

Report Tecnico - Vulnerability Remediation su Metasploitable

1. Introduzione tecnica

Durante un'attività di penetration testing eseguita in ambiente controllato, è stata condotta un'analisi delle vulnerabilità sulla macchina target Metasploitable (IP 192.168.50.101) utilizzando il software **Nessus**. La prima scansione ha evidenziato diverse vulnerabilità critiche, successivamente confermate tramite strumenti come **Nmap**, **Netcat**, **VNCViewer** e altre tecniche di verifica manuale.

Sono state selezionate quattro vulnerabilità significative per procedere con un processo di remediation. Dopo l'applicazione delle contromisure, è stata eseguita una **nuova scansione con Nessus** per verificare l'effettiva risoluzione delle problematiche rilevate in precedenza.

Le vulnerabilità identificate erano:

- **Porta 1524:** presenza di una bind shell backdoor attiva.



```
(kali㉿kali)-[~]  
$ nc 192.168.50.101 1524  
root@metasploitable:/#
```

- **Porta 513:** servizio rlogin attivo, con autenticazione debole.

```

(kali㉿kali)-[~]
$ nmap -p 513 -sV 192.168.50.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 00:24 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
513/tcp   open  login
MAC Address: 08:00:27:EF:83:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

(kali㉿kali)-[~]
$

```

- **Porta 5900:** servizio VNC accessibile con password predefinita.

```

(kali㉿kali)-[~]
$ vncviewer 192.168.50.101:5900

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

(kali㉿kali)-[~]
$

```

- **Porta 8009:** vulnerabilità Ghostcat (AJP connector di Tomcat).

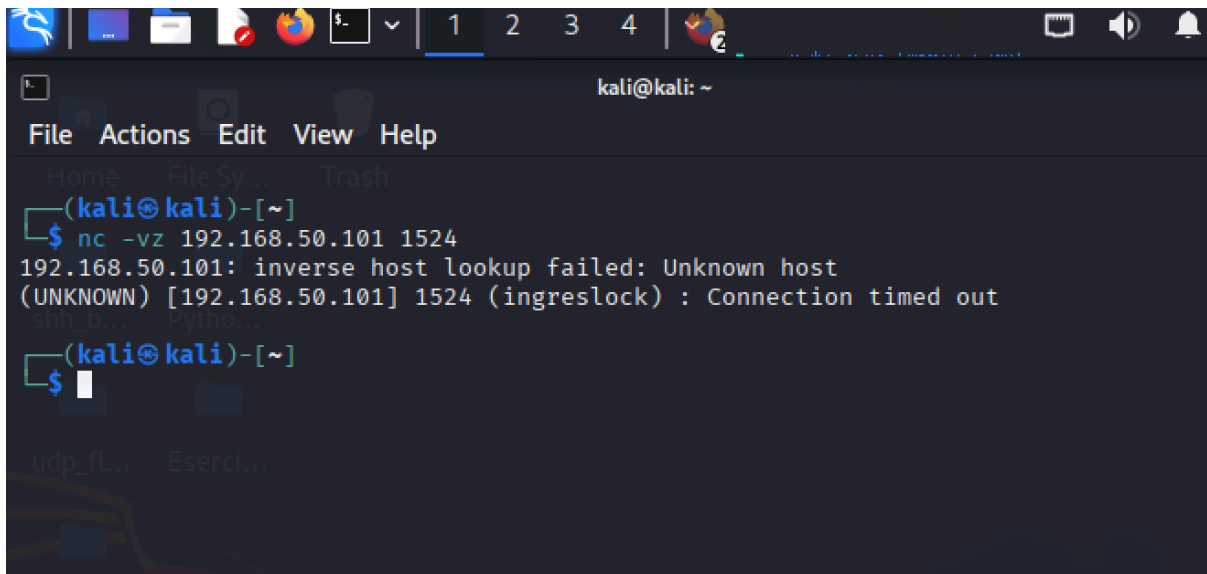
```
(kali㉿kali)-[~]  
$ nmap --script ajp-headers -p 8009 192.168.50.101  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 00:29 EDT  
Nmap scan report for 192.168.50.101  
Host is up (0.00096s latency).  
  
PORT      STATE SERVICE  
8009/tcp  open  ajp13  
| ajp-headers:  
|_ Content-Type: text/html;charset=ISO-8859-1  
MAC Address: 08:00:27:EF:83:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds  
  
(kali㉿kali)-[~]  
$
```

2. Dettaglio delle remediation eseguite

Vulnerabilità 1: Porta 1524 – Bind Shell

- **Metodo:** Blocco del traffico in ingresso tramite iptables.
Comando utilizzato:
`sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`
- **Verifica:** il servizio non ha più risposto alla connessione via Netcat. La porta risultava chiusa anche nella scansione finale con Nessus.

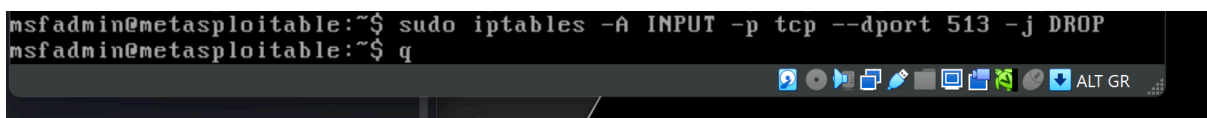
```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP  
msfadmin@metasploitable:~$
```



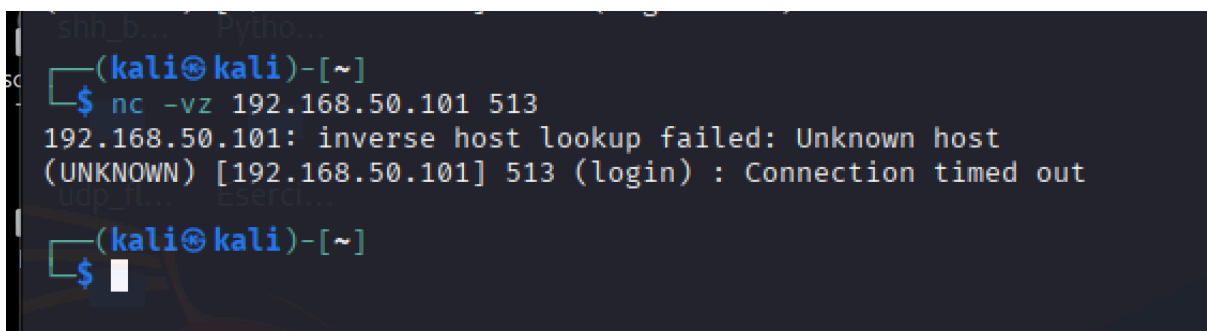
```
kali@kali: ~  
File Actions Edit View Help  
Home File Sy... Trash  
(kali@kali)-[~]  
$ nc -vz 192.168.50.101 1524  
192.168.50.101: inverse host lookup failed: Unknown host  
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection timed out  
(kali@kali)-[~]  
$
```

Vulnerabilità 2: Porta 513 – rlogin

- **Metodo:** Blocco del servizio tramite iptables.
Comando:
`sudo iptables -A INPUT -p tcp --dport 513 -j DROP`
- **Verifica:** la porta risultava non raggiungibile da Kali Linux tramite Netcat e non più rilevata nella successiva scansione Nessus.



```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 513 -j DROP  
msfadmin@metasploitable:~$ q
```



```
(kali@kali)-[~]  
$ nc -vz 192.168.50.101 513  
192.168.50.101: inverse host lookup failed: Unknown host  
(UNKNOWN) [192.168.50.101] 513 (login) : Connection timed out  
(kali@kali)-[~]  
$
```

Vulnerabilità 3: Porta 5900 – VNC con password debole

- **Metodo:** Modifica della password VNC tramite il comando `vncpasswd`, seguita da riavvio del servizio.
- **Verifica:** l'accesso remoto tramite la password debole è fallito e la vulnerabilità non è più stata segnalata da Nessus nel secondo test.

```
Meta2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Password too short
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
msfadmin@metasploitable:~$ sudo pkill Xtightvnc
msfadmin@metasploitable:~$ vncserver :0
xauth: creating new authority file /home/msfadmin/.Xauthority
New 'X' desktop is metasploitable:0
Creating default startup script /home/msfadmin/.vnc/xstartup
Starting applications specified in /home/msfadmin/.vnc/xstartup
Log file is /home/msfadmin/.vnc/metasploitable:0.log
msfadmin@metasploitable:~$
```

```
(kali@kali) [192.168.50.101] 315 (login) : Connection timed out
(kali@kali)-[~]
$ vncviewer 192.168.50.101:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
(kali@kali)-[~]
$
```

Vulnerabilità 4: Porta 8009 – Apache Ghostcat (CVE-2020-1938)

- **Metodo:** Blocco della porta tramite iptables.
Comando:
sudo iptables -A INPUT -p tcp --dport 8009 -j DROP
- **Verifica:** la scansione finale con Nessus ha mostrato che la porta era chiusa/filtrata e non più vulnerabile.

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 8009 -j DROP
msfadmin@metasploitable:~$ Q
```

Authentication Failure

```
(kali㉿kali)-[~]
$ nmap -p 8009 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 01:05 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0020s latency).

PORT      STATE      SERVICE
8009/tcp   filtered  ajp13
MAC Address: 08:00:27:EF:83:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

(kali㉿kali)-[~]
$
```

3. Sintesi divulgativa per non addetti ai lavori

Durante il test di sicurezza su una macchina vulnerabile chiamata Metasploitable, sono state individuate quattro gravi falle di sicurezza. Queste vulnerabilità permettevano, tra le altre cose, di accedere al sistema come amministratore, di vedere lo schermo remoto del computer o di eseguire comandi da remoto senza autorizzazione.

Abbiamo eseguito un primo controllo con un programma specializzato chiamato **Nessus**, che ci ha mostrato in quali punti il sistema era debole. Dopo aver preso contromisure tecniche mirate (chiusura di porte non sicure e modifica delle credenziali), abbiamo rieseguito lo stesso test e verificato che le vulnerabilità non erano più presenti.

Queste operazioni dimostrano quanto sia importante eseguire test regolari e aggiornamenti di sicurezza per proteggere sistemi e dati da accessi non autorizzati.

4. Integrazione PfSense

È opportuno evidenziare che tre delle quattro remediation applicate localmente su Metasploitable tramite iptables (relative alle porte TCP 1524, 513 e 8009) avrebbero potuto essere implementate anche a livello di firewall perimetrale mediante pfSense. L'interfaccia di configurazione di pfSense consente la creazione di regole granulari basate su indirizzi IP, protocolli e porte. In particolare, per ottenere un effetto equivalente, sarebbero state necessarie tre regole di tipo "block" o "reject" nella sezione:

Firewall > Rules > [interfaccia LAN], configurate come segue:

- **Regola 1**
Action: Block
Protocol: TCP
Destination: 192.168.50.101
Destination Port: 1524
Description: Blocco bind shell backdoor
- **Regola 2**
Action: Block
Protocol: TCP
Destination: 192.168.50.101
Destination Port: 513
Description: Blocco servizio rlogin
- **Regola 3**
Action: Block
Protocol: TCP
Destination: 192.168.50.101
Destination Port: 8009
Description: Blocco connettore AJP Tomcat (Ghostcat)

Le regole firewall configurate tramite pfSense sono **persistenti** e vengono automaticamente applicate a ogni riavvio, garantendo un livello di protezione centralizzato e gestibile tramite interfaccia grafica. Tuttavia, pfSense opera esclusivamente a livello di rete e non consente interventi diretti sulla configurazione interna dei servizi attivi sul sistema target. Per tale motivo, remediation come la modifica della password del servizio VNC (porta 5900) devono necessariamente essere applicate localmente. In contesti reali, l'approccio più efficace prevede la combinazione di configurazioni firewall a livello di rete (pfSense) e hardening locale (iptables, configurazione dei servizi) per garantire una difesa stratificata.