

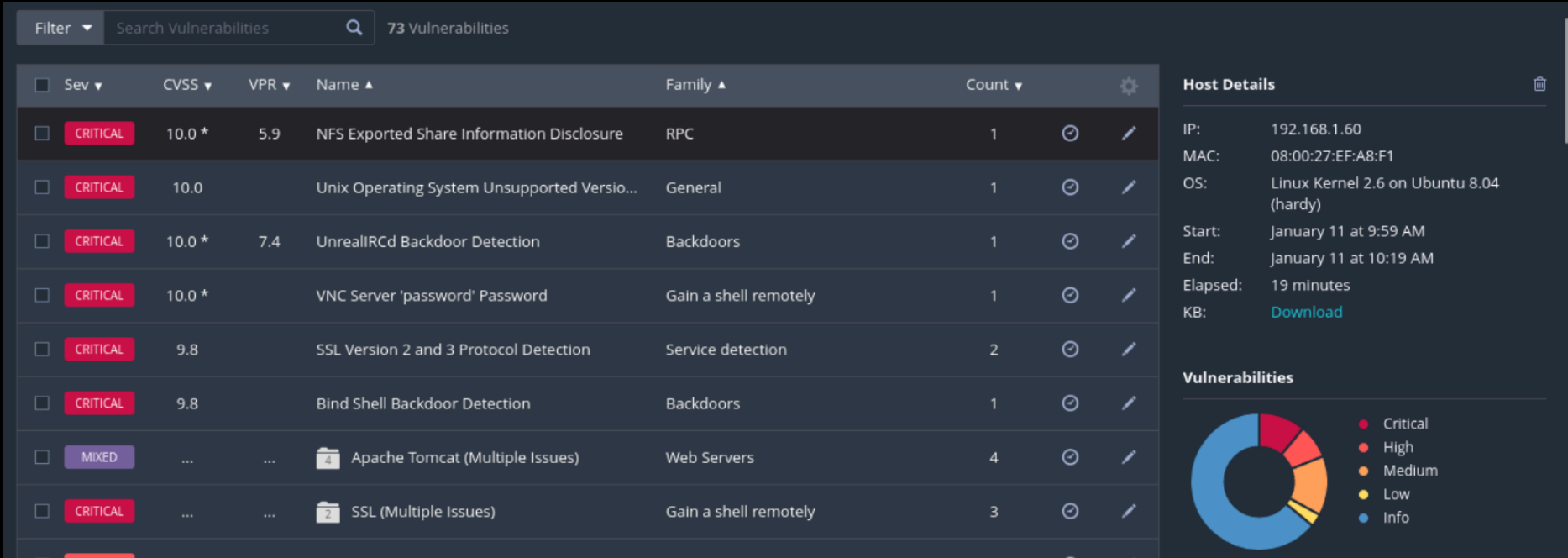
# Metasploitable vulnerability



Richiesta: Scanning vulnerabilità Metasploitable e implemento di azioni di rimedio.

Tool utilizzati: Nessus.

## Scanning:



Notiamo un elevato numero delle vulnerabilità rilevate.

Obiettivo: Ridurre il livello di criticità di almeno 2 vulnerabilità critiche.

### Vulnerabilità 1:

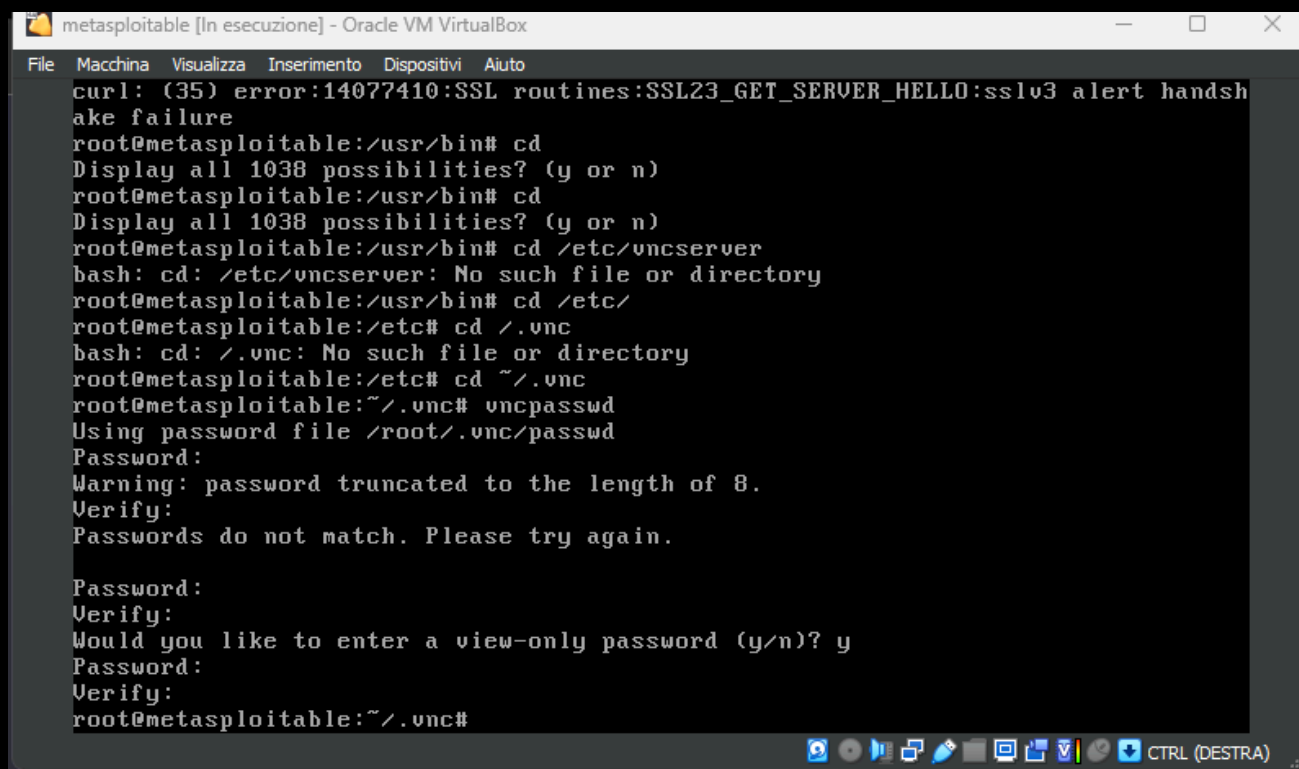
#### VNC Server “password” Password

**Descrizione:** VNC (Virtual Network Computing) è un sistema che consente di controllare un computer da remoto. Una vulnerabilità comune in VNC è l’uso di password deboli o predefinite. Questo rende il server suscettibile ad attacchi di forza bruta o di indovinamento delle password.

**Criticità:** Se un attaccante riesce ad accedere al tuo server VNC, può avere il pieno controllo del sistema remoto.

**Impatto:** Un attaccante potrebbe utilizzare strumenti di cracking delle password per decifrare la tua password VNC. Una volta dentro, potrebbe installare backdoor per un accesso futuro, sottrarre dati sensibili, o utilizzare il server come punto di partenza per ulteriori attacchi all’interno della rete.

## Soluzione:



```
metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
curl: (35) error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handsh
ake failure
root@metasploitable:/usr/bin# cd
Display all 1038 possibilities? (y or n)
root@metasploitable:/usr/bin# cd
Display all 1038 possibilities? (y or n)
root@metasploitable:/usr/bin# cd /etc/vncserver
bash: cd: /etc/vncserver: No such file or directory
root@metasploitable:/usr/bin# cd /etc/
root@metasploitable:/etc# cd /.vnc
bash: cd: /.vnc: No such file or directory
root@metasploitable:/etc# cd ~/.vnc
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:~/.vnc#
```

**Descrizione:** La password di default “password” è stata sostituita con una più robusta e sicura (“GHlje25%”). Questo è un passo fondamentale per aumentare la sicurezza del server VNC.

**Impatto della Soluzione:** Utilizzando una password complessa, si riduce significativamente il rischio di attacchi di forza bruta e si rende molto più difficile per gli attaccanti l’accesso non autorizzato al server VNC.

## Vulnerabilità 2:

### NFS Exported Share Information Disclosure

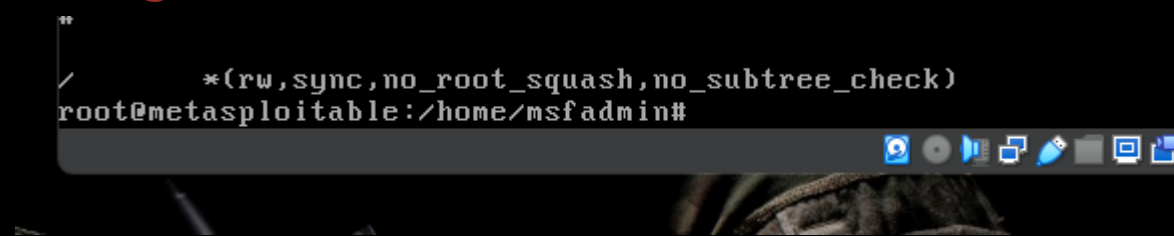
**Descrizione:** NFS (Network file system) è utilizzato per il montaggio di file system su una rete, permettendo a utenti e programmi di accedere a file su server remoti come se fossero memorizzati localmente. Una configurazione errata di NFS può lasciare i file system esposti a letture e scritture non autorizzate.

**Criticità:** Se un NFS è mal configurato, un attaccante potrebbe leggere o scrivere dati nei file system condivisi. Ciò potrebbe portare alla perdita di dati sensibili, alla manipolazione di file critici o addirittura al caricamento di file dannosi che potrebbero essere eseguiti sul server.

**Impatto:** potrebbe sfruttare questa vulnerabilità per mappare la rete e identificare file system NFS esposti. Potrebbe quindi tentare di montare questi file system sul proprio sistema e accedere o modificare i file. In alcuni casi,

potrebbero anche riuscire ad eseguire codice arbitrario se riescono a manipolare file eseguibili sul NFS.

### Configurazione critica:



**La configurazione mostrata nello screenshot è critica per diversi motivi:**

**Opzione \* per l'Esportazione:** L'asterisco indica che il NFS share è esportato a tutti, senza restrizioni di indirizzo IP.

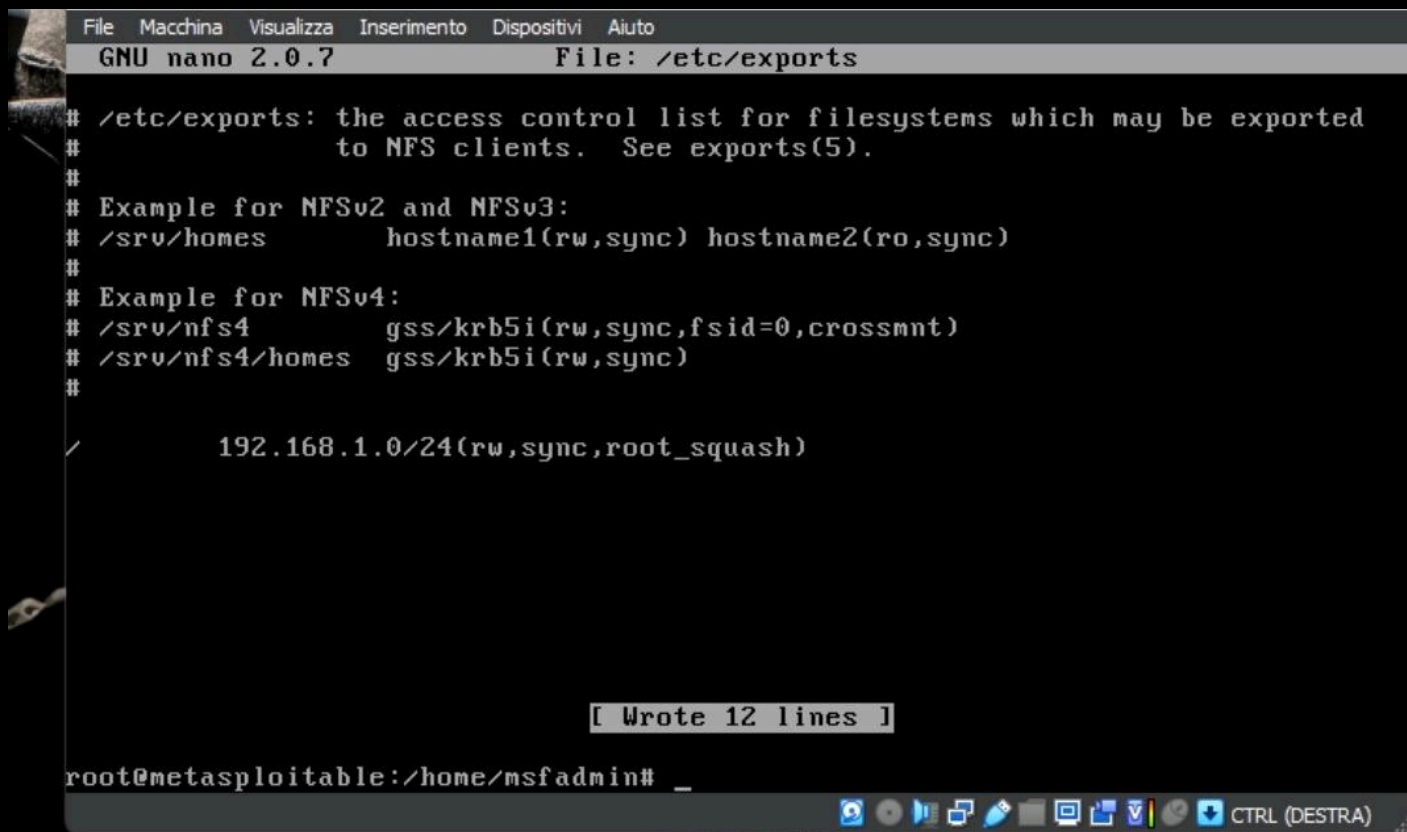
**Opzione rw:** L'opzione rw sta per read-write, che permette agli utenti di leggere e scrivere sulla condivisione NFS. Se questa condivisione è esposta a tutta la rete (o peggio, a internet), allora chiunque potrebbe scrivere file sul server, che potrebbero essere eseguiti o utilizzati per attacchi.

**Opzione no\_root\_squash:** Normalmente, root\_squash converte le richieste da root (l'utente amministratore) in un utente anonimo per prevenire che gli utenti root su client NFS possano scrivere file come root sul server NFS. no\_root\_squash disabilita questa misura di sicurezza, permettendo all'utente root su un client NFS di avere pieni privilegi anche sul server NFS, aumentando il rischio di attacchi di elevazione dei privilegi.

**Opzione sync:** L'opzione sync è positiva in termini di integrità dei dati perché assicura che le modifiche ai file siano scritte sul disco prima di completare i comandi di scrittura. Tuttavia, in combinazione con le altre opzioni permissive, garantisce che qualsiasi azione dannosa (come la scrittura di file dannosi) sia immediatamente effettiva e più difficile da rilevare o annullare.

**Opzione no\_subtree\_check:** Questa opzione disabilita il subtree checking (un'opzione di configurazione del server NFS), che può migliorare le prestazioni ma potrebbe anche aumentare il rischio di accesso non autorizzato a file system che non dovrebbero essere completamente accessibili, se non configurato correttamente.

## Soluzione:



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
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)
#
192.168.1.0/24(rw,sync,root_squash)

[ Wrote 12 lines ]
root@metasploitable:/home/msfadmin#
```

## Descrizione:

**192.168.1.0/24:** Questo indica che solo i dispositivi nella subnet 192.168.1.0 con una maschera di sottorete di 255.255.255.0 (che è cosa significa /24) possono montare questa condivisione NFS.

**root\_squash:** Mappa le richieste da UID/GID 0 (root) a un UID/GID anonimo.

**Eliminazione no\_subtree\_check:** Questa scelta influirà sulle prestazioni del server ma aumenterà la sicurezza. Grazie all'abilitazione di questo servizio si assicura che i file richiesti dagli utenti NFS corrispondano effettivamente a quelli ai quali l'utente dovrebbe avere accesso secondo le impostazioni del server NFS. Questo è importante perché impedisce agli utenti di accedere a file che non sono stati espressamente esportati.

**Impatto della soluzione:** Queste modifiche aumentano la sicurezza del NFS limitando l'accesso solo a utenti autorizzati e riducendo il rischio di modifiche non autorizzate o di accesso ai dati sensibili.



Risultato finale 2° scansione:

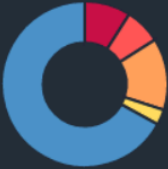
Filter Search Vulnerabilities 70 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
CRITICAL	10.0		Unix Operating System Unsupported Versio...	General	1	
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1	
MIXED	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1	
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	

Host Details

IP: 192.168.1.60  
MAC: 08:00:27:EF:A8:F1  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 10:43 AM  
End: Today at 11:02 AM  
Elapsed: 19 minutes  
KB: [Download](#)

Vulnerabilities



Critical

High

Medium

Low

Info

Conclusioni

La seconda scansione, sulla base degli obiettivi assegnati in precedenza, possiamo definirla un successo.

Implementando queste azioni di rimedio, si è riuscito ad aumentare il livello di sicurezza di metasploitable.

Le 2 vulnerabilità critiche analizzate sono state risolte.

