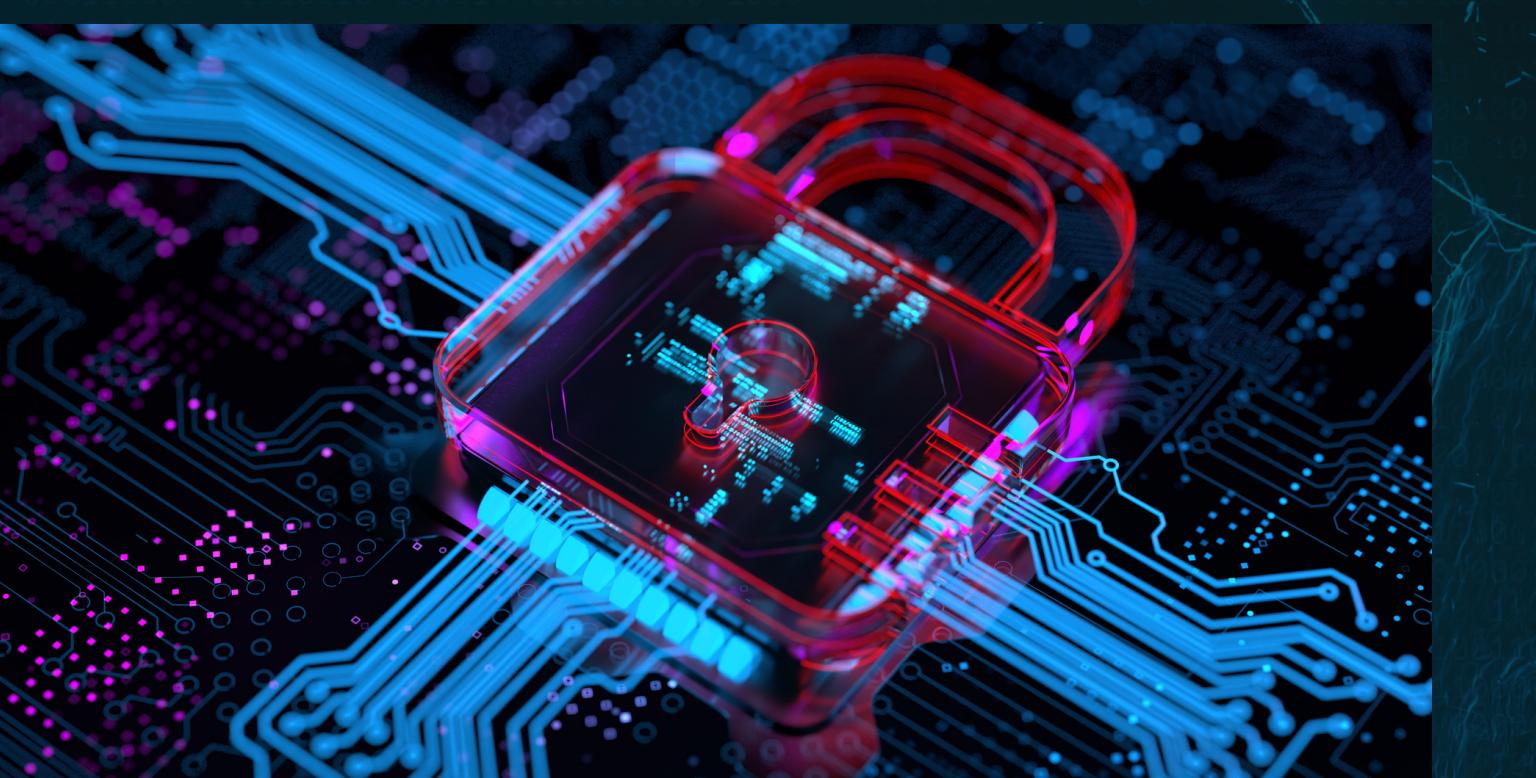


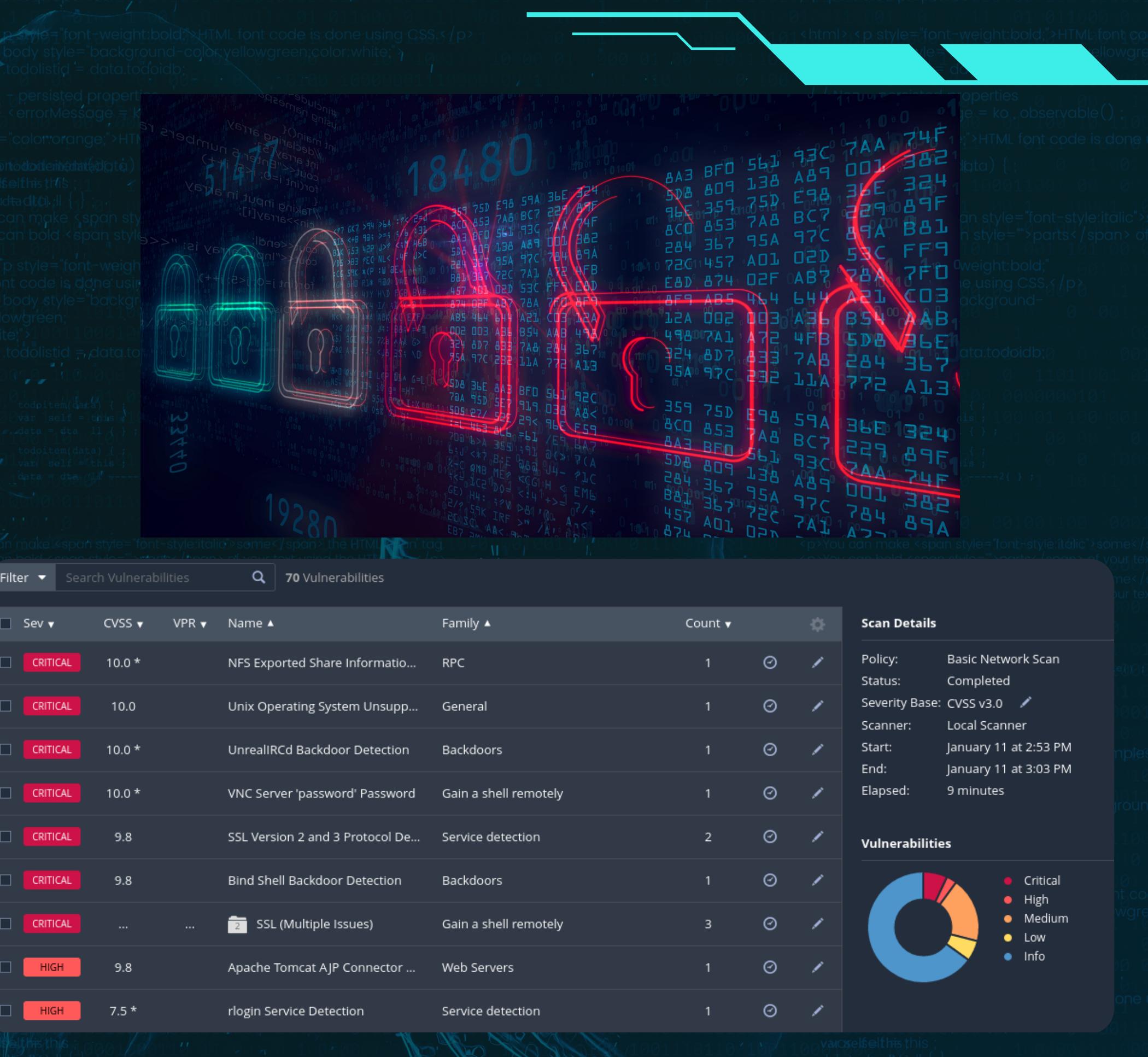


PROGETTO S5/L5





Nel progetto di oggi andremo a vedere alcune criticità rilevate da Nessus, un software di vulnerability scan, sulla macchina Metasploitable 2. Nessus a seguito di una scansione ci mette a disposizione una tabella con tutte le vulnerabilità da lui rilevate, andandole a catalogare in base al livello di criticità che rappresentano. Una volta analizzata la situazione andremo ad apportare delle soluzioni per risolvere queste criticità, infine proveremo nuovamente ad avviare una scansione del sistema per confermare che le nostre azione abbiano portato il risultato aspettato.



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 -----  
  
To see debug logs, please visit individual host
```

Port ▾	Hosts
1524 / tcp / wild_shell	192.168.1.104

Come prima vulnerabilità da risolvere ho scelto la Bind Shell Backdoor Detection, questo indica che un'interfaccia a riga di comando è in ascolto sulla porta 1524 e non è richiesta nessuna autenticazione per accedervi

Per risolvere questa vulnerabilità potrei agire in vari modi, considerato che attualmente non necessito di questo servizio ho pensato di andare a chiudere il servizio attualmente utilizzato su quella porta, in più potrei disabilitarlo per i successivi riavvii del sistema in modo che questa vulnerabilità non si ripresenti. Potrei inoltre risolvere il problema andando ad inserire le corrispettive autenticazioni nel caso in cui io necessiti di questo servizio.

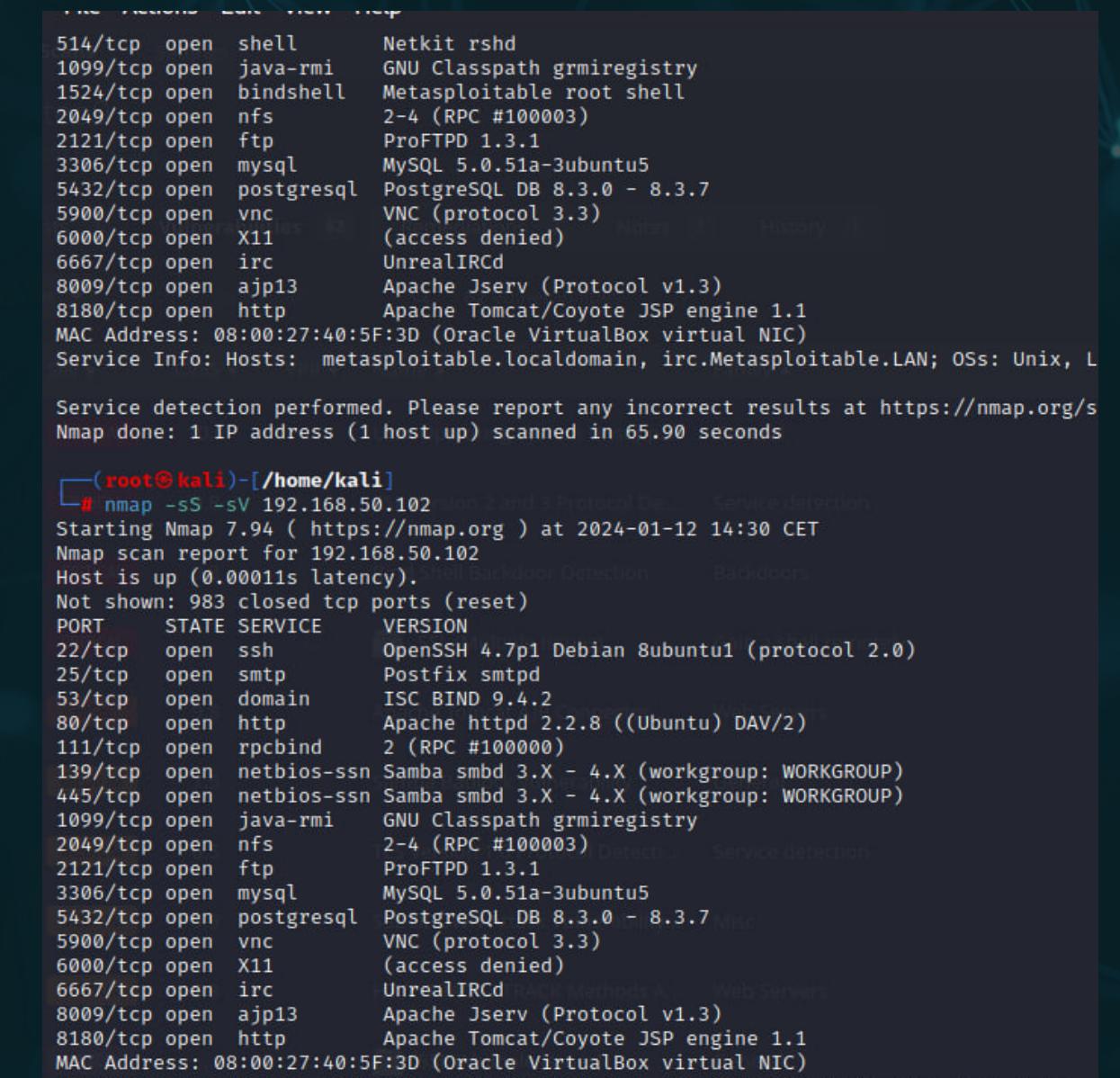
Conoscendo la porta sul quale si trova il servizio mi sono avvalso del comando riportato qui di fianco per andare ad individuare il PID del processo riguardante il servizio che voglio andare a chiudere

```
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
xinetd  4391 root    12u  IPv4 12002      TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin# kill 4391
root@metasploitable:/home/msfadmin# _
```

Una volta ottenuto il PID mi è bastato usare il comando "kill" seguito dal PID per andarlo a terminare, per avere un riscontro sullo stato attuale del servizio ho lanciato una scansione con nmap, come possiamo vedere nell'immagine qui riportata la porta "1524" non compare, mentre prima era presente

```
THE Nmap 7.94 scan tool. Version 7.94 ( https://nmap.org ) Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-12 14:30 CET Nmap scan report for 192.168.50.102 Host is up (0.00011s latency). Not shown: 983 closed tcp ports (reset) PORT      STATE SERVICE      VERSION 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) 25/tcp    open  smtp         Postfix smtpd 53/tcp    open  domain        ISC BIND 9.4.2 80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2) 111/tcp   open  rpcbind      2 (RPC #100000) 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 1099/tcp  open  java-rmi    GNU Classpath grmiregistry 2049/tcp  open  nfs          2-4 (RPC #100003) 2121/tcp  open  ftp          ProFTPD 1.3.1 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7 5900/tcp  open  vnc          VNC (protocol 3.3) 6000/tcp  open  X11          (access denied) 6667/tcp  open  irc          UnrealIRCd 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3) 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1 MAC Address: 08:00:27:40:5F:3D (Oracle VirtualBox virtual NIC) Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux  
Service detection performed. Please report any incorrect results at https://nmap.org/servicedetect Nmap done: 1 IP address (1 host up) scanned in 65.90 seconds
```

```
[root@kali)-[~/home/kali]# nmap -sS -sV 192.168.50.102
```



CRITICAL NFS Exported Share Information Disclosure

< >

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :
```

```
+ /  
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
- etc  
- home  
- initrd  
- initrd.img  
- lib  
- lost+found  
- media  
- mnt  
- nohup.out  
- opt  
- proc  
- root  
- sbin  
- srv  
- sys  
- tmp
```

Dopo aver risolto la precedente vulnerabilità ho deciso di spostare la mia attenzione su NFS Exported Share Information Disclosure, ciò indica che tramite il protocollo di rete NFS il sistema permette di manipolare ciò che è contenuto nella directory "/" ad host esterni, in quanto non sono presenti le giuste autorizzazioni.

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(ro,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4      gss/krb5i(ro,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(ro,sync)
#
# *(ro,sync,no_subtree_check)
```

[Read 12 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

CTRL (DESTRA)

Per evitare ciò sono andato tramite la macchina Metasploitable 2 nel file che si occupa della gestione della condivisione tramite il protocollo NFS dei file e delle directory, per evitare questa vulnerabilità potrei agire su questo file in molti modi, ma considerando che attualmente non necessito del servizio mi sono limitato a mettere come commento la condivisione che creava la precedente vulnerabilità, così facendo questa condivisione non sarà più presente

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.

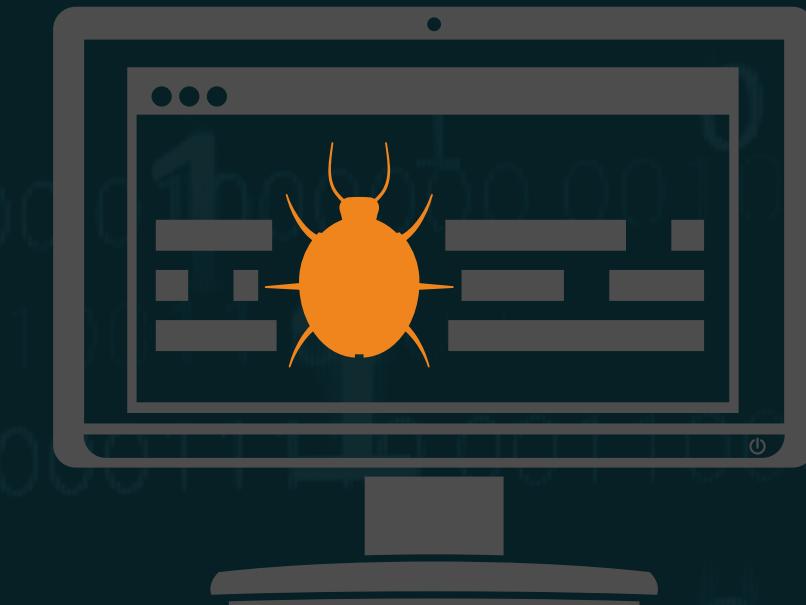
Output

```
Nessus logged in using a password of "password".  
To see debug logs, please visit individual host  
Port ▲ Hosts  
5900 / tcp / vnc 192.168.1.104
```

L'ultima vulnerabilità che andremo ad affrontare oggi è VNC Server 'password' Password, questo sta a indicare che il server VNC in esecuzione sull'host è protetto da una password debole, in questo caso "password", questo server consente l'accesso remoto a un computer da un altro dispositivo tramite una connessione di rete

Il modo più veloce con il quale posso andare a mettere in sicurezza questa vulnerabilità è quella di impostare una password più sicura, ciò può essere fatto eseguendo un semplice comando da macchina

Metasploitable 2



```
msfadmin@metasploitable:~$ sudo vncpasswd
[sudo] password for msfadmin:
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$ _
```

A seguito di queste operazioni non ci rimane che controllare se i nostri interventi hanno ricevuto il risultato gradito, di seguito il confronto tra le tabelle di Nessus prima degli interventi e dopo, come possiamo notare le vulnerabilità oggetto di risoluzione sono andate a buon fine.

	Sev	CVSS	VPR	Name	Family
<input type="checkbox"/>	CRITICAL	10.0 *		NFS Exported Share Informatio...	RPC
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupp...	General
<input type="checkbox"/>	CRITICAL	10.0 *		UnrealIRCd Backdoor Detection	Backdoors
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol De...	Service detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	HIGH	9.8		Apache Tomcat AJP Connector ...	Web Servers
<input type="checkbox"/>	HIGH	7.5 *		rlogin Service Detection	Service detection
<input type="checkbox"/>	HIGH	7.5 *		rsh Service Detection	Service detection
<input type="checkbox"/>	MIXED	DNS (Multiple Issues)	DNS

	Sev	CVSS	VPR	Name	Family
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupp...	General
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol De...	Service detection
<input type="checkbox"/>	CRITICAL	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/>	HIGH	9.8		Apache Tomcat AJP Connector ...	Web Servers
<input type="checkbox"/>	MEDIUM	7.5		Samba Badlock Vulnerability	General
<input type="checkbox"/>	MEDIUM	6.5		TLS Version 1.0 Protocol Detecti...	Service detection
<input type="checkbox"/>	MEDIUM	5.9		SSL DROWN Attack Vulnerability...	Misc.
<input type="checkbox"/>	MEDIUM	5.3		HTTP TRACE / TRACK Methods A...	Web Servers
<input type="checkbox"/>	MIXED	SSL (Multiple Issues)	General
<input type="checkbox"/>	MIXED	SSH (Multiple Issues)	Misc.
<input type="checkbox"/>	MIXED	ISC Bind (Multiple Issues)	DNS