

# Remediation vulnerability project

## metasploitable 2

## Vulnerabilità risolte: 3

### Vulnerabilità 1

```
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)? y  
Password:  
Verify:  
root@metasploitable:/home/msfadmin# vncserver -kill :1  
  
Can't find file /root/.vnc/metasploitable:1.pid  
You'll have to kill the Xtightvnc process manually  
  
root@metasploitable:/home/msfadmin# vncserver  
  
New 'X' desktop is metasploitable:1  
  
Starting applications specified in /root/.vnc/xstartup  
Log file is /root/.vnc/metasploitable:1.log  
  
root@metasploitable:/home/msfadmin#
```

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

# Vulnerabilità 2

```
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)
#
#/*              *(rw,sync,no_root_squash,no_subtree_check)
/nfs/share 192.158.50.2(rw,sync,no_root_squash)

[ Read 13 lines ]
```

- 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
```

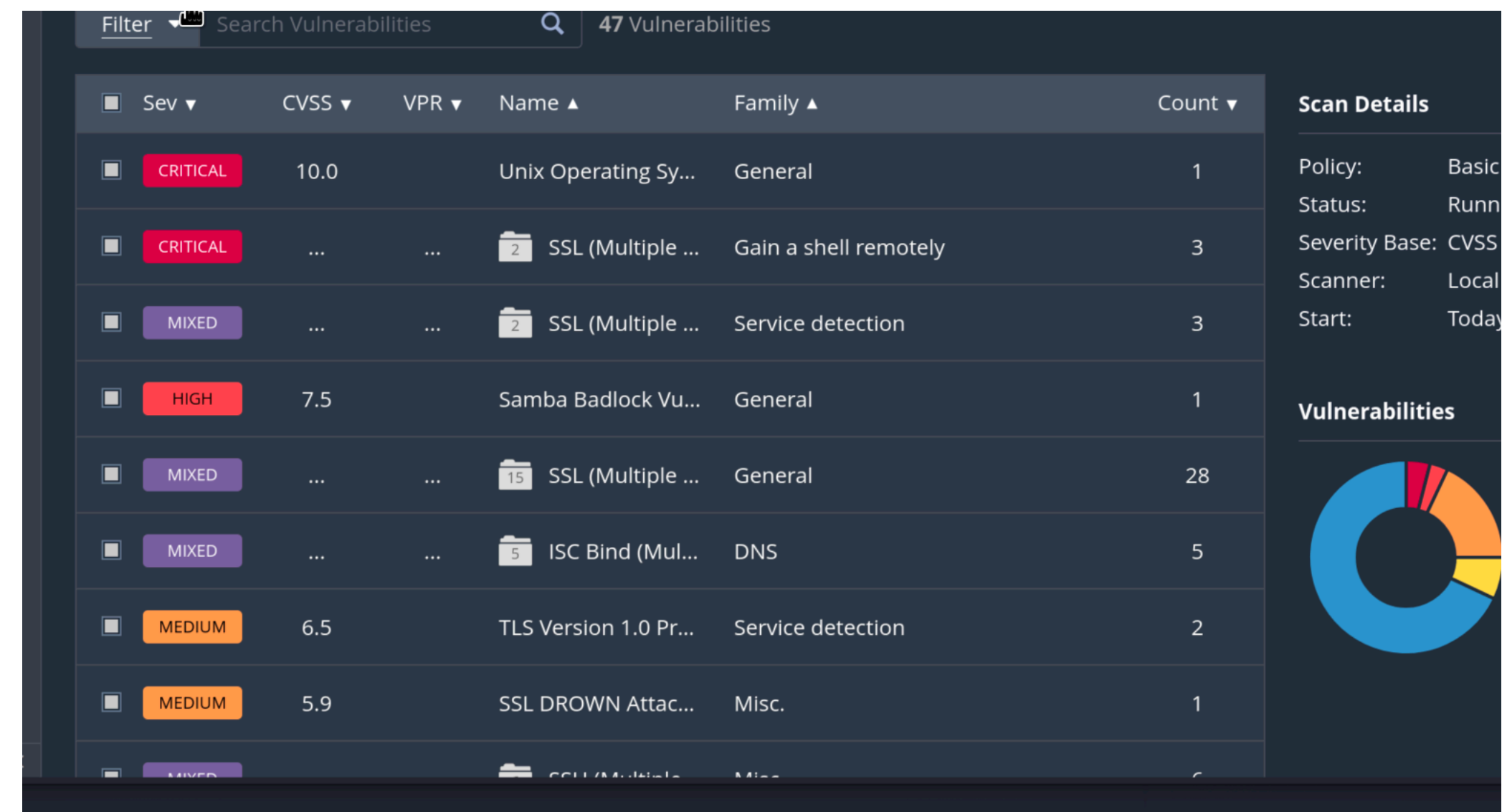
```
Nmap done: 1 IP address (1 host up) scanned in 0.122 seconds

(nicholas@kali)-[~]
$ sudo nmap 192.168.50.2
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-30 22:57 CEST
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 directory/etc/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 il 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