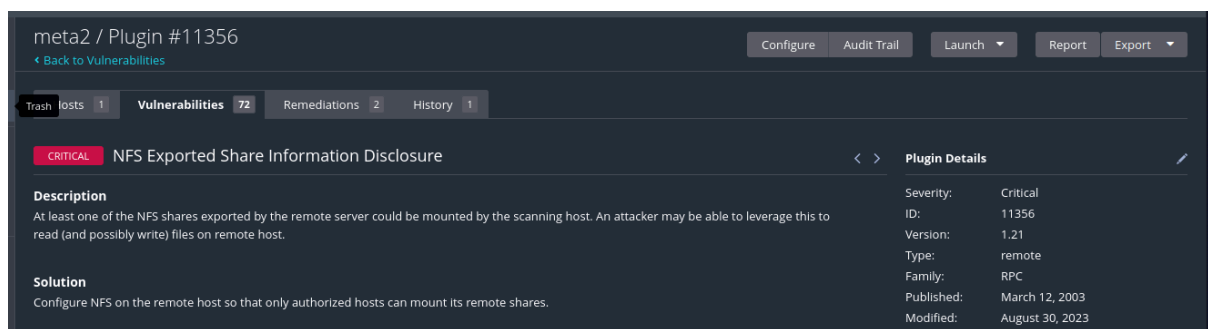
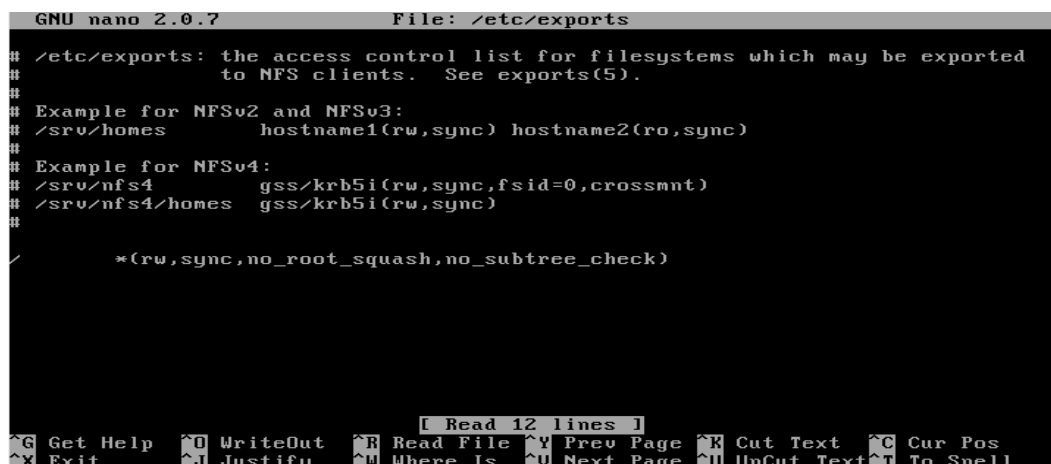


Consegna: effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

La prima criticità che ho scelto di fixare è quella che riguarda l'**NFS**: il Network file system è un protocollo utilizzato solitamente per condividere files o directory da un sistema Linux/Unix su una rete. La vulnerabilità "NFS exported share information disclosure" si ha quando le informazioni sulle condivisioni effettuate possono essere intercettate da host non autorizzati e potrebbero potenzialmente far leggere o scrivere file sul server remoto.



Ho utilizzato il comando `sudo nano + /etc/exports` e in questo modo sono entrata nella directory, dopodiché ho eliminato i permessi (l'ultima stringa) in modo che host non autorizzati non possano leggere o scrivere file sul server remoto.



Come si vede nei seguenti screen, il comando è stato eliminato e la vulnerabilità è stata risolta.

```
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)
#
```

Vulnerabilities 80

Filter nfs 1 of 80 Vulnerabilities

Sev CVSS VPR Na... Family Count

INFO

NFS :RPC

1

results per page 50 Showing: 1 to 1 of 1

Host Details

IP: 192.168.64.8

MAC: 1A:44:A4:FE:11:BB

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Start: Today at 1:35 PM

End: Today at 1:43 PM

Elapsed: 8 minutes

KB: [Download](#)

Vulnerabilities

La seconda criticità che ho scelto di fixare è la **VNC** (VNC Server 'password' Password), che presenta un rischio di criticità alta poiché la password è troppo debole e deve essere cambiata per aumentare la sicurezza.

Filter password 1 of 79 Vulnerabilities

Sev CVSS VPR Na... Family Count

CRITICAL

10.0 *

VNC Gain a shell remotely

1

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: January 11 at 12:14 PM

End: January 11 at 12:22 PM

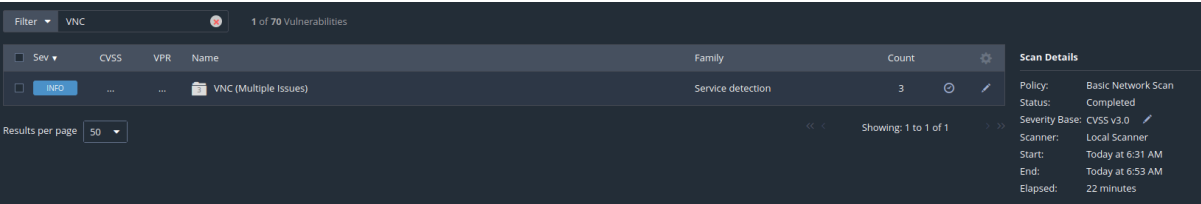
Elapsed: 9 minutes

Per questo ho usato il comando `sudo su`, poi `vncpasswd` e ho messo una nuova password di almeno 8 caratteri resolvendo in questo modo la criticità, come si vede negli screen seguenti.

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? no
root@metasploitable:/home/msfadmin#

```



Sev	CVSS	VPR	Name	Family	Count
INFO	VNC (Multiple Issues)	Service detection	3

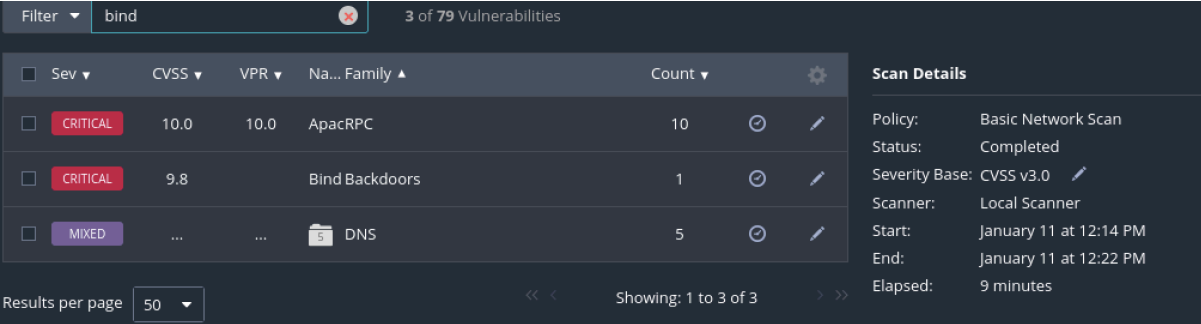
Results per page: 50

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

La terza criticità che ho scelto di risolvere riguarda la **backdoor**: la presenza di una backdoor rappresenta una criticità perché una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.



Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0	10.0	ApacRPC		10
CRITICAL	9.8		Bind Backdoors		1
MIXED	DNS		5

Results per page: 50

Showing: 1 to 3 of 3

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: January 11 at 12:14 PM
 End: January 11 at 12:22 PM
 Elapsed: 9 minutes

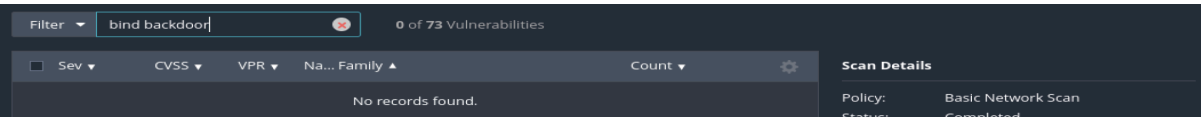
Come si vede nello screen seguente, ho utilizzato il comando `sudo su` e poi `lsof -i :1524`, e poi il comando `kill 4473` (numero di processo assegnato al protocollo della porta) per chiudere la backdoor.

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# lsof -i :1524
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd  4473 root   12u  IPv4  12086      TCP *:ingreslock (LISTEN)
root@metasploitable:/home/msfadmin# kill 4473
root@metasploitable:/home/msfadmin#

```

Questo ha risolto la criticità, come si vede nello screen seguente.



Filter: bind backdoor 0 of 73 Vulnerabilities

No records found.

Scan Details

Policy: Basic Network Scan
 Status: Completed