Thu Apr 14 13:10:34 2011
1053.mst AH 143360 Tue Sep 5 15:00:48 2017
1055.mst AH 102400 Tue Sep 5 15:00:48 2017
Discover DH 0 Thu Mar 22 23:11:03 2018
1045.mst AH 151552 Tue Sep 5 15:00:48 2017
1035.mst AH 147456 Tue Sep 5 15:00:48 2017
0x041d.ini AH 22224 Thu Apr 14 13:10:34 2011
1040.mst AH 155648 Tue Sep 5 15:00:48 2017
eSPDUNI.cfg H 229 Mon Sep 18 17:38:07 2023
eSPDUNI.exe AH 370176 Tue Sep 5 15:18:22 2017
0x0414.ini AH 22816 Thu Apr 14 13:10:34 2011
0x0415.ini AH 23108 Thu Apr 14 13:10:34 2011
eSPDUNI.msi AH 1725952 Mon Oct 23 14:11:40 2017
32bit DH 0 Thu Mar 22 23:11:02 2018
1049.mst AH 147456 Tue Sep 5 15:00:48 2017
1044.mst AH 143360 Tue Sep 5 15:00:48 2017
0x040c.ini AH 24944 Thu Apr 14 13:10:34 2011
STRINGS DH 0 Mon Oct 23 12:42:08 2017
0x040b.ini AH 21602 Thu Apr 14 13:10:34 2011
1028.mst AH 122880 Tue Sep 5 15:00:48 2017

```

```

Setup.ini AH 5308 Mon Oct 23 12:42:08 2017
0x0410.ini AH 23754 Thu Apr 14 13:10:34 2011
1043.mst AH 151552 Tue Sep 5 15:00:48 2017
0x041f.ini AH 21928 Fri Jul 27 02:35:10 2012
1036.mst AH 196608 Tue Sep 5 15:00:48 2017
1031.mst AH 159744 Tue Sep 5 15:00:48 2017
0x0419.ini AH 22256 Thu Apr 14 13:10:34 2011
1030.mst AH 147456 Tue Sep 5 15:00:48 2017
1033.mst AH 20480 Tue Sep 5 15:00:48 2017
essetup.exe A 1646048 Mon Oct 23 14:10:38 2017
eSf3fw.dll AH 4412928 Tue Sep 5 15:18:20 2017
0x0416.ini AH 22964 Tue Jun 18 11:15:18 2013
Readme DH 0 Thu Mar 22 23:11:03 2018
0x0409.ini AH 21440 Thu Apr 14 13:10:34 2011
1046.mst AH 102400 Tue Sep 5 15:00:48 2017
64bit DH 0 Thu Mar 22 23:11:03 2018
0x0413.ini AH 23734 Thu Apr 14 13:10:34 2011
2052.mst AH 184320 Tue Sep 5 15:00:48 2017
1041.mst AH 278528 Tue Sep 5 15:00:48 2017
25671196 blocks of size 1024. 23474196 blocks available

```

Vulnerabilità	Sendmail Man in the Middle Attacks
Livello rischio	Medio
Porta	25/tcp
SPID	43141
Impatto	The identified Sendmail mail server found running is subject to a remote Man in the Middle attack vulnerability. An attacker can exploit this vulnerability to do man in the middle attacks on the target system with the same privileges as the Sendmail Program. This can lead to a system compromise.
Soluzione	Please upgrade to the latest version of Sendmail from http://www.sendmail.org or use your *NIX distribution package system.
Output della vulnerabilità / Evidenze	
AttackOutput: 220 192.168.0.37 ESMTP Sendmail 8.14.3/8.14.3 Tue, 19 Sep 2023 16:18:42 +0200	

Vulnerabilità	List of Netbios service lists installed
Livello rischio	Basso
SPID	2616
Impatto	It is possible on the remote system via the NetBIOS service to retrieve a list of installed servicelist patches on the system. An attacker can use this information to base other attacks on.
Soluzione	It is recommended to block incoming traffic to the NetBIOS service running on the UDP ports 135,136,137,139,445 TCP ports 135,136,137,139,445
Output della vulnerabilità / Evidenze	
servicelist List: Server: \\192.168.0.37: User: Domain: Connection: OK Services ----- Spooler: Print Spooler	

NETLOGON: Net Logon
RemoteRegistry: Remote Registry Service
WINS: Windows Internet Name Service (WINS)
Exit Status: SUCCESS

Vulnerabilità	HTTP only port without SSL found
Livello rischio	☐ ☒ ☐ Basso
Porta	80/tcp, 8080/tcp, 20080/tcp
SPID	58373
Impatto	The identified Web server port found open does not support SSL encryption. This is high security risk to have a http port open without forced ssl support. It can allow attackers to obtain sensitive information.
Soluzione	It is recommended to firewall off the identified port so only local users can connect to it and only allow http with ssl to be open. If you have redirected the port to example port 443 with SSL you can ignore this check.
Output della vulnerabilità / Evidenze	
	AttackOutput: Protocol on 192.168.0.37:80/tcp matches http-apache-2

Vulnerabilità	NetBIOS service listening 137 UDP
Livello rischio	☐ ☒ ☐ Basso
Porta	137/udp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	MAC address obtained via NetBIOS
Livello rischio	☐ ☒ ☐ Basso
SPID	1771

Impatto	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the physical address on the netcard. An attacker can use this number to spoof on the attackers own netcard and do hacks which will look like to be done with your netcard.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	MAC Address: 00-00-00-00-00-00

Vulnerabilità	It is possible to obtain remote NetBIOS name table
Livello rischio	☐ ☐ ☒ Basso
SPID	1770
Impatto	Attackers can use this information to base other attacks on.
Soluzione	Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135, 137, 138, 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet though a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP.
Output della vulnerabilità / Evidenze	
	<pre>Name Service Type ----- MFP12172073 Workstation Service MFP12172073 Messenger Service MFP12172073 File Server Service WORKGROUP Domain Name WORKGROUP Browser Service Elections</pre>

Vulnerabilità	HP Laserjet or brand Printer Identified
Livello rischio	☐ ☐ ☒ Basso
Porta	9100/tcp
SPID	2470
Impatto	The identified port found is known to host the HP Laserjet Service. It is subject to several Denial of Service vulnerabilities where it is possible for a remote attacker to crash the printer. Further vulnerabilities where it is possible for the attacker to change the text in the physical display on the printer can lead to social engineering attacks.

Soluzione	Please filter incoming traffic to the identified port. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	NetBIOS service listening 139 TCP
Livello rischio	☐ ☐ ☒ Basso
Porta	139/tcp
SPID	1990
Impatto	The identified port running is known to contain the NetBIOS service. It is known to contain several vulnerabilities and it is highly recommended not to have this service listening.
Soluzione	WINDOWS: Network filtering (through firewalling or host-based security settings) should be improved so that NetBIOS resources are not accessible from the Internet via. TCP ports 135 137 138 139 & 445. If you do require to allow NetBIOS services to be accessible, it is recommended that all shares of entire drives such as C: and D: do not exist, and that strong user passwords and authentication mechanisms are in use. If you wish to disable NetBIOS over TCP/IP locally - such as if you are connecting to the Internet through a dial-up connection, the following steps should be taken - Click through Start-> Settings-> Network and Dial-up Connection Right click on Local Area Connection -> Properties choose Internet Protocol (TCP/IP) -> Properties -> Advanced and WINS -> Disable NetBIOS over TCP/IP. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	SNMP service detected on udp
Livello rischio	☐ ☐ ☒ Basso
Porta	161/udp
SPID	2295
Impatto	The snmp service has been detected. It is normally used to control routers and to get information from routers and other network equipment. It is known to have contained several vulnerabilities in the past.

Soluzione	It is recommended to either disable the snmp service or block incoming traffic to the identified port. If you NEED this service make sure that ONLY trusted ips are allowed to connect to it. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	Printer Spooler access port 515 TCP
Livello rischio	Basso
Porta	515/tcp
SPID	2359
CVE	CVE-2001-0670
CVE	CVE-2001-1022
CVE	CVE-2001-0353
CVE	CVE-2000-0839
CVSS	CVE-2001-0670 - CVSS Score V2: 7.5
CVSS	CVE-2001-1022 - CVSS Score V2: 7.5
CVSS	CVE-2001-0353 - CVSS Score V2: 10
CVSS	CVE-2000-0839 - CVSS Score V2: 5
Impatto	The Printer spooler service has been found listening. This service is known to have contained many vulnerabilities on multiple platforms. The vulnerabilities can lead to system access by an attacker. It is possible for an attacker in some cases to gain access to the printer and by this doing social engineer and denial of service attacks by overly flooding the printer and make it print out constantly. The attacker can also print information out on your printer that can look like it is validate and trick the employers to give the attacker access.
Soluzione	It is recommended to block incoming traffic to the printer on the identified port and make sure only trusted IPs are allowed to connect to the printer. NOTE: In this check we only relied on the presences of the identified port. Some system are setup to act with many ghost ports open in order to trick attackers. So it is recommended that you verify the service running on the port and if you KNOW you and can verify that another service is run on the port that is not equal to what we detected please ignore this check.
Output della vulnerabilità / Evidenze	
	Please note in this check we only relied on the presence of the found port. If you run another service on the found port please mark this check as a false positive in the menu.

Vulnerabilità	SMTP Ehlo Command
Livello rischio	Informazione
Porta	25/tcp
SPID	1765
CVE	CVE-1999-0531
CVSS	