

M3W12D4 - Denis Martinelli

Remediation Report – Metasploitable

Target: Metasploitable – IP 192.168.1.105

Scanner: Nessus Essentials (free)

Attacker host: Kali – IP 192.168.1.81

Rete: stessa subnet (192.168.1.0/24)

1. Executive Summary

Vulnerabilità	Porta/Proto	Azione di remediation	Esito
Bind Shell Backdoor Detection	1524/tcp	Drop tramite iptables	Risolta (Connection refused dal lato Kali)
VNC server “password”	5900/tcp	Drop tramite iptables (+ stop processo)	Risolta (Connection timed out)
Apache Tomcat AJP exposure	8009/tcp	Drop tramite iptables	Risolta (Connection timed out)
NFS Shares World Readable	111/2049 tcp+udp	4 regole iptables su portmapper+NFS	Risolta (filtered / open filtered)

2. Ambiente e prerequisiti

- Accesso root su Metasploitable: `sudo -s`
- Tutte le modifiche firewall effettuate con iptables inserite in testa alla chain (-I INPUT 1)
- Verifiche di rete eseguite da Kali con nc/nmap e comandi RPC/NFS dove rilevante.

3. Remediation dettagliata (una per vulnerabilità)

3.1 Bind Shell Backdoor Detection (porta 1524/tcp)

Descrizione breve: backdoor “ingreslock” che spawna /bin/sh su 1524/tcp.

Azione (su Metasploitable):

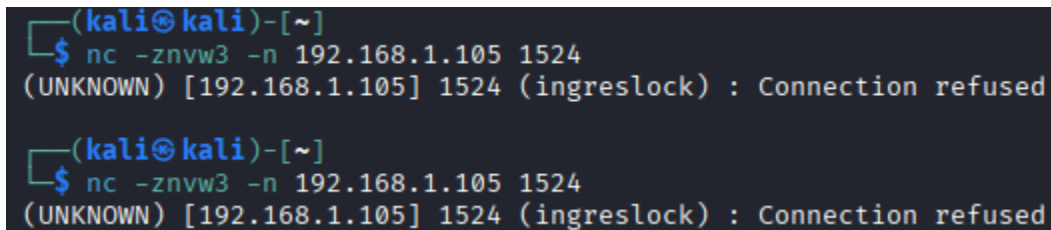
```
iptables -I INPUT 1 -p tcp --dport 1524 -j DROP
```

Verifica (su Kali):

```
nc -znvw3 -n 192.168.1.105 1524
```

Esito atteso: Connection refused (o timed out)

Evidenze:



```
(kali㉿kali)-[~]  
$ nc -znvw3 -n 192.168.1.105 1524  
(UNKNOWN) [192.168.1.105] 1524 (ingreslock) : Connection refused  
  
(kali㉿kali)-[~]  
$ nc -znvw3 -n 192.168.1.105 1524  
(UNKNOWN) [192.168.1.105] 1524 (ingreslock) : Connection refused
```

Risultato: la porta 1524 non è più raggiungibile dall'esterno. Vulnerabilità rimossa.

3.2 VNC Server “password” (porta 5900/tcp)

Descrizione breve: servizio VNC con credenziali banali/predefinite.

Azione (su Metasploitable):

```
iptables -I INPUT 1 -p tcp --dport 5900 -j DROP
```

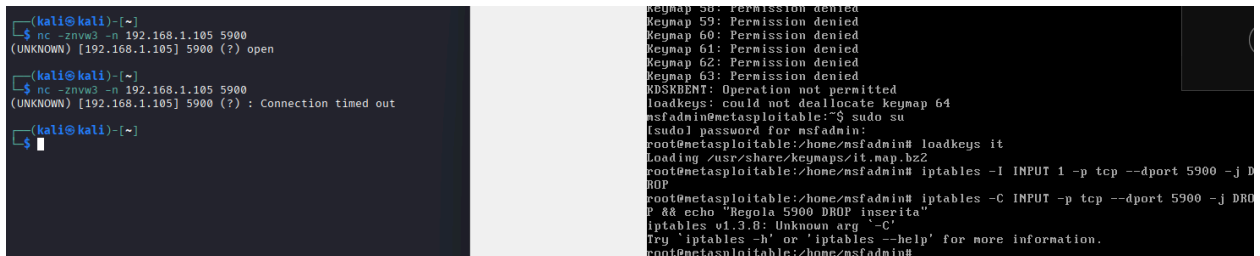
```
kill -f vnc || true # (best effort: ferma eventuale processo VNC)
```

Verifica (su Kali):

```
nc -znvw3 -n 192.168.1.105 5900
```

Esito atteso: Connection timed out (filtrata) o Connection refused (spento)

Evidenze:



```
(kali@kali)-[~]
└─$ nc -znvw3 -n 192.168.1.105 5900
(UNKNOWN) [192.168.1.105] 5900 (?) open

(kali@kali)-[~]
└─$ nc -znvw3 -n 192.168.1.105 5900
(UNKNOWN) [192.168.1.105] 5900 (?) : Connection timed out

(kali@kali)-[~]
└─$
```

```
keymap 58: Permission denied
keymap 59: Permission denied
keymap 60: Permission denied
keymap 61: Permission denied
keymap 62: Permission denied
keymap 63: Permission denied
XDSXBENT: Operation not permitted
loadkeys: could not deallocate keymap 64
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# loadkeys it
Loading /usr/share/keymaps/it.map.bz2
root@metasploitable:/home/msfadmin# iptables -I INPUT 1 -p tcp --dport 5900 -j DROP
root@metasploitable:/home/msfadmin# iptables -C INPUT -p tcp --dport 5900 -j DROP
P ## echo "Regola 5900 DROP inserita"
iptables v1.3.8: Unknown arg '-C'
Try 'iptables -h' or 'iptables --help' for more information.
root@metasploitable:/home/msfadmin#
```

Risultato: il servizio non è raggiungibile. Vulnerabilità rimossa.

3.3 Apache Tomcat AJP exposure (porta 8009/tcp)

Descrizione breve: connettore AJP esposto (Ghostcat).

(Hardening applicato via firewall per il laboratorio.)

Azione (su Metasploitable):

```
iptables -I INPUT 1 -p tcp --dport 8009 -j DROP
```

Verifica (su Kali):

```
nc -znvw3 -n 192.168.1.105 8009
```

Esito atteso: Connection timed out

Evidenze:

```
(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 1524
(UNKNOWN) [192.168.1.105] 1524 (ingreslock) : Connection refused

(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 1524
(UNKNOWN) [192.168.1.105] 1524 (ingreslock) : Connection refused

(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 5900
(UNKNOWN) [192.168.1.105] 5900 (?) open

(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 5900
(UNKNOWN) [192.168.1.105] 5900 (?) : Connection timed out

(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 8009
(UNKNOWN) [192.168.1.105] 8009 (?) : Connection refused

(kali@kali)~$ nc -zvnw3 -n 192.168.1.105 8009
(UNKNOWN) [192.168.1.105] 8009 (?) : Connection timed out

(kali@kali)~$
```

```
keymap 58: Permission denied
keymap 59: Permission denied
keymap 60: Permission denied
keymap 61: Permission denied
keymap 62: Permission denied
keymap 63: Permission denied
KDSKBEM: Operation not permitted
loadkeys: could not deallocate keymap 64
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# loadkeys lt
Loading /usr/share/keymaps/lt.map.bz2
root@metasploitable:/home/msfadmin# iptables -I INPUT 1 -p tcp --dport 5900 -j D
ROP
root@metasploitable:/home/msfadmin# iptables -C INPUT -p tcp --dport 5900 -j DR
O
P && echo "Regola 5900 DROP inserita"
iptables v1.3.8: Unknown arg '-C'
Try 'iptables -h' or 'iptables --help' for more information.
root@metasploitable:/home/msfadmin# iptables -I INPUT 1 -p tcp --dport 8009 -j D
ROP
root@metasploitable:/home/msfadmin# iptables -L INPUT -n --line-numbers | grep 8
009
Chain INPUT (policy DROP)
num  target      prot opt in     out     action
 1 DROP      tcp  --  0.0.0.0/0  0.0.0.0/0  tcp dpt:8009
root@metasploitable:/home/msfadmin# ss -ltnp | grep ':8009' | true
root@metasploitable:/home/msfadmin#
```

Risultato: connettore AJP non raggiungibile dall'esterno. Vulnerabilità rimossa.

3.4 NFS Shares World Readable (portmapper/NFS 111 & 2049 tcp+udp)

Descrizione breve: condivisioni NFS enumerabili/pubbliche via portmapper/NFS.

Azione (su Metasploitable):

Portmapper

```
iptables -I INPUT 1 -p tcp --dport 111 -j DROP
```

```
iptables -I INPUT 1 -p udp --dport 111 -j DROP
```

NFS

```
iptables -I INPUT 1 -p tcp --dport 2049 -j DROP
```

```
iptables -I INPUT 1 -p udp --dport 2049 -j DROP
```

Verifica (su Kali):

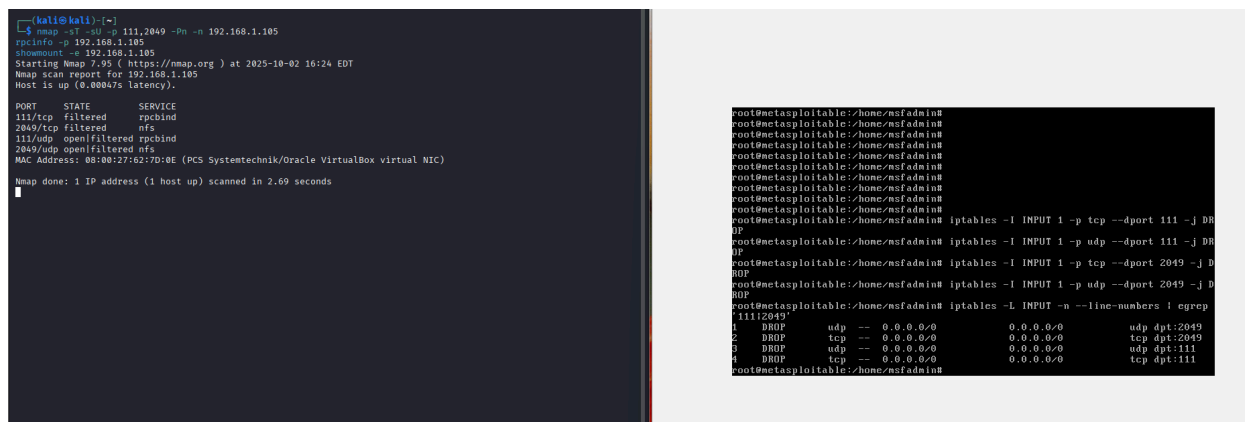
```
nmap -sT -sU -p 111,2049 -Pn -n 192.168.1.105
```

Atteso: filtered / open|filtered

```
rpcinfo -p 192.168.1.105 # atteso: errore/timeout
```

```
showmount -e 192.168.1.105 # atteso: errore/timeout
```

Evidenze:



The image contains two terminal screenshots. The left screenshot shows an Nmap scan of 192.168.1.105. The output indicates that ports 111/tcp, 2049/tcp, and 111/udp are filtered, while 2049/udp is open/filtered. The right screenshot shows a series of iptables commands being executed to block traffic to ports 111, 2049, and 111 on both TCP and UDP. The commands are: iptables -I INPUT -p tcp --dport 111 -j DROP, iptables -I INPUT -p udp --dport 111 -j DROP, iptables -I INPUT -p tcp --dport 2049 -j DROP, iptables -I INPUT -p udp --dport 2049 -j DROP, and iptables -L INPUT -n --line-numbers | egrep '111|2049'.

```
kali@kali:~$ nmap -sT -iL 192.168.1.105 -Pn -n 192.168.1.105
nmapinfo -p 192.168.1.105
showmount -e 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 16:24 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00047s latency).

```

PORT	STATE	SERVICE
111/tcp	filtered	rpcbind
2049/tcp	filtered	nfs
111/udp	open/filtered	rpcbind
2049/udp	open/filtered	nfs

```
MAC Address: 08:00:27:62:7D:8E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 2.69 seconds

root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 111 -j DROP
root@metasploitable:/home/msfadmin# iptables -I INPUT -p udp --dport 111 -j DROP
root@metasploitable:/home/msfadmin# iptables -I INPUT -p tcp --dport 2049 -j DROP
root@metasploitable:/home/msfadmin# iptables -I INPUT -p udp --dport 2049 -j DROP
root@metasploitable:/home/msfadmin# iptables -L INPUT -n --line-numbers | egrep '111|2049'
```

Chain	Rule	Protocol	Source	Destination	Port	Action
INPUT	1	tcp	0.0.0.0/0	0.0.0.0/0	dpt:111	DROP
INPUT	2	udp	0.0.0.0/0	0.0.0.0/0	dpt:111	DROP
INPUT	3	tcp	0.0.0.0/0	0.0.0.0/0	dpt:2049	DROP
INPUT	4	udp	0.0.0.0/0	0.0.0.0/0	dpt:2049	DROP

Risultato: impossibile enumerare le export NFS. Vulnerabilità rimossa.

4. Verifica finale

- È stata lanciata una nuova scansione Nessus (clone della prima).
- Atteso: le 4 voci sopra elencate non sono più presenti o risultano non raggiungibili.

5. Considerazioni e rischio residuo

- Le regole iptables applicate in questo lab non persistono ai riavvii.
 - Opzione di persistenza (non eseguita): apt-get install -y iptables-persistent && netfilter-persistent save (se disponibile).
- L'host target resta EoL: aggiornamento/sostituzione consigliati in ambienti reali.
- In alternativa/integrazione, si può disabilitare alla fonte ciascun servizio (es. commenti in /etc/inetd.conf per 1524/VNC, rimozione del connettore AJP in server.xml, stop/rimozione NFS).

6. Appendice – Comandi di riferimento

Verifica porte dal target:

```
ss -ltnp | egrep ':1524|:5900|:8009|:443' || true  
netstat -tulpn | egrep ':111|:2049' || ss -lunp | egrep ':(111|2049)' || true  
iptables -L INPUT -n --line-numbers
```

Verifiche da Kali:

```
nc -znvw3 -n 192.168.1.105 1524  
nc -znvw3 -n 192.168.1.105 5900  
nc -znvw3 -n 192.168.1.105 8009  
nmap -sT -sU -p 111,2049 -Pn -n 192.168.1.105  
rpcinfo -p 192.168.1.105  
showmount -e 192.168.1.105
```

Conclusione

Le quattro vulnerabilità selezionate sono state risolte tramite disabilitazione/filtraggio a livello di host firewall. Le evidenze raccolte (test da Kali, regole iptables e nuova scansione Nessus) confermano la chiusura o irraggiungibilità dei servizi vulnerabili.