

# REPORT S5 – L3

## 1) Introduzione

Il presente report documenta l'attività di **Vulnerability Scanning** svolta nell'ambito dell'esercizio S5 – L3, utilizzando lo strumento Nessus Essentials.

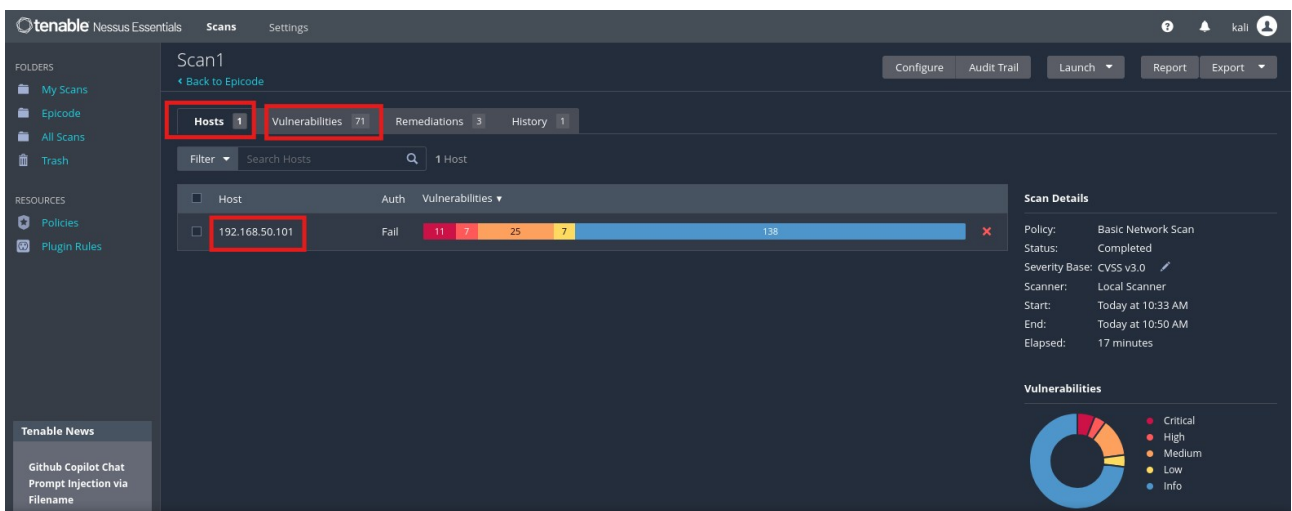
**L'obiettivo dell'attività è identificare e analizzare le vulnerabilità presenti su un sistema deliberatamente vulnerabile**, al fine di comprendere il funzionamento di uno scanner di sicurezza e l'interpretazione dei risultati ottenuti.

La scansione è stata eseguita su un singolo host di laboratorio (**Metasploitable**) mediante una **Basic Network Scan**, senza l'utilizzo di credenziali, simulando uno scenario di attacco esterno.

**Le vulnerabilità rilevate sono state successivamente classificate in base alla severità e analizzate in termini di descrizione, impatto e possibili contromisure.**

## 2) Panoramica

- Host: 192.168.50.101
- Totale vulnerabilità: 71
- Suddivisione per severità (Critical / High / Medium / Low)
- Policy: *Basic Network Scan*
- Status: *Completed*



## 2) Sezione vulnerabilità

A seguire sono state suddivise le vulnerabilità in base alla severità come da esempio.

### Vulnerabilities >>> Severity: CRITICAL

The screenshot shows the Tenable Nessus Essentials interface for a scan named 'Scan1'. The 'Vulnerabilities' tab is selected, showing 7 vulnerabilities. The table lists the following critical vulnerabilities:

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	2

On the right, the 'Scan Details' section shows: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 10:33 AM, End: Today at 10:50 AM, Elapsed: 17 minutes. Below this, a 'Vulnerabilities' donut chart shows 7 Critical vulnerabilities.

### Vulnerabilities >>> Severity: HIGH

The screenshot shows the Tenable Nessus Essentials interface for a scan named 'Scan1'. The 'Vulnerabilities' tab is selected, showing 6 vulnerabilities. The table lists the following high vulnerabilities:

Sev	CVSS	VPR	EPSS	Name	Family	Count
HIGH	8.6	5.2	0.1988	ISC BIND Service Downgrade / Reflected...	DNS	1
HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
HIGH	7.5	6.1	0.4002	SSL Medium Strength Cipher Suites Sup...	General	2
HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1

On the right, the 'Scan Details' section shows: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 10:33 AM, End: Today at 10:50 AM, Elapsed: 17 minutes. Below this, a 'Vulnerabilities' donut chart shows 6 High vulnerabilities.

## Vulnerabilities >>> Severity: MEDIUM

**tenable** Nessus Essentials Scans Settings

FOLDERS: My Scans, Epicode, All Scans, Trash

RESOURCES: Policies, Plugin Rules

Tenable News: Cybersecurity Snapshot: Predictions for 2026: AI A... [Read More](#)

Search Vulnerabilities: 12 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decry...	Misc.	1
MEDIUM	5.3	4.0	0.6899	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MEDIUM	5.3			Apache Tomcat Default Files	Web Servers	1
MEDIUM	5.3			SMB Signing not required	Misc.	1
MEDIUM	4.3 *	1.4	0.9194	SSL/TLS EXPORT_RSA <= 512-bit Cipher ...	Misc.	1
MEDIUM	4.0 *	7.3	0.6945	SMTP Service STARTTLS Plaintext Comm...	SMTP problems	1
MEDIUM	...	...	...	SSL (Multiple Issues)	General	11
MEDIUM	...	...	...	DNS (Multiple Issues)	DNS	2
MEDIUM	...	...	...	ISC Bind (Multiple Issues)	DNS	2

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 10:33 AM  
End: Today at 10:50 AM  
Elapsed: 17 minutes

**Vulnerabilities**

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

## Vulnerabilities >>> Severity: LOW

**tenable** Nessus Essentials Scans Settings

FOLDERS: My Scans, Epicode, All Scans, Trash

RESOURCES: Policies, Plugin Rules

Tenable News: CVE-2025-14847 (MongoBleed): MongoDB Memory Leak V... [Read More](#)

Search Vulnerabilities: 5 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
LOW	3.7	3.9	0.9403	SSL/TLS EXPORT_DHE <= 512-bit Export ...	Misc.	1
LOW	3.4	5.1	0.9402	SSLv3 Padding Oracle On Downgraded ...	General	2
LOW	2.6 *			X Server Detection	Service detection	1
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date ...	General	1
LOW	...	...	...	SSH (Multiple Issues)	Misc.	2

**Scan Details**

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 10:33 AM  
End: Today at 10:50 AM  
Elapsed: 17 minutes

**Vulnerabilities**

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

# Vulnerabilities >>> Severity: INFO

Tenable

Nessus Essentials

Scans

Settings

My Scans

Epicode

All Scans

Trash

Policies

Plugin Rules

Tenable News

Trend Micro Apex Central Multiple Vulnerabilities

Read More

Scan1

Back to Epicode

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 54

Remediations 3

History 1

Filter

Search Vulnerabilities

54 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
Info	...	...	...	SSL (Multiple Issues)	General	13	
Info	...	...	...	SMB (Multiple Issues)	Windows	7	
Info	...	...	...	HTTP (Multiple Issues)	Web Servers	4	
Info	...	...	...	TLS (Multiple Issues)	General	4	
Info	...	...	...	DNS (Multiple Issues)	DNS	3	
Info	...	...	...	FTP (Multiple Issues)	Service detection	3	
Info	...	...	...	VNC (Multiple Issues)	Service detection	3	
Info	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2	
Info	...	...	...	ISC Bind (Multiple Issues)	DNS	2	
Info	...	...	...	PHP (Multiple Issues)	Web Servers	2	
Info	...	...	...	RPC (Multiple Issues)	RPC	2	
Info	...	...	...	SSH (Multiple Issues)	General	2	
Info	...	...	...	SSH (Multiple Issues)	Service detection	2	
Info	...	...	...	Web Server (Multiple Issues)	Web Servers	2	
Info	...	...	...	Nessus SYN scanner	Port scanners	25	

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 10:33 AM

End: Today at 10:50 AM

Elapsed: 17 minutes

Vulnerabilities

Critical

High

Medium

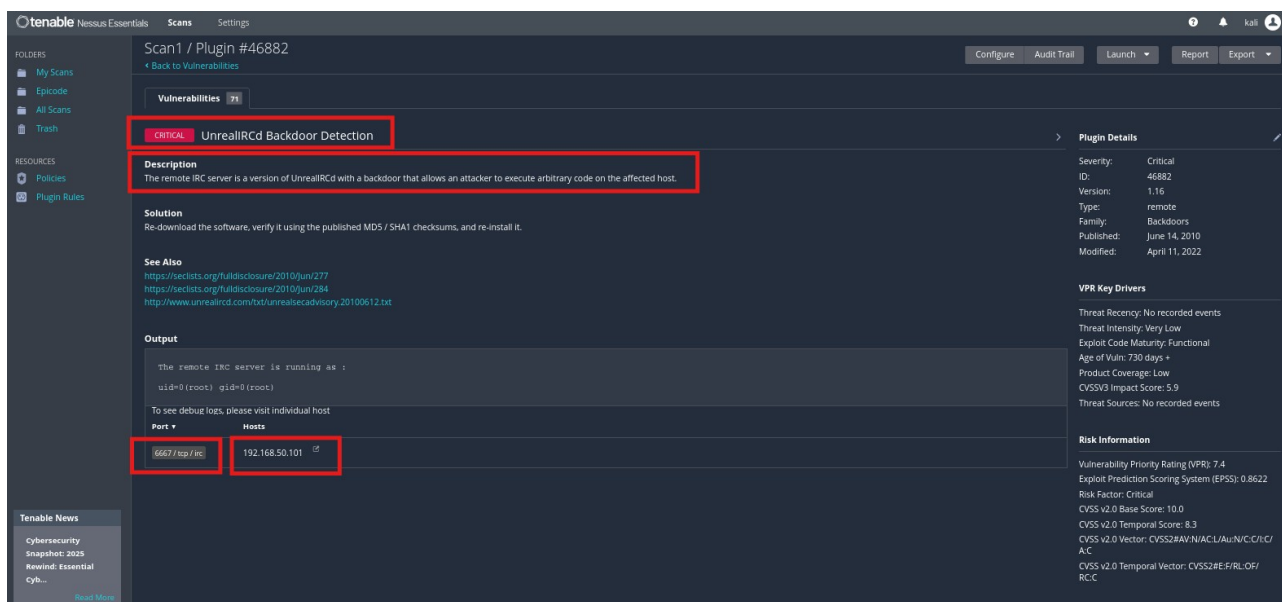
Low

Info

### 3) Analisi Vulnerabilità – *UnrealIRCd Backdoor Detection*

#### - Identificazione della vulnerabilità

- **Nome:** UnrealIRCd Backdoor Detection
- **Gravità:** Critical
- **Servizio coinvolto:** IRC (porta 6667/TCP)
- **Host interessato:** 192.168.50.101
- **Tipo di vulnerabilità:** Backdoor / Remote Code Execution
- **Scanner:** Nessus Essentials
- **Policy utilizzata:** Basic Network Scan



#### Descrizione della vulnerabilità – *UnrealIRCd Backdoor Detection*

La vulnerabilità indica la presenza di una versione compromessa del software **UnrealIRCd**, un server IRC che contiene una **backdoor intenzionalmente inserita**. Questa backdoor consente a un attaccante remoto di **eseguire codice arbitrario** sul sistema bersaglio semplicemente inviando comandi appositamente costruiti al servizio IRC.

In pratica, il servizio IRC in esecuzione sulla macchina Metasploitable è stato avviato utilizzando una versione **non sicura e già compromessa**, rendendo il sistema completamente esposto ad attacchi remoti.

## Impatto (Risk / Impact)

L'impatto di questa vulnerabilità è **molto elevato**.

Un attaccante remoto potrebbe:

- eseguire comandi arbitrari sul sistema
- ottenere una shell remota
- compromettere completamente il server
- installare malware o backdoor persistenti
- utilizzare la macchina come punto di partenza per attacchi verso altri sistemi della rete

Trattandosi di una **Remote Code Execution con privilegi root**, la riservatezza, l'integrità e la disponibilità del sistema risultano totalmente compromesse.

## Soluzione (Remediation)

Nessus consiglia di:

- rimuovere la versione compromessa di UnrealIRCd
- reinstallare il software da fonti ufficiali
- verificare l'integrità del pacchetto tramite checksum **MD5/SHA**
- in alternativa, **disabilitare completamente il servizio IRC** se non necessario

In un contesto reale, la presenza di una backdoor richiederebbe anche:

- analisi forense del sistema
- verifica di eventuali compromissioni successive

## 4) Analisi Vulnerabilità – *rlogin Service Detection*

### - Identificazione della vulnerabilità

- **Nome:** rlogin Service Detection
- **Gravità:** High
- **Servizio coinvolto:** rlogin
- **Porta:** 513/TCP
- **Host interessato:** 192.168.50.101
- **Tipo di vulnerabilità:** Servizio legacy non sicuro / Cleartext authentication
- **Scanner:** Nessus Essentials
- **Policy:** Basic Network Scan

**tenable** Nessus Essentials Scans Settings

**FOLDERS**

- My Scans
- Epicode
- All Scans
- Trash

**RESOURCES**

- Policies
- Plugin Rules

**Tenable News**

WordPress - Ultimate Dashboard exposed API key

**Output**

Port	Hosts
513 / tcp / rlogin	192.168.50.101

**Description**

The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts equiv files.

**Solution**

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

**Plugin Details**

Severity: High  
ID: 10205  
Version: 1.36  
Type: remote  
Family: Service detection  
Published: August 30, 1999  
Modified: April 11, 2022

**VPR Key Drivers**

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Unproven  
Age of Vuln: 730 days +  
Product Coverage: Low  
CVSSv3 Impact Score: 5.9  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 6.7  
Exploit Prediction Scoring System (EPSS): 0.5006  
Risk Factor: High  
CVSS v2.0 Base Score: 7.5  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/AP

**Vulnerability Information**

Exploit Available: true  
Exploit Ease: Exploits are available  
Vulnerability Pub Date: January 1, 1990

Exploitable With

### Descrizione della vulnerabilità – *rlogin Service Detection*

La vulnerabilità indica la presenza del servizio **rlogin** attivo sul sistema remoto. rlogin è un servizio legacy utilizzato per l'accesso remoto, ma è considerato **insicuro** perché trasmette **credenziali e dati in chiaro** (cleartext) tra client e server.

Un attaccante posizionato sulla rete potrebbe intercettare le credenziali tramite tecniche di **sniffing** o **man-in-the-middle**, compromettendo l'accesso al sistema. Inoltre, il servizio può consentire autenticazioni deboli o bypass dell'autenticazione basati su hostname o indirizzi IP.

## Impatto (Impact)

L'impatto della vulnerabilità è significativo.

Un attaccante potrebbe:

- intercettare username e password in chiaro
- effettuare accessi non autorizzati
- sfruttare meccanismi di trust basati su hostname o IP
- utilizzare il servizio come punto di ingresso per attacchi successivi

La compromissione dell'accesso remoto può portare a una violazione della **riservatezza** e dell'**integrità** del sistema.

## Soluzione (Remediation)

Nessus consiglia di:

- disabilitare il servizio rlogin
- rimuovere la voce `login` dai file di configurazione di `inetd`
- riavviare il servizio di rete
- utilizzare protocolli sicuri come **SSH** per l'accesso remoto

La migrazione verso SSH consente l'uso di **cifratura, autenticazione forte e integrità dei dati**.

## 5) Analisi Vulnerabilità – *TLS Version 1.0 Protocol Detection*

### - Identificazione della vulnerabilità

- **Nome:** TLS Version 1.0 Protocol Detection
- **Gravità: Medium**
- **Protocollo coinvolto:** TLS 1.0
- **Servizi interessati:**
  - **PostgreSQL** – porta 5432/TCP
  - **SMTP** – porta 25/TCP
- **Host interessato:** 192.168.50.101
- **Tipo di vulnerabilità:** Protocollo crittografico obsoleto
- **Scanner:** Nessus Essentials
- **Policy:** Basic Network Scan

**tenable** Nessus Essentials Scans Settings

Scan1 / Plugin #104743

Configure Audit Trail Launch Report Export

**Vulnerabilities** 71

**MEDIUM** TLS Version 1.0 Protocol Detection

**Description**  
The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

**Solution**  
Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

**See Also**  
<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

**Output**  
TLSv1 is enabled and the server supports at least one cipher.  
To see debug logs, please visit individual host

Port	Hosts
5432 / tcp / postgresql	192.168.50.101
25 / tcp / smtp	192.168.50.101

**Plugin Details**

Severity: Medium  
ID: 104743  
Version: 1.10  
Type: remote  
Family: Service detection  
Published: November 22, 2017  
Modified: April 19, 2023

**Risk Information**  
Risk Factor: Medium  
CVSS v3.0 Base Score: 6.5  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/L:LA/N  
CVSS v2.0 Base Score: 6.1  
CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:L/P:A/N

**Vulnerability Information**  
Asset Inventory: True

**Reference Information**  
CVE: 327

**Tenable News**  
The 3th Rule: How To Silence 97% of Your Cloud Alert...  
[Read More](#)

## Descrizione della vulnerabilità – *TLS Version 1.0 Protocol Detection*

La vulnerabilità indica che il sistema remoto accetta connessioni cifrate utilizzando **TLS versione 1.0**, un protocollo considerato **obsoleto e non più sicuro**.

TLS 1.0 presenta diverse **debolezze crittografiche** che possono essere sfruttate da un attaccante per compromettere la sicurezza delle comunicazioni.

Le versioni più recenti del protocollo, come **TLS 1.2 e TLS 1.3**, sono progettate per mitigare queste debolezze e rappresentano lo standard attuale per le comunicazioni sicure.

## Impatto (Impact)

L'impatto di questa vulnerabilità è **moderato**, ma comunque rilevante in un contesto reale.

Un attaccante potrebbe:

- intercettare comunicazioni cifrate debolmente
- sfruttare vulnerabilità note di TLS 1.0
- compromettere la riservatezza dei dati trasmessi

Inoltre, l'utilizzo di TLS 1.0 può causare **problemi di compatibilità** con browser e client moderni e comportare **non conformità** agli standard di sicurezza.

## Soluzione (Remediation)

Nessus raccomanda di:

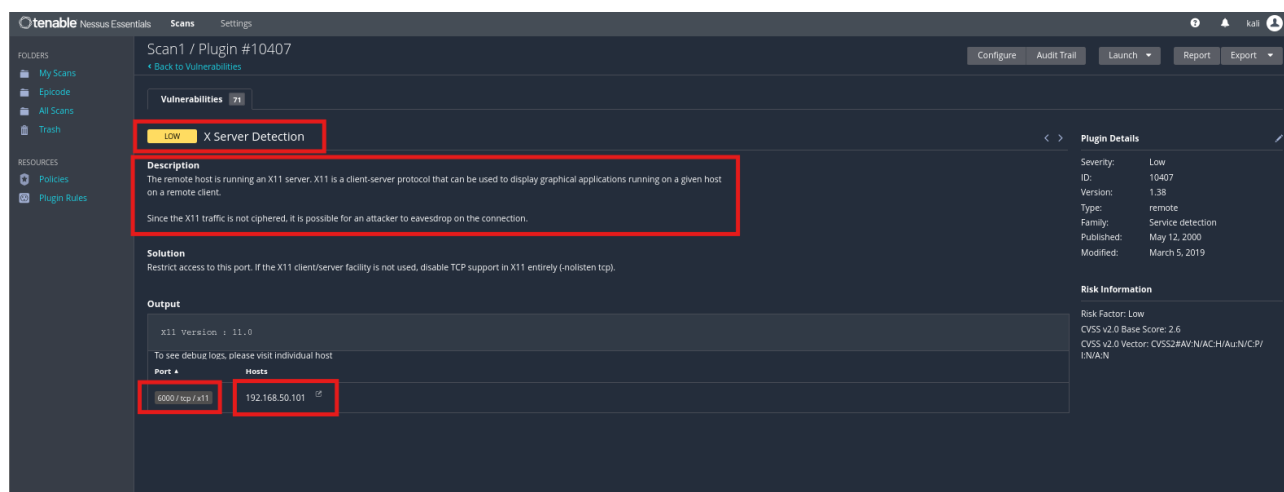
- **abilitare TLS 1.2 e TLS 1.3**
- **disabilitare completamente TLS 1.0**
- aggiornare le configurazioni dei servizi interessati (PostgreSQL, SMTP)
- verificare la compatibilità dei client dopo la modifica

L'adozione di protocolli più recenti migliora la sicurezza delle comunicazioni e garantisce la conformità agli standard attuali.

## 6) Analisi Vulnerabilità – X Server Detection

### - Identificazione della vulnerabilità

- **Nome:** X Server Detection
- **Gravità:** Low
- **Servizio coinvolto:** X11 (X Server)
- **Porta:** 6000/TCP
- **Host interessato:** 192.168.50.101
- **Tipo di vulnerabilità:** Servizio di rete non cifrato / Information Exposure
- **Scanner:** Nessus Essentials
- **Policy:** Basic Network Scan



### Descrizione della vulnerabilità – X Server Detection

La vulnerabilità indica che il sistema remoto sta eseguendo un **server X11** accessibile tramite rete.

Il protocollo X11 utilizza un'architettura client-server per la visualizzazione grafica delle applicazioni, ma **non cifra il traffico di rete**.

Di conseguenza, un attaccante presente sulla stessa rete potrebbe **intercettare (eavesdropping)** i dati scambiati tra client e server, ottenendo informazioni sulle sessioni grafiche.

## Impatto (Impact)

L'impatto di questa vulnerabilità è considerato **basso**, in quanto non consente direttamente l'esecuzione di codice o l'accesso non autorizzato al sistema.

Tuttavia, in specifiche condizioni di rete, un attaccante potrebbe:

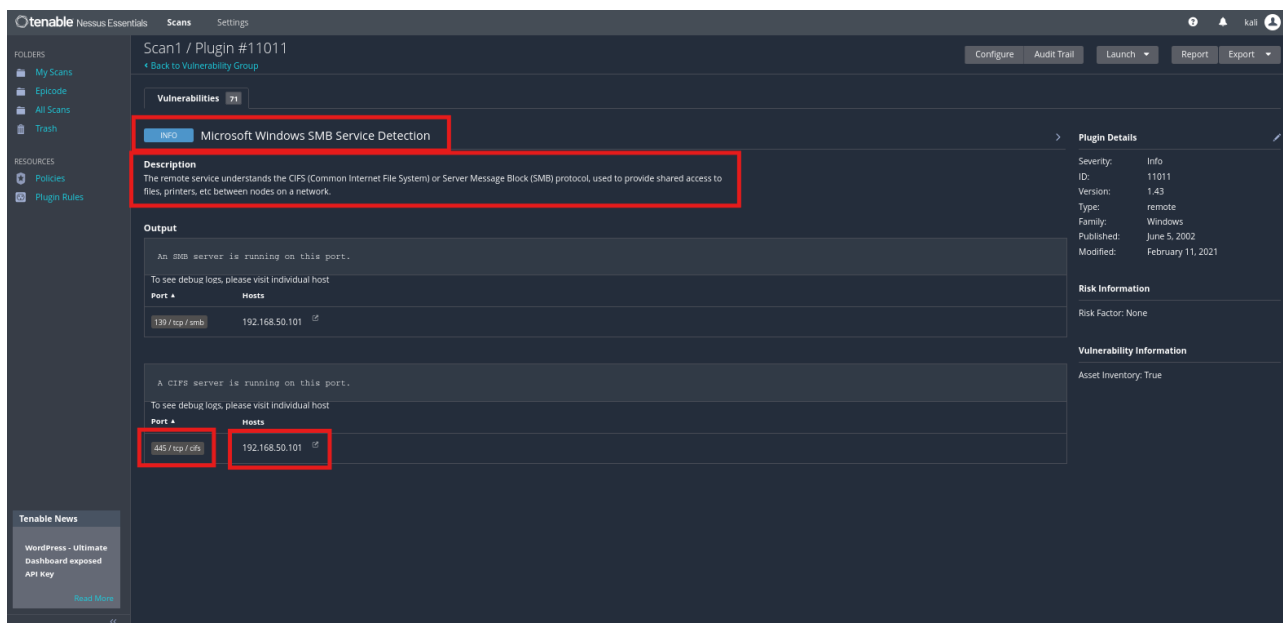
- intercettare informazioni visive
- osservare le attività dell'utente
- raccogliere informazioni utili per attacchi successivi

## Soluzione (Remediation)

Nessus consiglia di:

- limitare l'accesso alla porta **6000/TCP**
- disabilitare il supporto TCP di X11 se non necessario
- utilizzare meccanismi sicuri come **SSH tunneling** per l'accesso grafico remoto
- avviare X11 con l'opzione `-no listen tcp` per impedire connessioni remote

**NB:** Durante la scansione è stata inoltre rilevata la presenza del servizio SMB/CIFS sulle porte 139 e 445/TCP. **Questa informazione è classificata come “Informational” da Nessus e non rappresenta una vulnerabilità diretta, ma indica semplicemente che il servizio di condivisione file è attivo sul sistema.** Tali informazioni possono essere utili nelle fasi successive di analisi per individuare eventuali vulnerabilità specifiche del protocollo SMB.



## CONCLUSIONI:

La scansione ha evidenziato vulnerabilità di diversa severità, dalle criticità più gravi fino a configurazioni e servizi meno impattanti, permettendo di comprendere come interpretare correttamente i risultati forniti da uno scanner di sicurezza.

L'analisi svolta si è limitata alla valutazione del rischio e delle possibili contromisure, senza procedere allo sfruttamento delle vulnerabilità individuate, in linea con gli obiettivi dell'esercizio.

L'attività ha dimostrato l'importanza di una corretta configurazione dei servizi di rete e dell'aggiornamento dei sistemi, evidenziando come la presenza di componenti obsoleti o non necessari possa aumentare significativamente la superficie di attacco.