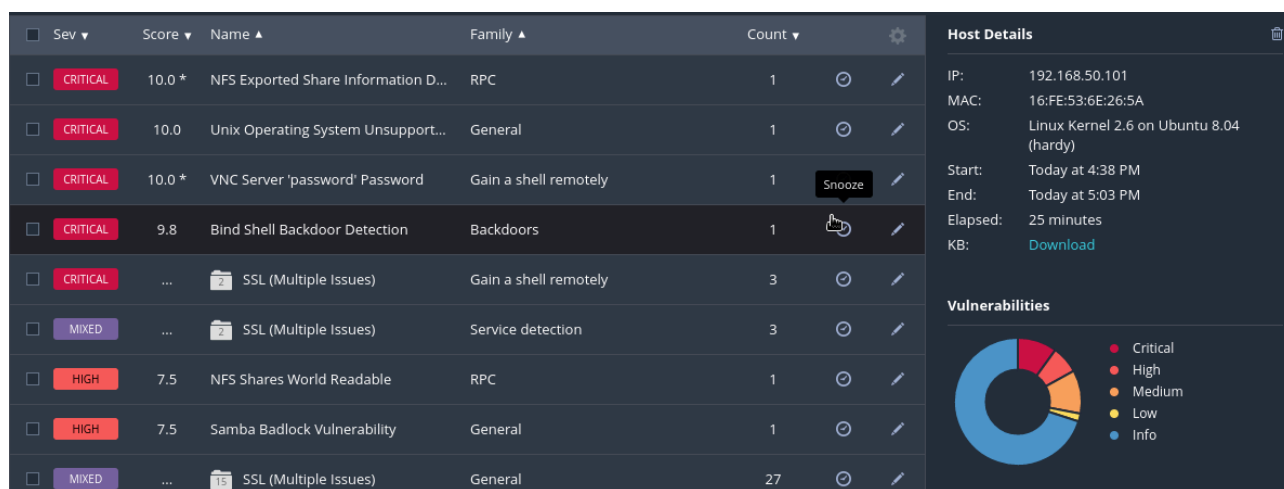


Relazione Progetto

Le scansioni d'oggi le andremo a fare con il vulnerability scanner di Nessus, con questo scanner andremo a fare una scansione completa del sistema di metasploitable.

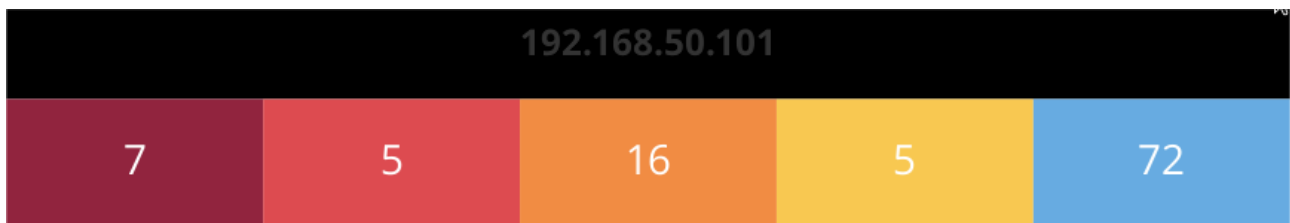
Scansione Iniziale

Con la scansione iniziale si va verificare quali sono le problematiche che presenta Metasploitable.



Con questa prima scansione ci mostra tutte le vulnerabilità che ha riscontrato nella nostra macchina, in questo caso metasploitable.

Sev	Score	Name	Family	Count	
CRITICAL	10.0 *	NFS Exported Share Information D...	RPC	1	
CRITICAL	10.0	Unix Operating System Unsupport...	General	1	
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	
CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	...	2 SSL (Multiple Issues)	Service detection	3	
HIGH	7.5	NFS Shares World Readable	RPC	1	
HIGH	7.5	Samba Badlock Vulnerability	General	1	
MIXED	...	15 SSL (Multiple Issues)	General	27	



Le vulnerabilità che troviamo sono:

- 👉 Info
- 👉 Low
- 👉 Medium
- 👉 High
- 👉 Critical

Le vulnerabilità più pericolose per il nostro sistema sono le “Critical” queste sono quelle più dannose per il nostro sistema e sono quelle sulle quali siamo andati ad agire.

Una delle vulnerabilità critiche che troviamo è quella **VNC Server** ‘password’

CRITICAL VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
Secure the VNC service with a strong password.

Output
Nessus logged in using a password of "password".

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

Per risolvere questo problema mi sono basato sulla descrizione del problema il quale chiede che la sorgente di vnc necessita una password forte.

```

[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd .vnc
root@metasploitable:/home/msfadmin/.vnc# ls
metasploitable:1.log  metasploitable:1.pid  passwd  xstartup
root@metasploitable:/home/msfadmin/.vnc# 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/.vnc#

```

Come si può vedere dall'immagine nella pagina precedente possiamo migliorare la sicurezza andando a fare delle modifiche nella macchina attaccata:

1. Con il comando sudo su entriamo nella sezione d'amministratore.
2. Con cd .vnc entriamo nella cartella
3. Con il ls verifichiamo se il file che stiamo cercando è all'interno
4. Dopo aver selezionato il file che ci serve andiamo modificare la password, la quale ci verrà fatta una richiesta di verifica
5. Dopo aver verificato la password ci chiederà se vogliamo che la password sia visibile, noi selezioniamo "n"

Come possiamo vedere nell'immagine non presenta più la vulnerabilità di prima.

<input type="checkbox"/>	Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼		⚙
<input type="checkbox"/>	CRITICAL	10.0 *	Debian Op...	Gain a shell remotely	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0 *	NFS Export...	RPC	1	🕒	✎
<input type="checkbox"/>	CRITICAL	10.0	Unix Opera...	General	1	🕒	✎
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell ...	Backdoors	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	NFS Shares...	RPC	1	🕒	✎
<input type="checkbox"/>	HIGH	7.5	Samba Bad...	General	1	🕒	✎
<input type="checkbox"/>	MIXED	...	ISC Bi...	DNS	5	🕒	✎
<input type="checkbox"/>	MEDIUM	5.3	SMB Signin...	Misc.	1	🕒	✎

Un'altra delle vulnerabilità critiche che troviamo è quella **Band Shell Backdoor Detection**

CRITICAL Bind Shell Backdoor Detection < >

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.50.101

Questo problema ci dice che un attaccante può essere in ascolto sulla porta, per migliorare le difese della macchina bisogna andare a mettere un firewall sulla macchina (Porta 1524), come si può vedere nella immagine di sotto:

```
root@metasploitable:/home/msfadmin# ufw

Usage: ufw COMMAND

Commands:
  enable                Enables the firewall
  disable               Disables the firewall
  default ARG           set default policy to ALLOW or DENY
  logging ARG           set logging to ON or OFF
  allow|deny RULE       allow or deny RULE
  delete allow|deny RULE delete the allow/deny RULE
  status                show firewall status
  version               display version information

root@metasploitable:/home/msfadmin# ufw disable
Firewall stopped and disabled on system startup
root@metasploitable:/home/msfadmin# ufw enable 1524
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rules updated
root@metasploitable:/home/msfadmin# _
```

