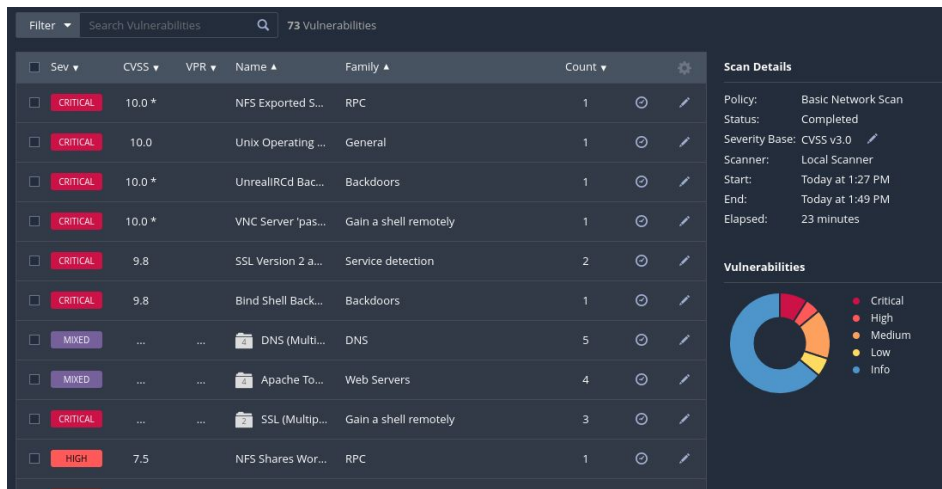




# Progetto S5-L5

# Nessus

Dopo aver completato questa procedura, possiamo visualizzare un elenco delle vulnerabilità, ognuna classificata con un livello di pericolo che può essere 'Info', 'Low', 'Medium', 'High', o 'Critical'. Le vulnerabilità classificate come 'Critical' sono quelle che dovremmo risolvere prioritariamente.



# Nessus

In questo caso, abbiamo identificato una password piuttosto debole nel VNC server, (immagina di avere un computer (il server) e vuoi accedere e controllare il suo desktop da un altro computer (il client) situato in un luogo diverso), e attraverso una simulazione di attacco, Nessus è riuscito a penetrare facilmente. . La soluzione consigliata sarebbe quindi di utilizzare una password robusta.

CRITICAL

VNC Server 'password' Password

< >

Plugin Details

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	192.168.1.168

Severity: Critical

ID: 61708

Version: \$Revision: 1.2 \$

Type: remote

Family: Gain a shell remotely

Published: August 29, 2012

Modified: September 24, 2015

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

# Nessus

Andiamo su metasploitable e inseriamo i vari comandi dove su **password** e **verify** andiamo a scegliere la nuova password. Dopo facciamo un sudo reboot.

```
root@metasploitable:/home/msfadmin# sudo su
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# sudo reboot
```

Filter ▼ VNC

1 of 70 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/>	INFO	...	...	VNC (Multiple Issues)	Service detection	3	🕒 ✎

Results per page 50

Showing: 1 to 1 of 1

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0 ✎

Scanner:

Local Scanner

Start:

Today at 6:31 AM

End:

Today at 6:53 AM

Elapsed:

22 minutes



# Nessus

NFS (Network File System) è un protocollo che consente di condividere file e risorse tra computer su una rete. In questo caso, abbiamo un dispositivo remoto che potrebbe essere facilmente attaccato, aumentando il rischio di perdita, rimozione o modifica dei file da parte di un black hat. Per prevenire questo problema, è sufficiente modificare il dispositivo in modo tale che siano autorizzati solo i dispositivi da noi desiderati.

**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
```

**Plugin Details**

Severity:	Critical
ID:	11356
Version:	1.21
Type:	remote
Family:	RPC
Published:	March 12, 2003
Modified:	August 30, 2023

**Risk Information**

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C  
/I:C/A:C

# Nessus

Per questo è po più complicato, scrivere prima il comando `sudo nano /etc/exports` ed andiamo a scrivere una nuova riga sotto.

```
/home/user/share *(rw,sync,no_root_squash,no_subtree_check)
192.168.1.167(rw,sync,no_root_squash)
```

dove la prima parte è la cartella in cui andiamo a salvare e l'ip sono gli host autorizzati, se mettete un \* qualsiasi host è autorizzato. Dopo riavviamo con un `sudo reboot`.

Filter ▼ NFS 2 of 70 Vulnerabilities						Scan Details	
Sev ▼	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1	Policy:	Basic Network Scan
						Status:	Completed
<input type="checkbox"/> INFO			NFS Share Export List	RPC	1	Severity Base:	CVSS v3.0
						Scanner:	Local Scanner

Ora mi rimane da risolvere l'altro problema con NFS in uno scenario reale.



# Nessus

Per questa vulnerabilità abbiamo sostanzialmente una porta aperta la 1024 che funge da backdoor dove l'attaccante può creare dei problemi dando dei comandi diretti. La soluzione che io ho trovato è diversa da quella detta da Nessus

CRITICAL

Bind Shell Backdoor Detection

< >

Plugin Details

**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.

Severity: Critical

ID: 51988

Version: 1.10

Type: remote

Family: Backdoors

Published: February 15, 2011

Modified: April 11, 2022

# Nessus

Constatato che la porta 1524 non ci serve, ho deciso di disattivarla usando il firewall iptables, vado ad utilizzare i seguenti comandi. `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP` poi l'altro per assicurarsi che sia corretto `sudo iptables -L`.

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:ingreslock
DROP      tcp  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@metasploitable:/home/msfadmin#
```

Filter bind shell backdoor 0 of 56 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
No records found.					

Results per page 50 Showing 0 to 0 of 0 entries

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 9:45 AM  
End: Today at 9:54 AM  
Elapsed: 9 minutes





# Nessun

Il servizio RSH (Remote Shell) è un protocollo di rete che consente di eseguire comandi su un computer remoto su una rete. In parole più semplici, RSH permette a un utente di eseguire comandi su un altro computer attraverso la rete, come se fosse direttamente connesso a quel computer. Stesso discorso di prima questa porta mi serve, e andrò nel file ad inserire un `#` per non considerare la shell.

HIGH

rsh Service Detection

< >

Plugin Details

**Description**

The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the `.rhosts` or `rhosts.equiv` files.

**Solution**

Comment out the 'rsh' line in `/etc/inetd.conf` and restart the `inetd` process. Alternatively, disable this service and use SSH instead.

Severity: High

ID: 10245

Version: 1.38

Type: remote

Family: Service detection

Published: August 22, 1999

Modified: April 11, 2022

Risk Information

# Nessus

Su metasploitable facciamo `sudo nano/etc/inetd.conf` e cerchiamo la shell dove vediamo la dicitura rsh e mettiamo un # per renderlo un commento.

```
#shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rsh
```

A questo punto salviamo e facciamo sudo reboot.

Filter ▼ rsh 0 of 69 Vulnerabilities

Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼
No records found.					

Results per page 50

Showing 0 to 0 of 0 entries

**Scan Details**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 9:07 AM
- End: Today at 9:30 AM
- Elapsed: 23 minutes

# Fine

Grazie a queste piccole soluzioni siamo riusciti a rimuovere le vulnerabilità e dopo avere scansionato nuovamente possiamo vedere se effettivamente sono state risolte, infatti le mie vulnerabilità iniziali da 73 sono scese a 56 (probabilmente alcuni problemi low derivano da quelli critical o high quindi risolvendo uno ne risolvi molteplici).

Hosts 1Vulnerabilities 56Remediations 2History 3

Filter Search Vulnerabilities 56 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/>	MIXED	...	DNS (Multiple Issues)	DNS	4	
<input type="checkbox"/>	CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	HIGH	7.5	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	...	SSL (Multiple Issues)	General	28	
<input type="checkbox"/>	MIXED	...	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/>	MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2	
<input type="checkbox"/>	MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1	
<input type="checkbox"/>	MEDIUM	5.9	SSL Anonymous Cipher Suites Supported	Service detection	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0   
Scanner: Local Scanner  
Start: Today at 9:45 AM  
End: Today at 9:54 AM  
Elapsed: 9 minutes

Vulnerabilities

Critical

High

Medium

Low

Info