

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.

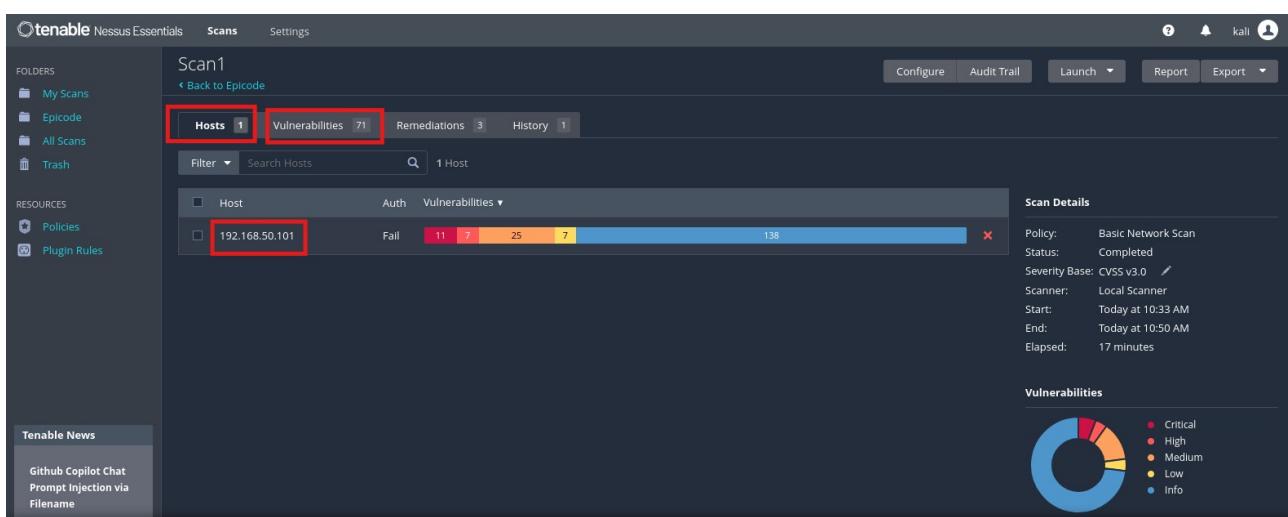
L'obiettivo dell'attività è identificare e analizzare le vulnerabilità presenti su un sistema deliberatamente **vulnerabile**, al fine di comprendere il funzionamento di uno scanner di sicurezza e l'interpretazione dei risultati ottenuti.

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

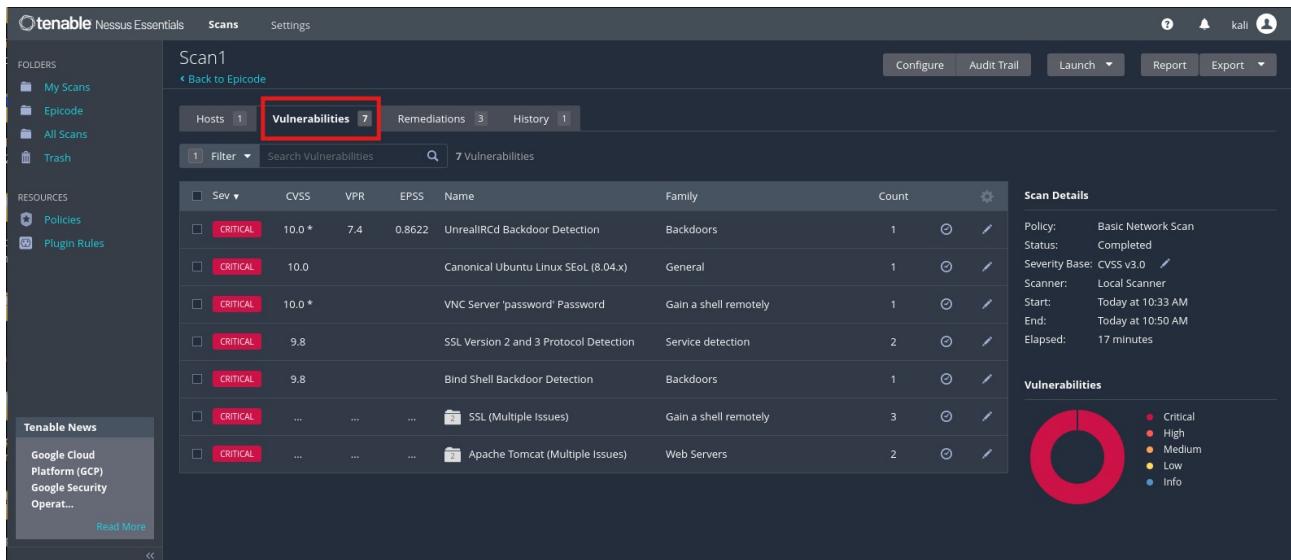
- Host: **192.168.50.101**
- Totale vulnerabilità: **71**
- Suddivisione per severità (Critical / High / Medium / Low)
- Policy: *Basic Network Scan*
- Status: *Completed*



2) Sezione vulnerabilità

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

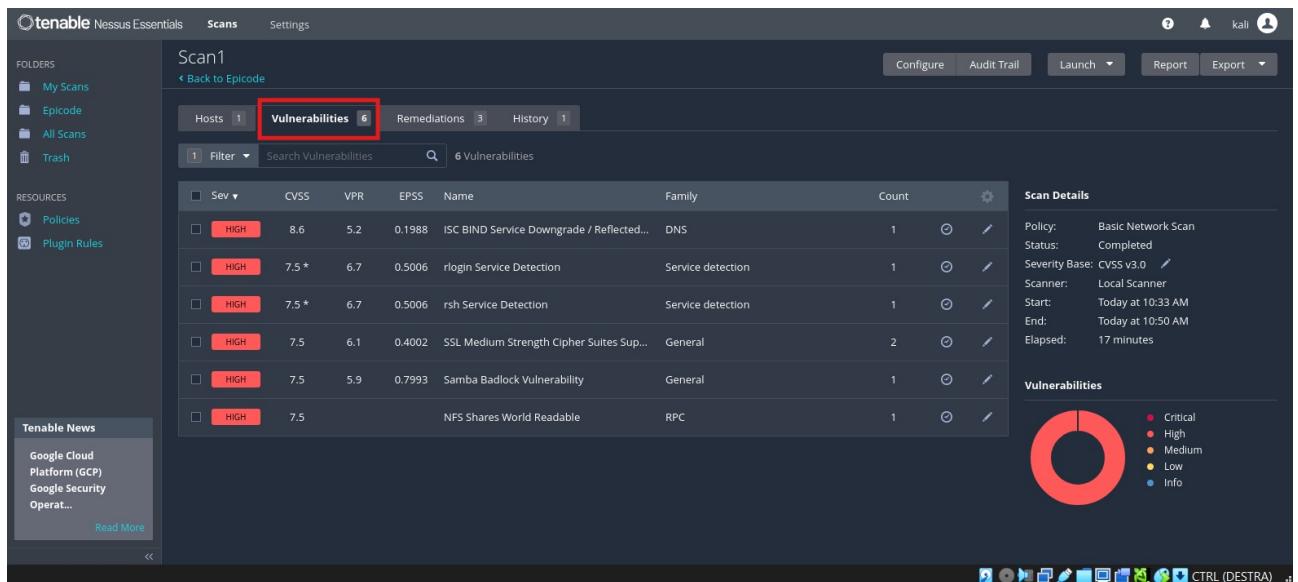
Vulnerabilities >>> Severity: CRITICAL



The screenshot shows the Nessus Essentials interface for a scan named "Scan1". The "Vulnerabilities" tab is selected, highlighted with a red box. The table lists 7 critical vulnerabilities across various hosts and families. The "Scan Details" panel on the right indicates a completed basic network scan with CVSS v3.0 using a local scanner, taking 17 minutes. A pie chart at the bottom shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light green).

Host	Severity	CVSS	VPR	EPSS	Name	Family	Count
Host 1	Critical	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors	1
Host 2	Critical	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
Host 3	Critical	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
Host 4	Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
Host 5	Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Host 6	Critical	SSL (Multiple Issues)	Gain a shell remotely	3
Host 7	Critical	Apache Tomcat (Multiple Issues)	Web Servers	2

Vulnerabilities >>> Severity: HIGH



The screenshot shows the Nessus Essentials interface for a scan named "Scan1". The "Vulnerabilities" tab is selected, highlighted with a red box. The table lists 6 high severity vulnerabilities across various hosts and families. The "Scan Details" panel on the right indicates a completed basic network scan with CVSS v3.0 using a local scanner, taking 17 minutes. A pie chart at the bottom shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light green).

Host	Severity	CVSS	VPR	EPSS	Name	Family	Count
Host 1	High	8.6	5.2	0.1988	ISC BIND Service Downgrade / Reflected...	DNS	1
Host 2	High	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1
Host 3	High	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1
Host 4	High	7.5	6.1	0.4002	SSL Medium Strength Cipher Suites Sup...	General	2
Host 5	High	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1
Host 6	High	7.5			NFS Shares World Readable	RPC	1

Vulnerabilities >>> Severity: MEDIUM

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'My Scans', 'Episode', 'All Scans', and 'Trash'. Below that is a 'Tenable News' section with a 'Cybersecurity Snapshot' for 2026. The main area has tabs for 'Hosts' (1), 'Vulnerabilities' (12), 'Remediations' (3), and 'History' (1). A search bar at the top right shows '12 Vulnerabilities'. The central table lists the vulnerabilities with columns for Severity (Medium), CVSS, VPR, EPSS, Name, Family, Count, and a gear icon. The 'Scan Details' panel on the right shows a completed scan with various metrics. A donut chart at the bottom indicates the severity distribution.

Severity	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

Vulnerabilities >>> Severity: LOW

This screenshot is similar to the previous one but shows 5 Low severity vulnerabilities. The layout is identical, with the sidebar, search bar, and 'Scan Details' panel. The central table now lists 5 vulnerabilities with low severity. The donut chart at the bottom shows the low severity count.

Severity	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

Vulnerabilities >>> Severity: INFO

Screenshot of the Tenable Nessus Essentials interface showing the results of a scan titled "Scan1". The "Vulnerabilities" tab is selected, displaying 54 vulnerabilities across various service families.

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 10:56 AM
- Elapsed: 17 minutes

Vulnerabilities:

Severity	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

Tenable News:

- Trend Micro Apex Central Multiple Vulnerabilities

[Read More](#)

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

The screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'My Scans' (selected), 'Epicode', 'Trash', 'Policies', and 'Plugin Rules'. The main area shows a scan titled 'Scan1 / Plugin #46882'. A red box highlights the 'CRITICAL' status of the 'UnrealIRCd Backdoor Detection' vulnerability. The 'Description' section states: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' Below it, the 'Solution' section suggests re-downloading the software, verifying MD5 / SHA1 checksums, and re-installing it. The 'Output' section shows command-line logs indicating the server is running as root. The 'Hosts' section lists the target IP 192.168.50.101. On the right, the 'Plugin Details' panel provides technical details: Severity: Critical, ID: 46882, Version: 1.16, Type: remote, Family: Backdoors, Published: June 14, 2010, Modified: April 11, 2022. It also includes sections for 'VPR Key Drivers' and 'Risk Information'.

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

The screenshot shows the Tenable Nessus Essentials web interface. In the top navigation bar, 'Scans' is selected. On the left sidebar, under 'FOLDERS', 'My Scans' is highlighted. The main content area displays a scan titled 'HIGH rlogin Service Detection'. A red box highlights the 'Description' section, which contains a detailed explanation of the vulnerability. Another red box highlights the 'Output' section, specifically the 'Hosts' table where '513/tcp/rlogin' and '192.168.50.101' are listed. To the right, the 'Plugin Details' panel is open, showing the following information:
Severity: High
ID: 10205
Version: 1.36
Type: remote
Family: Service detection
Published: August 30, 1999
Modified: April 11, 2022
The 'VPR Key Drivers' and 'Risk Information' sections are also visible on the right.

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

The screenshot shows the Tenable Nessus Essentials web interface. The main title is "Scan1 / Plugin #104743". The left sidebar has sections for FOLDERS (My Scans, Epicodes, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and Tenable News (The 3% Rule: How To Silence 97% of Your Cloud Alerts...). The main content area shows a "Vulnerabilities" section with 71 items. A specific item is highlighted with a red box: "TLS Version 1.0 Protocol Detection" (Severity: MEDIUM, ID: 104743, Version: 1.10, Type: remote, Family: Service detection, Published: November 22, 2017, Modified: April 19, 2023). The "Description" field contains text about TLS 1.0 design flaws and deprecation. The "Solution" field suggests enabling TLS 1.2 and higher. The "See Also" field links to IETF draft documentation. The "Output" table lists ports and hosts affected: 5432/tcp/postgresql (192.168.50.101) and 25/tcp/smtp (192.168.50.101). The right side of the screen displays "Plugin Details" (Risk Information, Vulnerability Information, Reference Information) and "Asset Inventory: True".

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

The screenshot shows the Nessus Essentials interface. In the center, a red box highlights the 'Description' section of the 'X Server Detection' vulnerability. The description states: 'The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client. Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.' To the right of the description, another red box highlights the 'Plugin Details' panel, which provides technical details about the vulnerability, such as Severity: Low, ID: 10407, Version: 1.38, Type: remote, Family: Service detection, Published: May 12, 2000, and Modified: March 5, 2019. At the bottom left, two red boxes highlight the 'Port' and 'Hosts' fields, which show '6000 / tcp / x11' and '192.168.50.101' respectively.

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 `-nolisten 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.

The screenshot shows the Tenable Nessus Essentials web interface. In the center, a scan result for 'Microsoft Windows SMB Service Detection' is displayed. The 'Description' section, which states 'The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.', is highlighted with a red box. Below this, under 'Output', there are two sections for port 139 and port 445. Each section has a 'Port' field and a 'Hosts' field. The 'Port' fields show '139 /tcp /smb' and '445 /tcp /cifs' respectively, both highlighted with red boxes. The 'Hosts' field in both cases contains '192.168.50.101'. To the right of the main content area, there are sections for 'Plugin Details', 'Risk Information', and 'Vulnerability Information', each with detailed information about the plugin.

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.