

Simone Tartaglia

Remediation Data

1) Per la vulnerabilità riguardo al VNC Server la quale problematica era che la login aveva come password "password"



Quindi su metasploitable 2 ho cambiato i permessi da user a root e dopo ho usato il comando "sudo vncpasswd" per cambiare password in modo renderla più forte.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
```

2) La vulnerabilità riguardante la bind shell backdoor



ho inserito una regola firewall con iptables per chiudere il traffico sulla porta "1524" dove è aperta la backdoor

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp --dport 1524 -j DROP
```

3) La vulnerabilità riguardante l'NFS server è stata risolta stoppando il server in modo tale da non avere una fuori uscita di file.



```
msfadmin@metasploitable:~$ sudo /etc/init.d/portmap stop
* Stopping portmap daemon... [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/nfs-kernel-server stop
* Stopping NFS kernel daemon [ OK ]
* Unexporting directories for NFS kernel daemon... [ OK ]
```