

# S5L5

SCANSIONE E RIPARAZIONE  
CRITICITÀ METASPLOITABLE




# INTRODUZIONE

Questo report dettaglia le vulnerabilità identificate su una macchina virtuale Metasploitable2 e le azioni intraprese per mitigarle. Il focus è su tre specifiche vulnerabilità critiche e di alta gravità che sono state corrette efficacemente; l'analisi è supportata dall'uso del software Tenable Nessus Essentials, che ha eseguito scansioni di sicurezza prima e dopo le modifiche.



# PANORAMICA VULNERABILITÀ

## PRIMA SCANSIONE

| <input type="checkbox"/> | Sev ▼    | CVSS ▼ | VPR ▼ | Name ▲  | Family ▲              | Count ▼ | ⚙   |
|--------------------------|----------|--------|-------|---|-----------------------|---------|-----|
| <input type="checkbox"/> | CRITICAL | 10.0 * | 5.9   | NFS Exported Share Information Disclosure   | RPC                   | 1       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | 10.0   |       | Unix Operating System Unsupported Version Detection   | General               | 1       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | 10.0 * |       | VNC Server 'password' Password  | Gain a shell remotely | 1       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | 9.8    | 9.0   | Apache Tomcat AJP Connector Request Injection (Ghostcat)  | Web Servers           | 1       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | 9.8    |       | SSL Version 2 and 3 Protocol Detection  | Service detection     | 2       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | 9.8    |       | Bind Shell Backdoor Detection   | Backdoors             | 1       | 🕒 ✎ |
| <input type="checkbox"/> | CRITICAL | ...    | ...   |  SSL (Multiple Issues) | Gain a shell remotely | 3       | 🕒 ✎ |

### Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0 ✎  
Scanner: Local Scanner  
Start: Today at 6:37 AM  
End: Today at 7:06 AM  
Elapsed: 28 minutes

### Vulnerabilities



# DESCRIZIONE VULNERABILITÀ EVIDENZIATE

- 1** VNC Server 'password' Password (CVSS 10.0)
  - Famiglia: Gain a shell remotely
  - Impatto: La configurazione del server VNC con password debole o predefinita esponeva il sistema a un accesso remoto non autorizzato, aumentando il rischio di attacchi malintenzionati e la possibile compromissione del sistema.
- 2** Apache Tomcat AJP Connector Request Injection (Ghostcat) (CVSS 9.8)
  - Famiglia: Web Servers
  - Impatto: Una vulnerabilità critica nel connettore AJP di Apache Tomcat che permetteva l'iniezione di richieste malevole, potenzialmente conducendo all'esecuzione di codice arbitrario da parte di un attaccante remoto.
- 3** Bind Shell Backdoor Detection (CVSS 9.8)
  - Famiglia: Backdoors
  - Impatto: Rilevamento di una backdoor che consente l'esecuzione remota di comandi, dando agli attaccanti un controllo potenzialmente illimitato sulla macchina compromessa.

# RIPARAZIONE PRIMA VULNERABILITÀ

## Cambio Password VNC (vncpasswd):

Ho aumentato la sicurezza del server VNC cambiando la password con una più forte e aggiungendo una password "solo visualizzazione".

Queste azioni hanno notevolmente ridotto la possibilità di accesso remoto non autorizzato.

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

# RIPARAZIONE SECONDA VULNERABILITÀ

## Configurazione di Tomcat:

Ho modificato la configurazione del connettore AJP per prevenire vulnerabilità come l'iniezione di richieste questo include la disabilitazione del connettore AJP o la sua configurazione in modo sicuro, seguito da un riavvio del servizio Tomcat per applicare le modifiche.

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS" />

-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!--<Connector port="8009"
          enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />-$

<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this. -->
<!--

[ Wrote 384 lines ]

msfadmin@metasploitable:~$ sudo service tomcat5.5 restart
sudo: service: command not found
msfadmin@metasploitable:~$ sudo /etc/init.d/tomcat5.5 restart
* Stopping Tomcat servlet engine tomcat5.5          [ OK ]
* Starting Tomcat servlet engine tomcat5.5          [ OK ]
msfadmin@metasploitable:~$ _
```



# RIPARAZIONE TERZA VULNERABILITÀ

Per affrontare la presenza di una backdoor di tipo bind shell, ho intrapreso un processo di mitigazione metodico, inizialmente, è importante comprendere che una backdoor bind shell è un tipo di malware configurato per ascoltare attivamente su una specifica porta TCP. Questo permette agli attaccanti di connettersi in remoto alla macchina compromessa e eseguire comandi arbitrari, quasi come se fossero seduti fisicamente di fronte al computer. Per eliminare questa minaccia, ho iniziato identificando il processo che manteneva aperta la porta sospetta, utilizzando netstat, ho potuto trovare il PID (Process ID) associato alla porta e successivamente ho esaminato i dettagli del processo per confermare la sua natura malevola. Dopo aver confermato che il processo era effettivamente parte della backdoor, ho proceduto con il terminare il processo utilizzando il comando kill. Successivamente, per prevenire la riattivazione della backdoor, ho cercato i file di configurazione o gli script di avvio automatico che potrebbero essere stati utilizzati per lanciare la backdoor al riavvio del sistema e li ho eliminati.

# SECONDA SCANSIONE

Questo screen mostra la scansione di mestasploitable dopo le azioni di riparazione ed evidenzia come sono state rimosse correttamente.

tenable

Nessus Essentials

Scans

Settings

?

🔔

lucagaspari

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

meta2

[Back to My Scans](#)

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities57

Remediations2

Notes2

History1

Filter

Search Vulnerabilities

57 Vulnerabilities

| <input type="checkbox"/> | Sev      | CVSS   | VPR | Name                            | Family                | Count |   |   |
|--------------------------|----------|--------|-----|---------------------------------|-----------------------|-------|---|---|
| <input type="checkbox"/> | CRITICAL | 10.0 * | 5.9 | NFS Exported Share Informa...   | RPC                   | 1     | 🔍 | ✎ |
| <input type="checkbox"/> | CRITICAL | 10.0   |     | Unix Operating System Uns...    | General               | 1     | 🔍 | ✎ |
| <input type="checkbox"/> | CRITICAL | 9.8    |     | SSL Version 2 and 3 Protocol... | Service detection     | 2     | 🔍 | ✎ |
| <input type="checkbox"/> | CRITICAL | ...    | ... | 2 SSL (Multiple Issues)         | Gain a shell remotely | 3     | 🔍 | ✎ |
| <input type="checkbox"/> | HIGH     | 7.5    | 5.9 | Samba Badlock Vulnerability     | General               | 1     | 🔍 | ✎ |
| <input type="checkbox"/> | HIGH     | 7.5    |     | NFS Shares World Readable       | RPC                   | 1     | 🔍 | ✎ |
| <input type="checkbox"/> | MIXED    | ...    | ... | 16 SSL (Multiple Issues)        | General               | 29    | 🔍 | ✎ |
| <input type="checkbox"/> | MIXED    | ...    | ... | 5 ISC Bind (Multiple Issues)    | DNS                   | 5     | 🔍 | ✎ |

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 6:11 AM

End:

Today at 6:34 AM

Elapsed:

24 minutes

Vulnerabilities

Critical

High

Medium

Low

Info