

# Report S5-L5

Vulnerability  
Scanner &  
Solving





# Indice

Introduzione .....	1
Risultati Prima Scansione .....	2
Analisi delle Vulnerabilità .....	3
Risoluzione delle Vulnerabilità .....	4
Risultati Seconda Scansione .....	6
Conclusioni .....	7

# Introduzione

Questo report illustra la procedura adottata per la scansione di sicurezza del sistema Metasploitable, con l'obiettivo di identificare e moderare da due a quattro vulnerabilità di livello critico o elevato.

Dopo la scansione iniziale e l'identificazione delle principali minacce, abbiamo implementato azioni di rimedio specifiche, incluse misure di configurazione delle regole firewall.

Successivamente, abbiamo eseguito una seconda scansione per valutare l'efficacia di tali interventi confrontando i risultati con quelli iniziali.

Questo processo ci permetterà di dimostrare come interventi mirati possano migliorare la sicurezza del sistema.

## Obiettivi

- Scansione e Analisi dei Rischi:** Condurre una scansione completa di sicurezza sul sistema Metasploitable per identificare le vulnerabilità critiche e ad alto rischio. Analizzare i rischi associati a queste vulnerabilità, comprendendo il potenziale impatto e le probabilità di sfruttamento.
- Implementazione di Contromisure:** Sviluppare e applicare misure di mitigazione specifiche per ciascuna delle vulnerabilità identificate. Questo include l'adozione di configurazioni di sicurezza migliorate, l'aggiornamento di software, e l'applicazione di regole di firewall dove appropriato.
- Valutazione dell'Efficacia delle Contromisure:** Rieseguire la scansione del sistema dopo l'implementazione delle contromisure per verificare la loro efficacia. Confrontare i risultati pre e post-intervento per determinare il grado di riduzione del rischio.
- Rapporto e Raccomandazioni:** Fornire un'analisi dettagliata dei risultati della scansione e delle azioni di rimedio, concludendo con raccomandazioni per ulteriori miglioramenti della sicurezza o per il mantenimento delle misure implementate.

## Note



### Metasploitable 2

Soggetto di Analisi:

**Metasploitable è una macchina virtuale volutamente vulnerabile, creata per esercitarsi in tecniche di penetration testing e sviluppare competenze in sicurezza informatica attraverso un ambiente controllato.**



### Laboratorio Virtuale

Ambiente sicuro:

**Utilizziamo un laboratorio virtuale per eseguire i test, garantendo un ambiente sicuro e controllato per le operazioni di penetration testing e altre prassi di sicurezza informatica.**

# Risultati Scansione

## Info

Nessus classifica le vulnerabilità rilevate in base a **quattro livelli di criticità**, che forniscono un'indicazione della gravità e del potenziale impatto di una vulnerabilità sul sistema. Questi livelli di criticità sono:

## Critical

Le vulnerabilità con una classificazione "**Critica**" rappresentano il massimo rischio per la sicurezza del sistema. Possono essere sfruttate dagli attaccanti per compromettere completamente il sistema, ottenere accesso totale o causare danni gravi. È essenziale affrontare **immediatamente** e **prioritariamente** queste vulnerabilità per evitare conseguenze gravi per la sicurezza.

## High

Le vulnerabilità classificate come "**Alte**" rappresentano rischi critici per la sicurezza del sistema. Possono consentire agli attaccanti di ottenere accesso privilegiato al sistema o di eseguire attacchi più gravi. È fondamentale risolvere queste vulnerabilità **immediatamente** per proteggere il sistema e i dati sensibili.

## Medium

Le vulnerabilità con una classificazione "**Media**" rappresentano un rischio significativo, sebbene non critico, per la sicurezza del sistema. Potrebbero consentire agli attaccanti di ottenere un certo grado di accesso non autorizzato o di compromettere la sicurezza del sistema in altri modi. È importante affrontare queste vulnerabilità in modo **tempestivo**.

## Low

Le vulnerabilità classificate come "**Bassa**" di solito rappresentano rischi minimi o limitati. Possono includere problemi minori che potrebbero avere un impatto limitato sulla sicurezza complessiva del sistema. Tali vulnerabilità possono richiedere azioni correttive, ma spesso **non sono urgenti**.

## Nessus Scanner

192.168.50.101



Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾	⚙️
<span>Critical</span>	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	<span>🔗</span>
<span>Critical</span>	10.0		Unix Operating System Unsupported Version Detection	General	1	<span>🔗</span>
<span>Critical</span>	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1	<span>🔗</span>
<span>Critical</span>	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	<span>🔗</span>
<span>Critical</span>	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	<span>🔗</span>
<span>Critical</span>	9.8		Bind Shell Backdoor Detection	Backdoors	1	<span>🔗</span>
<span>Critical</span>	...	...	<span>2</span> SSL (Multiple Issues)	Gain a shell remotely	3	<span>🔗</span>
<span>High</span>	7.5	5.9	Samba Badlock Vulnerability	General	1	<span>🔗</span>
<span>High</span>	7.5		NFS Shares World Readable	RPC	1	<span>🔗</span>
<span>Mixed</span>	...	...	<span>15</span> SSL (Multiple Issues)	General	28	<span>🔗</span>
<span>Mixed</span>	...	...	<span>5</span> ISC Bind (Multiple Issues)	DNS	5	<span>🔗</span>
<span>Medium</span>	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	<span>🔗</span>
<span>Medium</span>	5.0	4.4	SSL Anonymous Cipher Suites Supported	Service detection	1	<span>🔗</span>

# Analisi Vulnerabilità

Dalla scansione di sicurezza, abbiamo identificato diverse vulnerabilità, incluse alcune di livello critico che rappresentano un serio rischio per il sistema. Abbiamo selezionato e analizzato in dettaglio quattro di queste vulnerabilità critiche, le cui specifiche sono descritte nel seguente paragrafo.

## Bind shell backdoor detection

**Vulnerabilità:** L'host remoto potrebbe essere stato compromesso e presenta una shell in ascolto su una porta remota senza richiedere alcuna autenticazione.

**Sfruttamento:** Un attaccante potrebbe connettersi alla porta remota e inviare comandi direttamente alla shell, ottenendo così un accesso non autorizzato al sistema compromesso.

**Soluzione:** Per risolvere questa vulnerabilità, è necessario identificare e rimuovere la shell compromessa, inoltre aggiornare e configurare correttamente il software per prevenire future intrusioni.

## VNC Server 'password' Password

**Vulnerabilità:** Il server VNC in esecuzione sul host remoto è protetto da una password debole.

**Sfruttamento:** L'attaccante potrebbe sfruttare questa debolezza della password per accedere al server VNC e ottenere il controllo del sistema.

**Soluzione:** Per risolvere questa vulnerabilità, è necessario cambiare la password del server VNC utilizzando una password forte e complessa. È importante utilizzare una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali per creare una password robusta e efficace per evitare.

## NFS Exported Share Information Disclosure

**Vulnerabilità:** È possibile accedere alle condivisioni NFS sul host remoto.

**Sfruttamento:** Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sul host remoto.

**Soluzione:** Per mitigare questa vulnerabilità, è consigliabile configurare correttamente le autorizzazioni di accesso alle condivisioni NFS, limitando l'accesso solo agli utenti autorizzati e implementando le misure di sicurezza appropriate.

## Apache Tomcat AJP

**Vulnerabilità:** La vulnerabilità riguarda un'AJP connector che consente a un attaccante remoto non autenticato di leggere file dell'applicazione web o, se consentito, di caricare codice malevolo per ottenere l'esecuzione remota di codice (RCE).

**Sfruttamento:** Un attaccante potrebbe leggere file sensibili dell'applicazione o caricare codice malevolo tramite file JSP per assumere il controllo del server, compromettendo la sicurezza e l'integrità del sistema.

**Soluzione:** Per risolvere questa vulnerabilità, è consigliabile aggiornare il software, disabilitare o proteggere l'AJP connector, filtrare e validare l'input, implementare monitoraggio per rilevare attività sospette e utilizzare un firewall.

## Valutazione

Abbiamo deciso di intervenire sulle vulnerabilità di livello critico individuate, basandoci sulla loro gravità e sul potenziale impatto sulla sicurezza del sistema. Per ciascuna di queste, implementeremo le contromisure che abbiamo precedentemente delineato. Queste azioni sono mirate a risolvere efficacemente i rischi associati e a rafforzare la sicurezza del nostro ambiente.

Nel proseguimento del report, forniremo i dettagli tecnici delle soluzioni adottate e il processo di implementazione.

# Risoluzione Vulnerabilità

In questa sezione, discuteremo le misure adottate per risolvere le vulnerabilità rilevate, mostrando come ogni problema è stato affrontato per migliorare la sicurezza del sistema.

## Bind shell backdoor detection

### Procedura

Verifichiamo l'apertura delle porte su metasploitable dal terminale di kali con il comando **nmap +ip** e andremo a localizzare la porta **1524** che corrisponde al servizio **ingress lock** e ne verificheremo lo stato;

successivamente dal terminale di meta andremo a chiuderla con il comando **sudo kill+processo**.

```
512/tcp  open  exec  
513/tcp  open  login  
514/tcp  open  shell  
1099/tcp open  rmiregistry  
1524/tcp open  ingreslock  
2049/tcp open  nfs  
2121/tcp open  ccproxy-ftp  
3306/tcp open  mysql  
5432/tcp open  postgresql
```

```
Would you like to enter a view-only password (y/n)? n  
root@metasploitable:/home/msfadmin# sudo netstat -tulnp | grep 1524  
tcp        0      0 0.0.0.0:1524          0.0.0.0:*          LISTEN  
4442/xinetd  
root@metasploitable:/home/msfadmin# sudo kill 4442
```

### Verifica

Tentiamo una nuova connessione con il comando **nc+ip+porta** e come possiamo vedere ci da **connection refused**.

### Nota

Era possibile anche applicare una regola **firewall**, per mitigare questa vulnerabilità.

```
(kali㉿kali)-[~]  
$ sudo nmap -sS -p 1524 192.168.50.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 05:06 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00096s latency).  
  
PORT      STATE SERVICE  
1524/tcp  closed  ingreslock  
  
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds  
  
(kali㉿kali)-[~]  
$ nc 192.168.50.101 1524  
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused
```

## VNC Server 'password' Password

### Procedura

Per risolvere questa vulnerabilità andremo a modificare la password direttamente dal terminale di metasploitable con il comando **vncpasswd** in root, andremo a impostare una password più sicura e nel nostro caso abbiamo scelto "**Ep1Adm!n**".

### Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲	Hosts
--------	-------

5900 / tcp / vnc	192.168.50.101
------------------	----------------

### Verifica

La password è stata cambiata con successo, il terminale non è impostato per riportare a schermo la conferma ma possiamo esserne sicuri dal fatto che nessun messaggio di errore è stato mandato a schermo.

```
root@metasploitable:/home/msfadmin# vncpasswd  
Using password file /root/.vnc/passwd  
Password:  
Verify:  
Would you like to enter a view-only password (y/n)?  
root@metasploitable:/home/msfadmin#
```

## NFS Exported Share Information Disclosure

```
GNU nano 2.0.7          File: /etc/exports

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,async)
#
# *(rw,sync,no_root_squash,no_subtree_check)
```

### Procedura

Per risolvere questa vulnerabilità andremo a configurare in maniera corretta il file **NFS** così che solo chi è autorizzato può usufruire del servizio.

### Verifica

```
GNU nano 2.0.7          File: /etc/exports          Modified

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,async,root_squash) hostname2(ro,async,root_squash)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,async,fsid=0,crossmnt,root_squash)
# /srv/nfs4/homes  gss/krb5i(rw,async,root_squash)
#
```

siamo andati a rimuovere la stringa che autorizzava l'accesso globale con privilegi, abbiamo applicato un **root\_squash** a tutte le esportazioni, per impedire agli utenti root sui client NFS di avere privilegi elevati sul server NFS.

## Apache Tomcat AJP:

### Procedura

```
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8080/tcp filtered http
```

Per risolvere questa vulnerabilità abbiamo deciso di applicare una **regola firewall** che andrà a filtrare l'accesso alla porta **8009** ovvero la porta associata al **AJP13**.

x	TCP	*	*	192.168.50.101	8009	*	none
---	-----	---	---	----------------	------	---	------

### Verifica

```
6000/tcp open  X11
6667/tcp open  irc
8009/tcp filtered ajp13
```

come possiamo notare eseguendo nuovamente un **nmap** dal terminale di kali la porta non risulta più **open** ma **filtered**.

## Nota

inoltre è consigliato  
l'aggiornamento di apache  
all'ultima versione che può  
essere effettuato seguendo  
questi comandi eseguiti sul  
terminale di Metasploitable2

Aggiorna l'elenco dei pacchetti  
**sudo apt-get update**

Aggiorna Apache alla versione più recente  
**sudo apt-get install --only-upgrade**  
**apache2**

Verifica la versione  
**apache2 -v**

Riavvia il servizio Apache  
**sudo systemctl restart apache2**

# Risultati Seconda Scansione

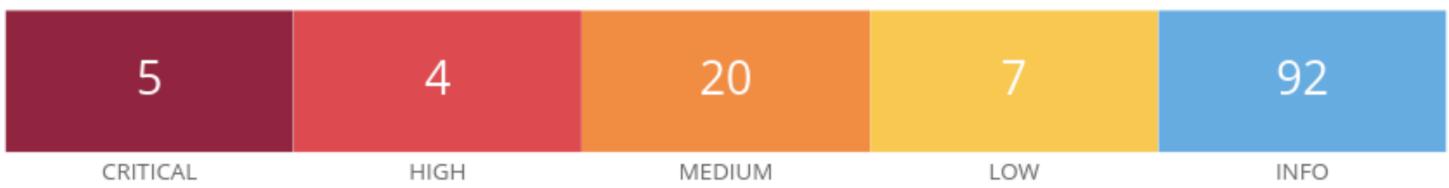
## In Sintesi

La seconda scansione di sicurezza ha mostrato una riduzione marcata del numero di rischi rilevati, passando da **dieci** a **cinque**. Questa diminuzione è un indicatore chiaro dell'efficacia delle misure correttive che abbiamo implementato. Dopo aver analizzato e affrontato le vulnerabilità emerse dalla prima scansione, abbiamo applicato soluzioni **tecniche specifiche**, che includono la riconfigurazione dei servizi e aggiornamenti software.

I risultati delle due scansioni confermano che le correzioni apportate hanno avuto un impatto positivo sulla sicurezza del sistema, riducendo **significativamente** le esposizioni a rischi potenziali.

## Nessus Scanner

**192.168.50.101**



Sev ▾	CVSS ▾	VPR ▾	Name ▾	Family ▾	Count ▾
Critical	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
Critical	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
High	7.5	5.9	Samba Badlock Vulnerability	General	1
Mixed	...	...	SSL (Multiple Issues)	General	26
Mixed	...	...	ISC Bind (Multiple Issues)	DNS	4
Medium	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
Medium	5.9	4.4	SSL Anonymous Cipher Suites Supported	Service detection	1
Medium	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
Mixed	...	...	SSH (Multiple Issues)	Misc.	6
Mixed	...	...	HTTP (Multiple Issues)	Web Servers	3
Mixed	...	...	SMB (Multiple Issues)	Misc.	2
Mixed	...	...	TLS (Multiple Issues)	Misc.	2
Mixed	...	...	TLS (Multiple Issues)	SMTP problems	2

# Conclusione

offriremo una panoramica generale di cosa si intende per vulnerabilità e discuteremo i sette livelli utilizzati per valutare il loro rischio potenziale. Questa analisi non entrerà nei dettagli specifici di ciascuna vulnerabilità, ma fornirà una comprensione essenziale di come vengono classificate e quali implicazioni possono avere sulla sicurezza complessiva del sistema.

## Vulnerability Recap

### Cosa si intende per vulnerabilità

Una vulnerabilità, nel contesto della sicurezza informatica, è una **debolezza** o una falla nel software, nell'hardware o nei processi di un sistema informatico, che può essere sfruttata da un attaccante per compromettere **l'integrità, la disponibilità o la riservatezza dei dati**.

## Valutazione dei Rischi

### 7 Regole per Valutare un rischio:

**Identificazione dei Rischi:** In questa fase, vengono identificati tutti i possibili rischi per la sicurezza e può includere minacce interne ed esterne, come attacchi informatici oppure errori umani.

**Analisi dei Rischi:** Una volta identificati i rischi, si procede con un'analisi approfondita per valutare la loro probabilità di verificarsi e l'impatto che potrebbero avere sull'organizzazione.

**Valutazione dei Controlli Esistenti:** Si valutano i controlli di sicurezza esistenti per determinare se sono efficaci nel mitigare i rischi identificati.

**Identificazione delle Vulnerabilità:** Durante questa fase, vengono individuate le vulnerabilità nei sistemi, processi e controlli di sicurezza esistenti che potrebbero essere sfruttate dalle minacce per causare danni.

**Stima del Rischio Residuo:** Una volta identificati i rischi e valutati i controlli esistenti, si stima il rischio residuo, ossia il livello di rischio che rimane dopo l'applicazione dei controlli. **Pianificazione delle Misure di Mitigazione:** Sulla base dei risultati della valutazione dei rischi, si pianificano e implementano misure di mitigazione per ridurre il rischio a un livello accettabile per l'organizzazione.

**Monitoraggio e Revisione:** Periodicamente, è necessario rivedere e aggiornare la valutazione dei rischi per garantire che l'organizzazione mantenga un livello adeguato di sicurezza informatica.

# Conclusioni Finali

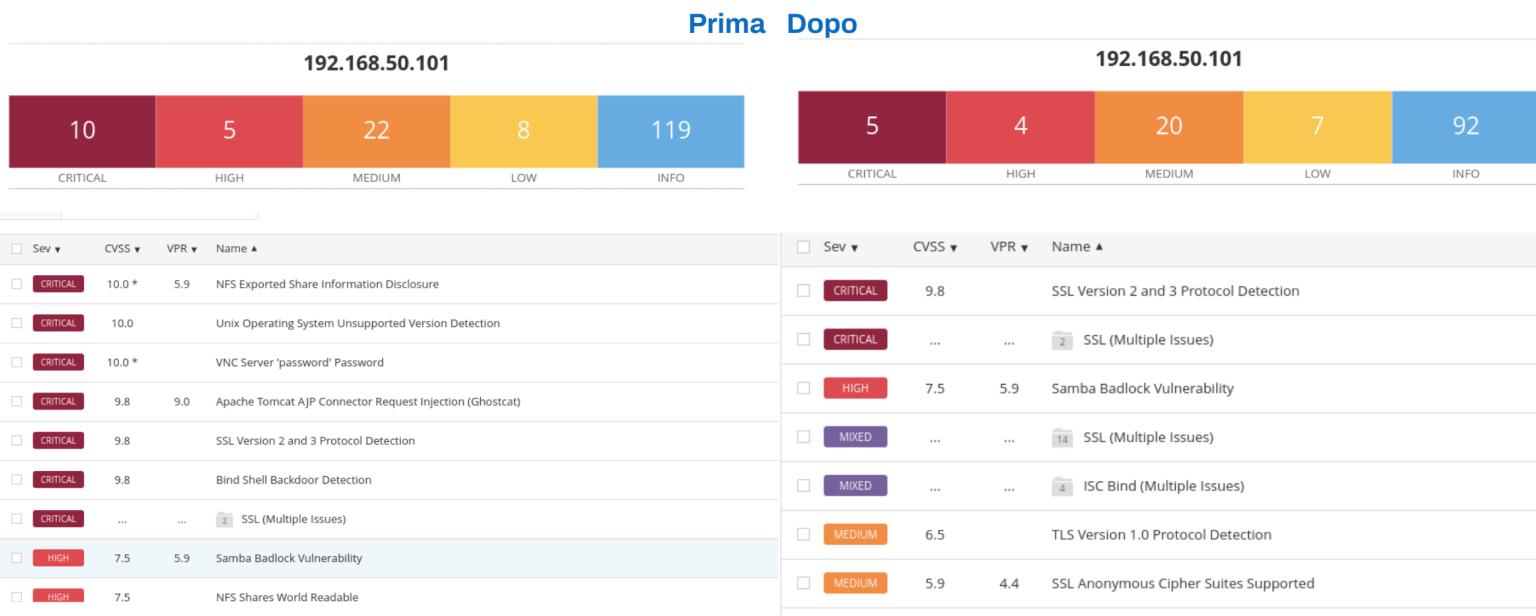
L'analisi condotta attraverso **Nessus** ha fornito una panoramica dettagliata dello stato di sicurezza della nostra macchina.

Le scansioni approfondite hanno rivelato **molte vulnerabilità** significative che richiedono interventi immediati per placare i rischi di compromissione della sicurezza.

Inoltre, il report fornito da **Nessus** fornisce una base solida per l'elaborazione di un piano d'azione mirato a migliorare la sicurezza complessiva del nostro sistema.

L'identificazione delle vulnerabilità critiche ci permette di concentrare le risorse su aree specifiche che richiedono urgenti interventi di mitigazione.

Va sottolineato che la sicurezza informatica è un processo continuo e in costante evoluzione. Pertanto, è fondamentale impegnarsi nella manutenzione regolare del sistema e di installare gli aggiornamenti per aggirare i malware.



## Crediti

<https://learn.epicode.com>

<https://www.offsec.com/metasploit-unleashed/msfconsole-commands/>

<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

<https://www.tenable.com>