

### Traccia:

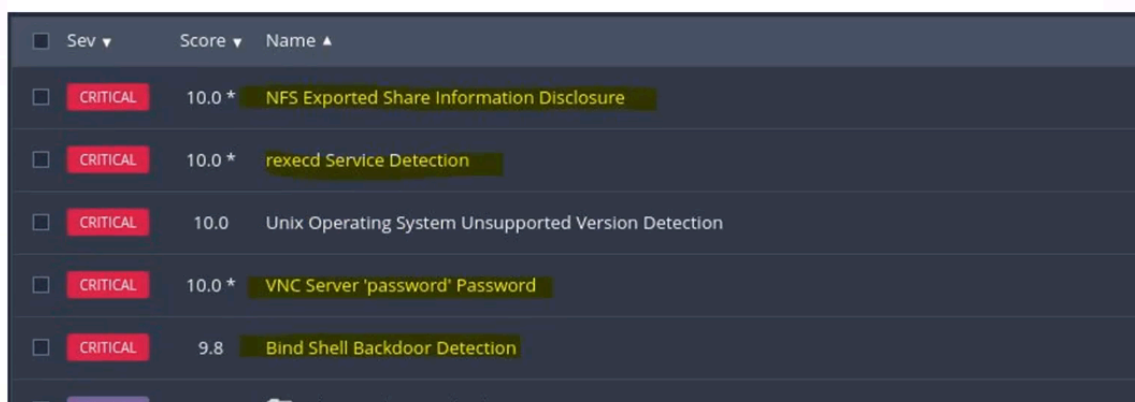
Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche / high** e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.



Sev	Score	Name
CRITICAL	10.0 *	NFS Exported Share Information Disclosure
CRITICAL	10.0 *	rexecd Service Detection
CRITICAL	10.0	Unix Operating System Unsupported Version Detection
CRITICAL	10.0 *	VNC Server 'password' Password
CRITICAL	9.8	Bind Shell Backdoor Detection

Vulnerabilities

Total: 133

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

Ecco le vulnerabilità trovate nel sistema.

Andremo ad analizzare e operare su:

### 1. NFS Exported Share Information Disclosure

## 2. VNC Server 'password' Password

### 3. Bind Shell Backdoor Detection

1. La divulgazione di informazioni tramite condivisioni NFS (Network File System) è una vulnerabilità che può essere rischiosa. Quando si parla di "NFS Exported Share Information Disclosure", ci si riferisce al fatto che le informazioni all'interno di una condivisione NFS possono essere accessibili a utenti non autorizzati. Questo potrebbe includere la possibilità di visualizzare, copiare o modificare file all'interno della condivisione.

Per mitigare questa vulnerabilità, ecco alcune misure che possono essere intraprese:

- Autenticazione e Autorizzazione: Assicurarsi che l'accesso alla condivisione NFS richieda un'adeguata autenticazione. Bisogna configurare correttamente i permessi sulla condivisione NFS per garantire che solo gli utenti autorizzati possano accedervi.
- Utilizzo di Versioni Sicure di NFS: Utilizzare versioni più recenti e sicure di NFS, come NFSv4, che offre migliorate caratteristiche di sicurezza rispetto alle versioni precedenti.
- Limitare l'Accesso: Bisogna limitare l'accesso solo agli host specifici che necessitano di accedere alla condivisione NFS. Configura i file exports correttamente per specificare gli host autorizzati.
- Patch e Aggiornamenti: Mantenere il sistema operativo e il software NFS aggiornati con le ultime patch di sicurezza per correggere eventuali vulnerabilità note.
- Firewall: Configurare un firewall per limitare l'accesso alla porta NFS solo dagli host autorizzati.

```
# 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)
#
#/*(rw, sync, no_root_squash, no_subtree_check)
/192.168.50.102(rw, root_squash, subtree_check)
```

Dunque, un esempio di come mitigare la vulnerabilità è configurare i file exports correttamente per specificare gli host autorizzati. Nella prima riga - che abbiamo commentato - viene indicato che qualsiasi host ha i permessi indicati all'interno delle parentesi. Invece nella seconda riga indichiamo un solo host, o un gruppo di host, che può avere determinate autorizzazioni. Per restartare NFS facciamo `sudo exportfs -ra`.

meta\_scan2 / 192.168.49.101

[Back to Hosts](#)

Vulnerabilities 56

Filter Search Vulnerabilities 56 Vulnerabilities

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	Name ▲
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating System Unsupported Version Detection
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'password' Password
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoor Detection
<input type="checkbox"/>	MIXED	...	...	Apache Tomcat (Multiple Issues)
<input type="checkbox"/>	CRITICAL	...	...	SSL (Multiple Issues)
<input type="checkbox"/>	HIGH	7.5 *	5.9	rlogin Service Detection
<input type="checkbox"/>	HIGH	7.5 *	5.9	rsh Service Detection
<input type="checkbox"/>	HIGH	7.5	5.9	Samba Badlock Vulnerability
<input type="checkbox"/>	MIXED	...	...	SSL (Multiple Issues)
<input type="checkbox"/>	MIXED	...	...	ISC Bind (Multiple Issues)

Vediamo dalla nuova scansione non è più presente la criticità precedente.

- VNC (Virtual Network Computing) è un protocollo usato per il controllo remoto del computer. Molte implementazioni di server VNC includono una funzionalità di autenticazione basata su password per proteggere l'accesso non autorizzato. Tuttavia, è importante notare che l'utilizzo di password deboli o predefinite può costituire un rischio per la sicurezza.

```
msfadmin@metasploitable:~$ vncpasswd
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:~$
```

La soluzione è proprio modificare la nostra password molto debole. Con il comando **vncpasswd** andiamo a modificare la password di default impostata nel sistema.

- La rilevazione di una "bind shell backdoor" comporta l'identificazione di un meccanismo che consente a un attaccante di ottenere un accesso remoto non autorizzato a un sistema. Una "bind shell" si riferisce a un tipo di shell che rimane in attesa su una porta specifica del sistema, pronta ad accettare una connessione in ingresso da parte di un attaccante.

Alcuni strumenti comuni per la rilevazione di backdoor:

- Monitoraggio del Traffico di Rete: Possiamo usare degli strumenti di monitoraggio del traffico di rete per individuare eventuali attività sospette.

L'analisi del traffico attraverso strumenti come Wireshark può rivelare comunicazioni non autorizzate.

- Scansione delle Porte: Possiamo utilizzare strumenti di scansione delle porte come Nmap per identificare porte aperte e servizi in ascolto sul sistema. Dobbiamo concentrarci su porte non standard o porte associate a servizi sospetti.
- Firewall e Filtraggio del Traffico: Configura regole del firewall per limitare l'accesso alle porte critiche e monitorare l'attività di rete in modo più stretto.

Una delle soluzioni dunque è configurare una regola nel firewall.

```
msfadmin@metasploitable:~$ sudo iptables -L
[sudo] password for msfadmin:
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num target     prot opt source                destination
1 DROP      tcp  -- anywhere             anywhere            tcp dpt:ingres
lock

Chain FORWARD (policy ACCEPT)
num target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num target     prot opt source                destination
msfadmin@metasploitable:~$
```

Con il comando - `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP` - impostiamo la regola.

Con il comando - `sudo iptables -nL | grep 1524` vediamo la sola regola impostata

Così abbiamo configurato il firewall per mitigare la vulnerabilità.

Vulnerabilities 62				
Filter	Search Vulnerabilities		62 Vulnerabilities	
Sev	CVSS	VPR	Name	Family
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General
<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 Detection	Service detection
<input type="checkbox"/> MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers
<input type="checkbox"/> CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely
<input type="checkbox"/> HIGH	7.5 *	5.9	rlogin Service Detection	Service detection
<input type="checkbox"/> HIGH	7.5 *	5.9	rsh Service Detection	Service detection
<input type="checkbox"/> HIGH	7.5	5.9	Samba Badlock Vulnerability	General
<input type="checkbox"/> MIXED	...	...	SSL (Multiple Issues)	General
<input type="checkbox"/> MIXED	...	...	ISC Bind (Multiple Issues)	DNS
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection
<input type="checkbox"/> MEDIUM	6.5		Unencrypted Telnet Server	Misc.

Attraverso una nuova scansione possiamo appurare che la vulnerabilità "bind shell backdoor" non è più presente.