

Report progetto 28-01-2024

2) Screenshot e spiegazione dei passaggi della remediation

Vulnerabilities 61								
Filter	Search Vulnerabilities						61 Vulnerabilities	
Sev	CVSS	VPR	Name	Family	Count		Host Details	
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1		<div>IP: 192.168.51.100 OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy) Start: January 26 at 3:27 PM End: January 26 at 3:54 PM Elapsed: 27 minutes KB: Download</div> <div>Vulnerabilities <ul style="list-style-type: none">CriticalHighMediumLowInfo</div>	
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1			
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1			
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2			
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1			
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1			
<input type="checkbox"/> CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3			
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1			
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1			
<input type="checkbox"/> MIXED	SSL (Multiple Issues)	General	28			
<input type="checkbox"/> MIXED	ISC Bind (Multiple Issues)	DNS	5			

Dall'analisi di nessus possiamo vedere che il sistema metaploitable 2 presenta 10 vulnerabilità critiche.

In questo report andro a risolvere alcune di queste tra cui :

- **NFS Exported Share Information Disclosure**

- **VNC Server 'password' Password**

NFS Exported Share Information Disclosure

Description

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

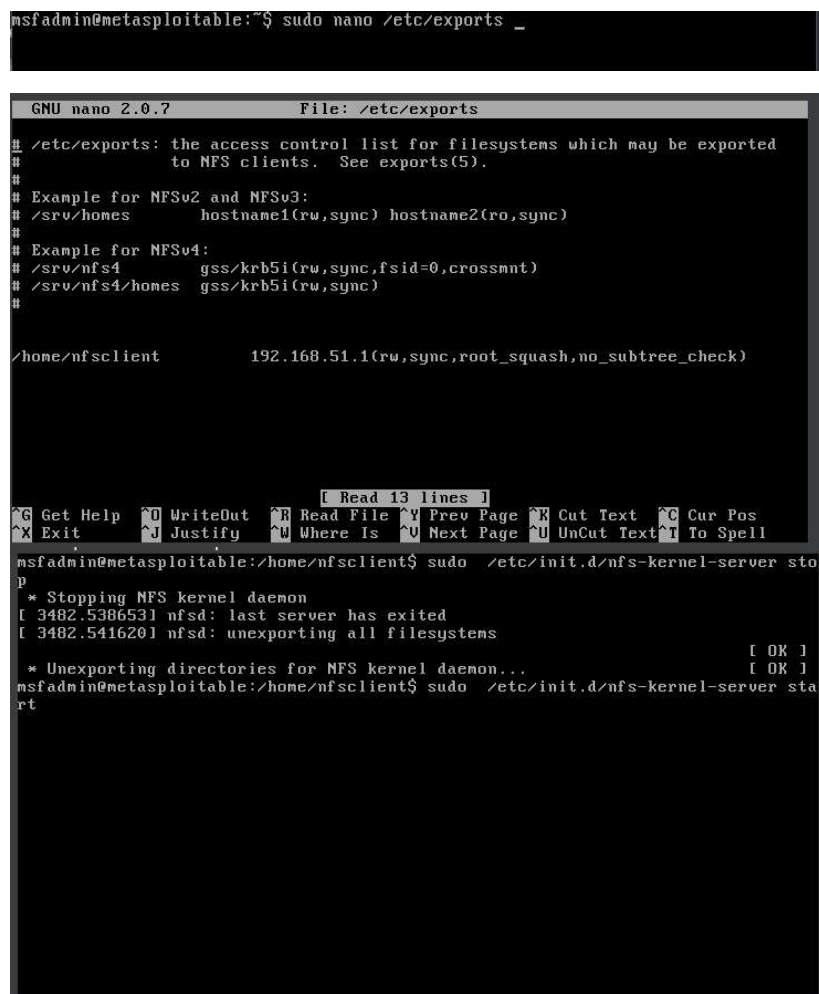
Solution proposed by nessus

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Remediation:

Ho modificato il file exports con l'ip per autorizzare solo alla macchina pfsense(192.168.51.1) l'accesso al servizio NFS sulla macchina metasploitable 2 , e dopo ho chiuso e riavviato il servizio.

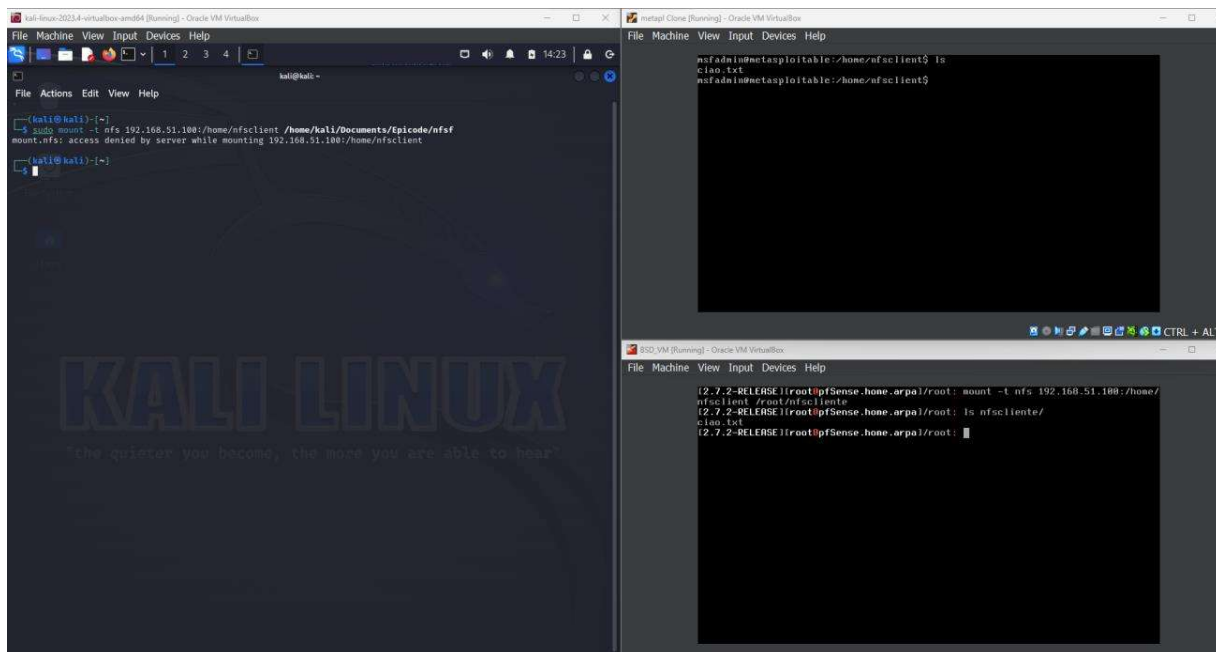
```
msfadmin@metasploitable:~$ sudo nano /etc/exports _
```



```
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(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/home/nfsclient 192.168.51.1(rw,sync,root_squash,no_subtree_check)

[ Read 13 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^X Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
msfadmin@metasploitable:/home/nfsclient$ sudo /etc/init.d/nfs-kernel-server stop
* Stopping NFS kernel daemon
[ 3482.538653] nfsd: last server has exited
[ 3482.541620] nfsd: unexporting all filesystems
* Unexporting directories for NFS kernel daemon...
msfadmin@metasploitable:/home/nfsclient$ sudo /etc/init.d/nfs-kernel-server start
```

Successivamente ho confermato che solo la macchina pfsense potesse usufruire del servizio nfs e come si può vedere la macchina Kali non può ha accesso al servizio mentre pfsense non ha problemi ad accedere .



VNC Server 'password' Password

Description

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password di tipo "password". Un attaccante remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

Solution proposed by nessus

Protegete il servizio VNC con una password forte.

Remediation:

Ho installato il software remmina su kali per verificare la connesione VNC e dopo essere entrato ho cambiato la password 'password' con un piu sicura fatta da me .

