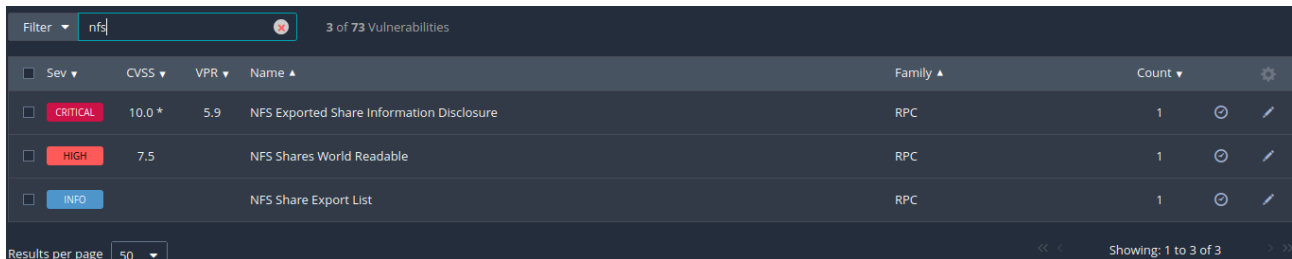


Analizzo 3 delle vulnerabilità critiche che sono state riportate dopo la scansione di Nessus su Metasploitable:

- VULNERABILITA' CRITICA NFS

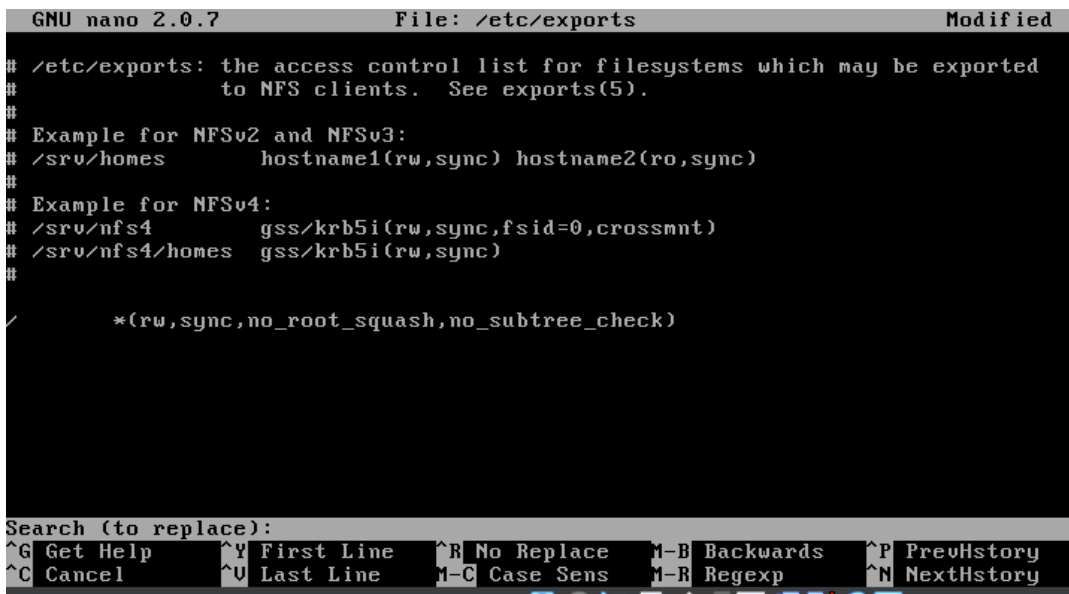


The screenshot shows the Nessus interface with a filter set to 'nfs'. It displays 3 of 73 vulnerabilities. The table lists three critical vulnerabilities related to NFS:

| Sev | CVSS | VPR | Name | Family | Count |
|----------|--------|-----|---|--------|-------|
| CRITICAL | 10.0 * | 5.9 | NFS Exported Share Information Disclosure | RPC | 1 |
| HIGH | 7.5 | | NFS Shares World Readable | RPC | 1 |
| INFO | | | NFS Share Export List | RPC | 1 |

Results per page: 50. Showing: 1 to 3 of 3.

Metasploitable presenta almeno una condivisione NFS che può essere montata dal nostro host di scansione. Questo costituisce un potenziale rischio, in quanto un attaccante potrebbe sfruttare questa opportunità per accedere ai file di Metasploitable. In particolare, l'attaccante potrebbe essere in grado di leggere, e in alcuni casi anche scrivere, nei file ospitati su Meta attraverso questa condivisione NFS.



```
GNU nano 2.0.7      File: /etc/exports      Modified
# /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)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

Search (to replace):

| | | | | |
|-------------|---------------|----------------|----------------|----------------|
| ^G Get Help | ^Y First Line | ^R No Replace | ^M-B Backwards | ^P PrevHistory |
| ^C Cancel | ^U Last Line | ^M-C Case Sens | ^M-R Regexp | ^N NextHistory |

Per risolvere questa vulnerabilità, sono entrato nella directory `/etc/exports` utilizzando il comando ***"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)
#
[ Read 11 lines ]
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

All'interno del file ho eliminato la riga che conteneva tutti i permessi abilitati.

Rifacendo una nuova scansione con Nessus, notiamo come ora la vulnerabilità critica riguardante NFS non sia più presente.

| Vulnerabilities 63 | | | | |
|--------------------------|------|------|-------------------------|------------------------|
| Filter | nfs | | 1 of 63 Vulnerabilities | |
| <input type="checkbox"/> | Sev | CVSS | VPR | Name |
| <input type="checkbox"/> | INFO | | | NFS Server Superfluous |
| | | | | RPC |

VULNERABILITA' CRITICA VNC

| | | | | |
|--------------------------|----------|--------|-------------------------|--------------------------------|
| Filter | vnc | | 2 of 73 Vulnerabilities | |
| <input type="checkbox"/> | Sev | CVSS | VPR | Name |
| <input type="checkbox"/> | CRITICAL | 10.0 * | | VNC Server 'password' Password |
| | | | | Gain a shell remotely |
| <input type="checkbox"/> | INFO | ... | | VNC (Multiple Issues) |
| | | | | Service detection |

Il server VNC (è un software che consente di condividere e controllare il desktop di un computer da un'altra posizione tramite una connessione di rete) che opera su Metasploitable è attualmente vulnerabile a causa dell'utilizzo di una password debole. In particolare, Nessus è riuscito ad accedere con successo utilizzando l'autenticazione VNC e inserendo una password estremamente semplice, ossia 'password'. Questa situazione apre la porta a un possibile attacco da parte di un malintenzionato remoto e non autenticato, il quale potrebbe sfruttare questa vulnerabilità per ottenere il controllo completo del sistema.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$
```

Per risolvere questa vulnerabilità, ho digitato il comando **“vncpasswd”**, che mi ha permesso di modificare la password. Ho utilizzato una password robusta e sicura, per evitare che potesse essere nuovamente e facilmente dedotta (com’era accaduto con la password **“password”**).

Rifacendo una nuova scansione con Nessus, notiamo come ora la vulnerabilità critica riguardante VNC non sia più presente.

| Vulnerabilities 63 | | | | | |
|--------------------|-----------------------------|-----|-----------------------|-------------------|--|
| Filter | vnc 1 of 63 Vulnerabilities | | | | |
| Sev | CVSS | VPR | Name | Family | |
| INFO | ... | ... | VNC (Multiple Issues) | Service detection | |

VULNERABILITA' CRITICA BACKDOOR

| Filter | backdoor 1 of 73 Vulnerabilities | | | | | |
|----------|----------------------------------|-----|-------------------------------|-----------|-------|--|
| Sev | CVSS | VPR | Name | Family | Count | |
| CRITICAL | 9.8 | | Bind Shell Backdoor Detection | Backdoors | 1 | |

Results per page 50 Showing: 1 to 1 of 1


Su Metasploitable è in ascolto una shell su una porta senza richiedere alcuna forma di autenticazione. Questo rappresenta un potenziale rischio, poiché ciò significa che un attaccante potrebbe ottenere accesso non autorizzato al sistema semplicemente connettendosi a questa porta e interagendo direttamente con la shell. Questo scenario è critico, in quanto consente a un potenziale aggressore di eseguire comandi sul server remoto senza alcuna restrizione, aprendo la porta a possibili violazioni della sicurezza e compromissioni del sistema.

```
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd  4522 root   12u  IPv4  12217      TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin# kill 4522
root@metasploitable:/home/msfadmin#
```

Per risolvere questa vulnerabilità, ho prima digitato **“sudo su”** per entrare in modalità root, poi ho usato il comando **“lsof -i :1524”** (1524 è il numero di porta dove vi è la backdoor). Sono riuscito poi a vedere il PID del processo compromesso(4522), e ho di conseguenza disabilitato la shell remota in ascolto sulla porta 1524, utilizzando il comando **“kill 4522”**.

Rifacendo una nuova scansione con Nessus, notiamo come ora la vulnerabilità critica riguardante la backdoor non sia più presente.

Vulnerabilities 63

Filter ▼ backdoor bi  0 of 63 Vulnerabilities

☐ Sev ▼

CVSS ▼

VPR ▼

Name ▲

No records found.