

## **Remediation delle vulnerabilità**

Vulnerabilità risolte:

Bind Shell Backdoor Detection  
NFS Exported Share Information Disclosure  
VNC server 'password' Password

### **1. Bind Shell Backdoor Detection**

Per quanto riguarda la risoluzione di questa vulnerabilità, ho abilitato il firewall di Metasploitable con il comando "UFW ENABLE"



Dopodiché, ho detto al firewall di acconsentire a tutte le regole di default con "UFW DEFAULT ALLOW"

```
[ Wrote 12 lines ]

msfadmin@metasploitable:~$ ufw enable
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin# ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule added
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded

To Action From
--
1524:tcp DENY Anywhere
1524:udp DENY Anywhere

root@metasploitable:/home/msfadmin# _
```

Integrazione del mouse...

Acquisizione automatica della tastiera...

## 2. NFS Exported Share Information Disclosures

Per quanto riguarda la prima vulnerabilità, la remediation da applicare è quella di inserire all'interno della sottocartella del root /etc.

La prima cosa da fare è quella di visualizzare all'interno delle sottocartelle del root con "ls -a".

Cerchiamo la directory "/etc" e apriamo il file "exports".

All'interno di questo file, andremo a modificare 1'\* in fondo alla pagina con l'ip della nostra macchina.

Una volta fatto, riavviamo la macchina.



### 3. VNC Server 'password' Password

Per modificare la password del VNC Server, troviamo all'interno della directory msfadmin, con il comando ls-a, il directory .vnc. All'interno di questa directory, andremo a eseguire il comando "vncpasswd" per cambiare la password.

Alla fine riavviamo la macchina.

