

# Report sulla Risoluzione delle Vulnerabilità nella VM Metasploitable

In questo report, descriverò come ho risolto le vulnerabilità trovate da Nessus nella macchina virtuale Metasploitable. Le vulnerabilità riguardano la rilevazione del servizio rexecd, la divulgazione delle informazioni sulle condivisioni esportate tramite nsf e la vulnerabilità della password del server VNC. Spiegherò brevemente ciascuna vulnerabilità e le azioni che ho intrapreso per risolverle.

## Vulnerabilità 1: Rilevazione del servizio rexecd

```
GNU nano 2.0.7      File: inetd.conf      Modified
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet               stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tel
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                 dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tft
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogi
#exec                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rex
ingreslock stream tcp nowait root /bin/bash bash -i

[ Read 8 lines ]
^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text    ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

Il servizio rexecd è un servizio che permette di eseguire comandi su un computer remoto. È possibile sfruttare questo servizio per ottenere accesso non autorizzato al sistema. Per risolvere questa vulnerabilità, ho seguito il consiglio di Nessus e ho commentato la riga corrispondente nel file inetd.conf. In pratica, ho disabilitato il servizio rexecd nel sistema, impedendo a eventuali attaccanti di sfruttarlo.

## Vulnerabilità 2: Divulgazione delle informazioni sulle condivisioni esportate tramite nsf

```
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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes   gss/krb5i(rw,sync)
#
# *(rw,sync,no_root_squash,no_subtree_check)
/ 192.168.50.101(ro)
```

```
(kali@kali)-[~]
$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ *

(kali@kali)-[~]
$ showmount -e 192.168.50.101
Export list for 192.168.50.101:
/ 192.168.50.101
```

Questa vulnerabilità riguarda la divulgazione non autorizzata delle informazioni sulle condivisioni esportate tramite il servizio nfs. Un attaccante potrebbe ottenere accesso ai file e alle directory esposte, mettendo a rischio la sicurezza del sistema. Per risolvere questa vulnerabilità, ho modificato il file "exports" aggiungendo l'indirizzo IP della macchina Metasploitable come directory radice e ho commentato la riga precedente. In questo modo, ho limitato l'accesso alle condivisioni esportate solo alla macchina locale, impedendo agli attaccanti di sfruttare la vulnerabilità.

### Vulnerabilità 3: Vulnerabilità della password del server VNC

```
Loading /usr/share/keymaps/it.map.bzz
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev    initrd    lost+found    nohup.out    q?      srv    usr
boot   etc    initrd.img    media        opt          root    sys    var
cdrom  home  lib       mnt          proc         sbin    tmp    vmlinuz
msfadmin@metasploitable:/$ sudo su
root@metasploitable:/# cd /root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd .vnc
root@metasploitable:~/vnc# ls
metasploitable:0.log  metasploitable:1.log  passwd
metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/vnc# cat passwd
epicode
root@metasploitable:~/vnc#
```

Questa vulnerabilità riguarda l'utilizzo di una password predefinita o debole per il server VNC, che potrebbe consentire a un attaccante di ottenere accesso non autorizzato al sistema. Per risolvere questa vulnerabilità, ho modificato la password nel file "passwd" utilizzato dal server VNC.

### Vulnerabilità 4: Rilevamento della backdoor Bind shell

```
GNU nano 2.0.7      File: /etc/inetd.conf
#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
telnet                stream  tcp    nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.tel
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                 dgram  udp    wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tft
shell                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
#exec                stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
#ingreslock stream tcp nowait root /bin/bash bash -i
```

La quarta vulnerabilità riguarda la presenza di una backdoor Bind shell sulla macchina Metasploitable. Una Bind shell è una porta segreta che consente agli attaccanti di ottenere un accesso non autorizzato al sistema. Questa backdoor consente loro di eseguire comandi sul sistema compromesso a loro discrezione. Per risolvere questa vulnerabilità, ho modificato il file di configurazione appropriato, commentando la riga relativa al servizio "ingreslock stream". Questo ha impedito alla backdoor Bind shell di funzionare, rendendo impossibile l'accesso non autorizzato attraverso questa vulnerabilità.

## Vulnerabilità 5: Connessione Apache Tomcat AJP

```
GNU nano 2.0.7      File: server.xml      Modified
    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" sec$
<!-- Define a Proxy HTTP/1.1 Connector on port 8082 -->
```

La quinta vulnerabilità che ho individuato riguarda il connettore AJP di Apache Tomcat. Il connettore AJP è un modo per far comunicare il server web Apache con il server Tomcat, ma può creare dei problemi di sicurezza se non viene configurato correttamente. Per risolvere questa vulnerabilità, ho disabilitato completamente il connettore AJP, in modo che non fosse più possibile comunicare tramite il protocollo AJP. Questo significa che non sarà più possibile sfruttare la vulnerabilità conosciuta come "Ghostcat" attraverso il connettore AJP. Disabilitando questa funzionalità, ho eliminato un possibile punto di ingresso per gli attaccanti, aumentando la sicurezza complessiva del sistema.