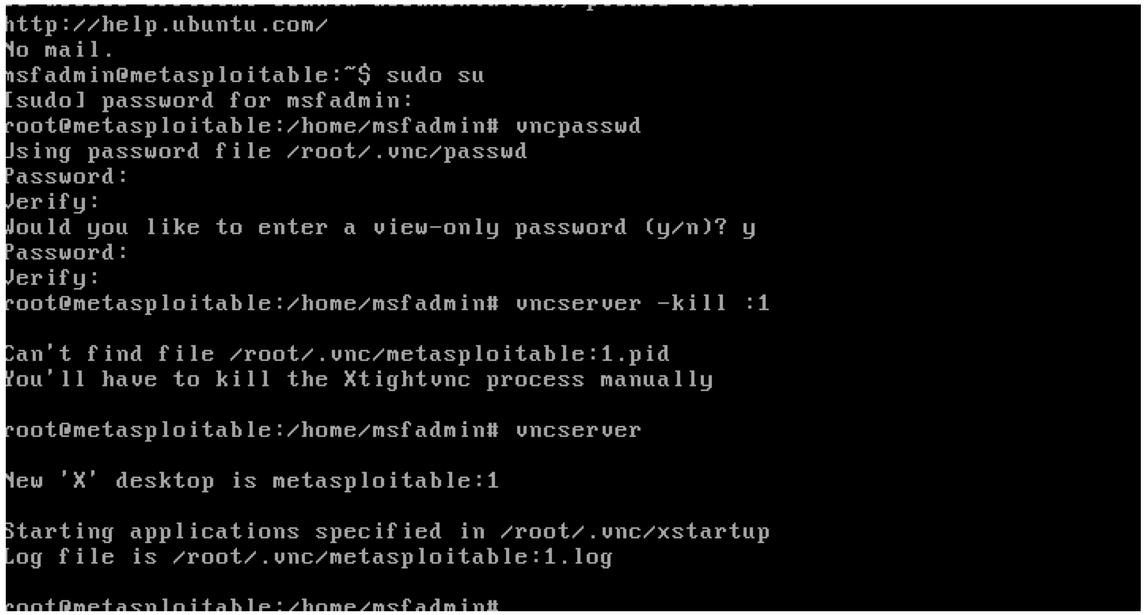
Remediation vulnerability project

metasploitable 2

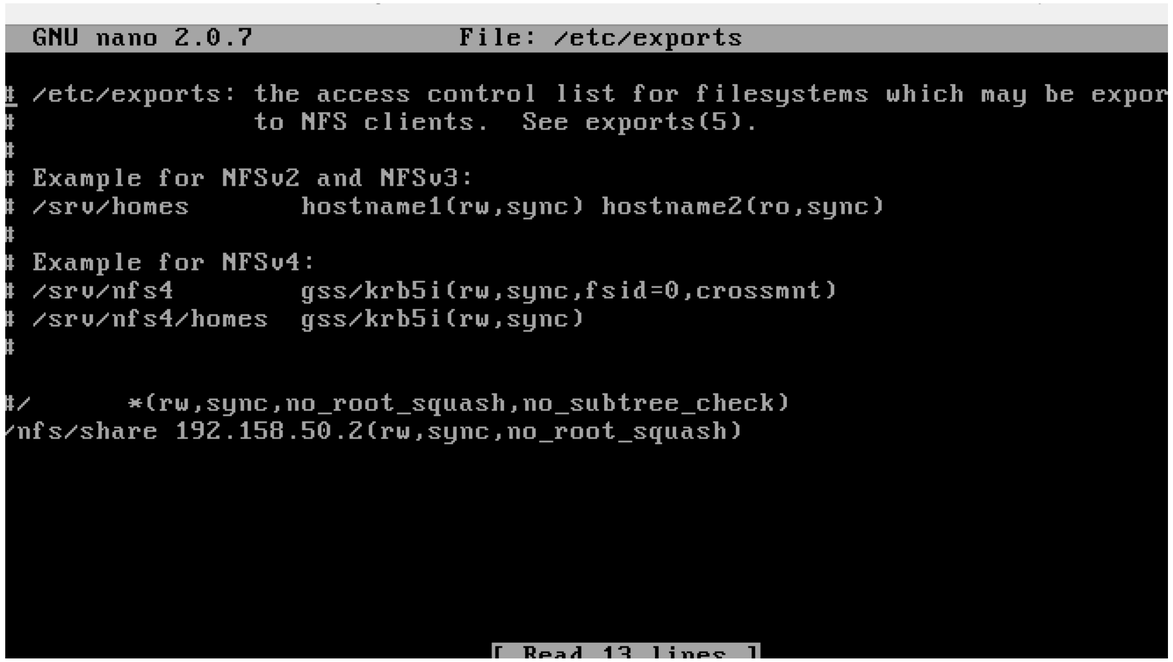
Vulnerabilità risolte: 3

Vulnerabilità 1



- Vulnerabilità: VNC Server 'password' Password
- Soluzione: come mostrato in figura, ho cambiato direttamente la password vnc

Vulnerabilità 2



- Vulnerabilità: NFS Exported Share Information Disclosure
- Soluzione: ho configurato NFS su host personalizzato in modo che solo l’ host autorizzato possa montare le sue condivisioni remote.

Vulnerabilità 3

```
 GNU nano 2.0.7                File: iptables

iptables -A INPUT -p tcp --dport 1524 -j DROP
```

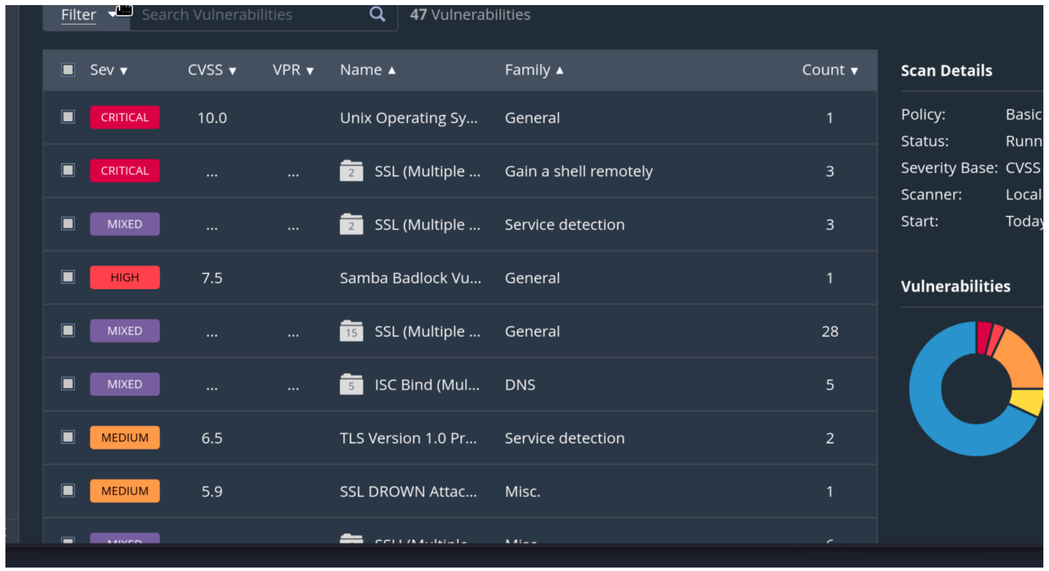
```
┌──(nicholas㉿kali)-[~]
└─$ sudo nmap 192.168.50.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-30 22:57 CES
mass_dns: warning: Unable to determine any DNS servers. Reverse
Nmap scan report for 192.168.50.2
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
8180/tcp open     unknown
MAC Address: CA:01:F0:3E:DD:B1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

- Vulnerabilità: Bind Shell Backdoor Detection
  - Soluzione: ho creato un file chiamato iptables nella directoryetc/init.d/ con all'interno il comando che serve per bloccare la porta di riferimento della backdoor, di conseguenza ho reso eseguibile il file tramite il comando sudo chmod +x /etc/init.d/iptables e ho creato dei collegamenti con il file per far si che venga eseguito ad ogni avvio della macchina, con l comando: sudo update-rc.d iptables defaults

- Eseguendo la scansione con nmap la porta 1524 relativa alla backdoor risulta filtrata

Final report



- Eseguendo per ultimo una scansione con Nessus, le vulnerabilità non sono state più trovate e di conseguenza posso confermare di aver risolto le 3 vulnerabilità sopra citate