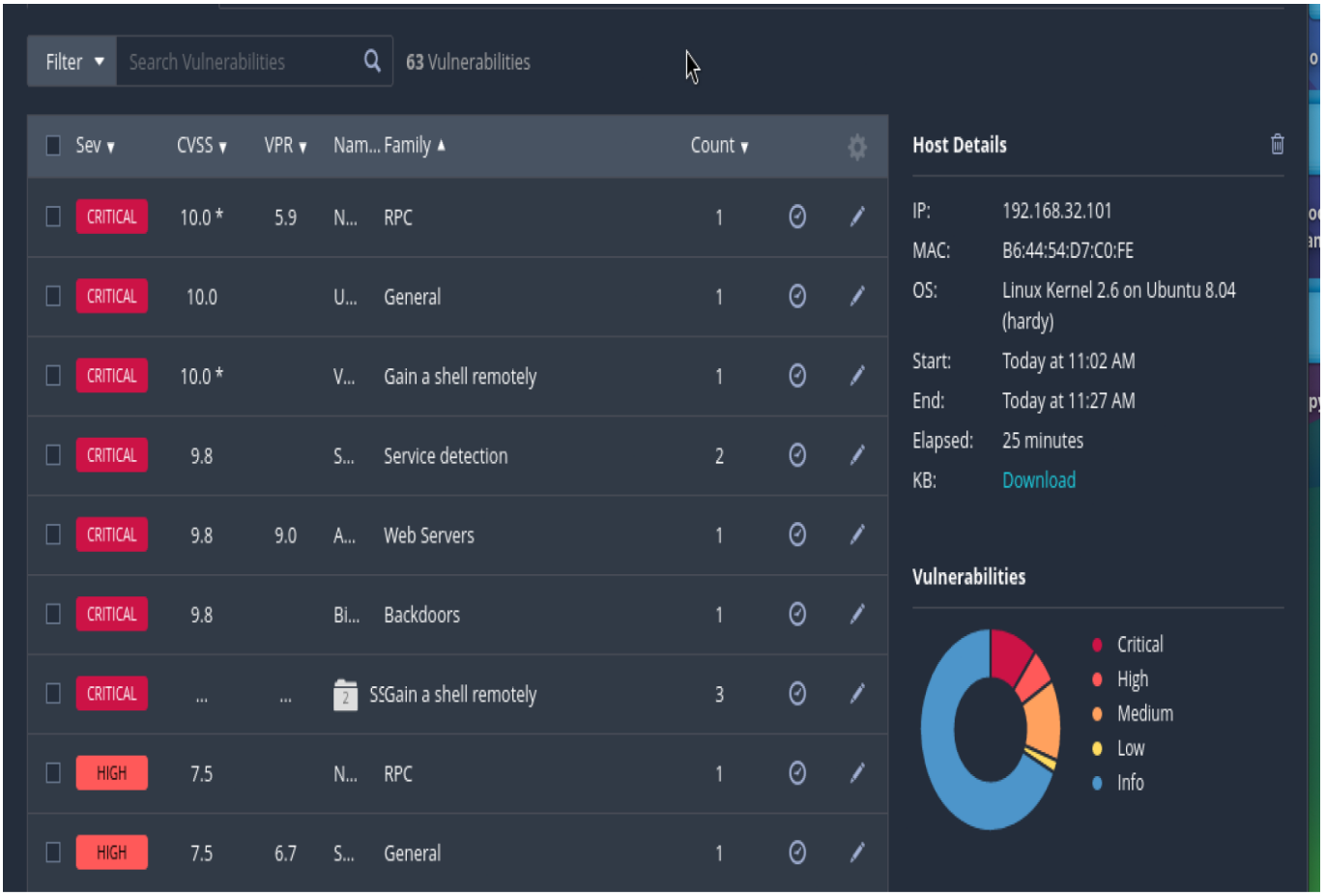
REMEDETION META

Mostriamo uno screenshot dello scanner svolto da Nessus:

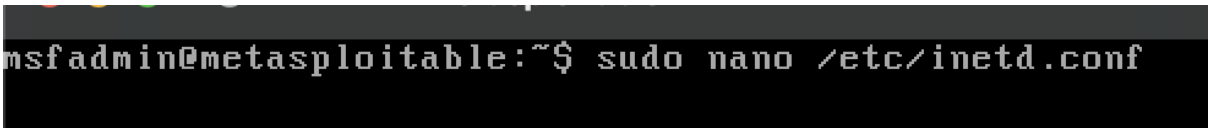


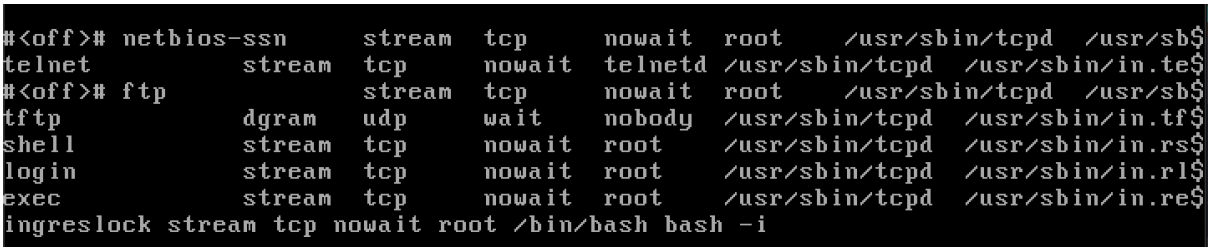
In questa remedetion abbiamo preso in considerazione 3 vulnerabilities:

1. BLIND BACKDOOR SHELL
2. VNC SERVER PASSWORD
3. NFS EXPORT SHARE INFORMATION DISCLOSURE

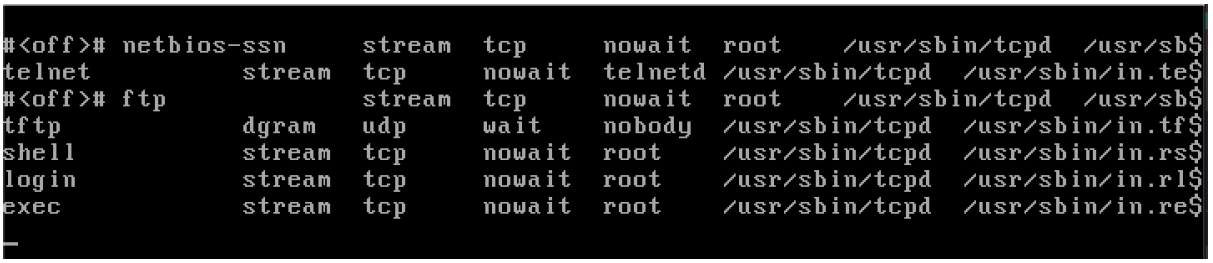
Procediamo in ordine con le procedure per la remedetion:

1.



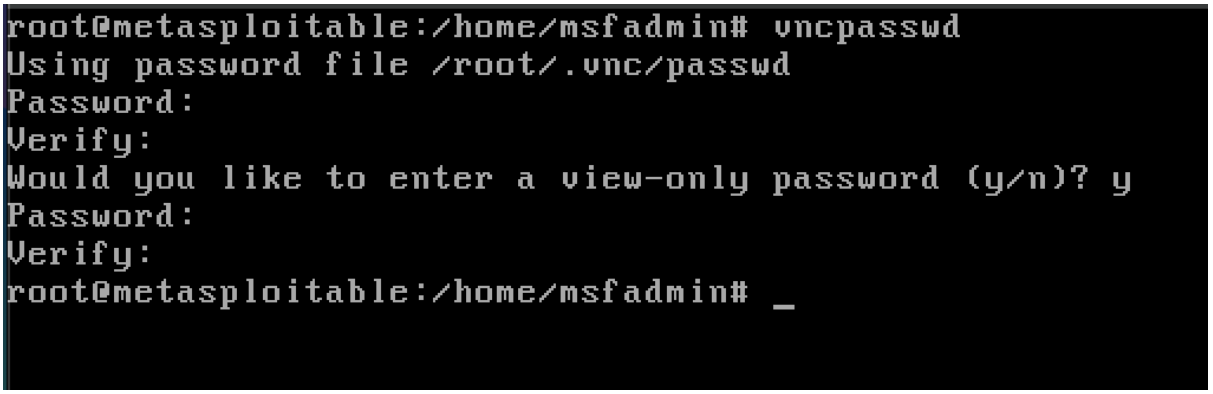


Questa è un Backdoor pre installata sulla nostra macchina Meta, possiamo accedere alla configurazione inetd e cancellando l'ultima riga di testo *ingreslock stream tcp nowait root /bin/bash -i* eliminiamo la backdoor.



2.

Dobbiamo sostituire la password del VNC serve, in quanto 'password' è troppo intuibile ed utilizzata.



Accediamo come admin al settaggio della nuova password: "kalilin" , e concludiamo l'operazione.

3.

Infine andiamo a rendere le share directory del NFS(Network File System)
non accessibili ad altri client, nello specifico andiamo a modificare i privilegi di read and write.

```
msfadmin@metasploitable:~$ sudo nano /etc/exports
```

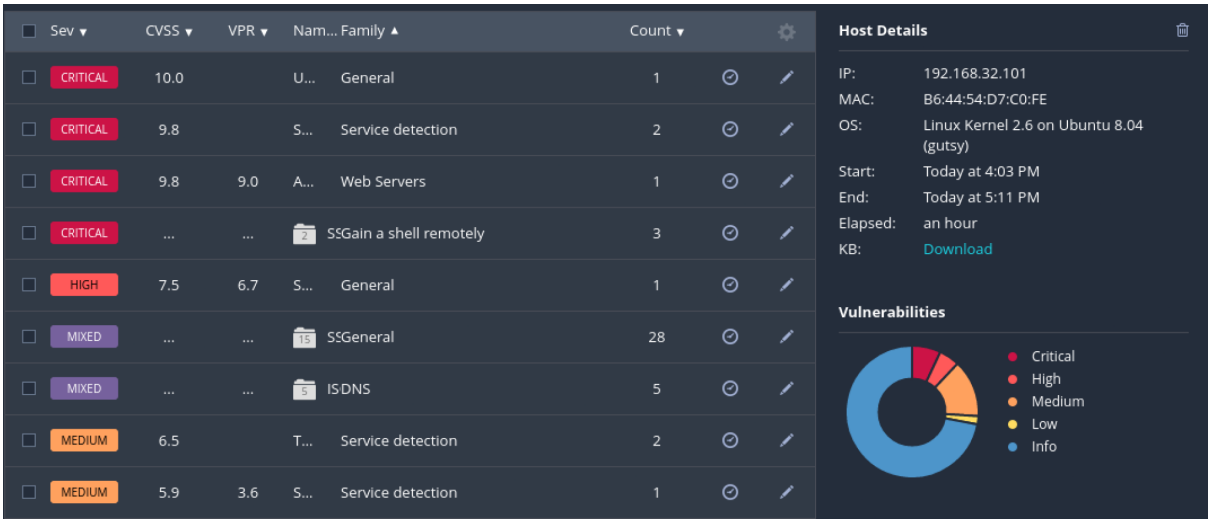
```
  GNU nano 2.0.7                File: /etc/exports

# /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)
#

/       *(--,sync,no_root_squash,no_subtree_check)
```

Nell'ultima riga **(--,sync, no_root_squash,no_subtree_check)* siamo andati a sostituire *rw* con -- a inizio parentesi.

In conclusione mostriamo uno screenshoot dello scanner di Nessus dopo il fix delle vulnerabilities.



Di seguito saranno mostrati i due report completi di Nessus pre e post remedation.

PS: in allegato ci sarà anche un terzo “ScansioneFinale???” report dove dopo aver provato a correggere la vulnerabilità Samba con questa procedure: commentando la linea di codice *username map script = /etc/samba/scripts/mapusers.sh*

```
# This boolean controls whether PAM will be used for password changes
# when requested by an SMB client instead of the program listed in
# 'passwd program'. The default is 'no'.
;   pam password change = no

#username map script = /etc/samba/scripts/mapusers.sh

########## Printing ##########

# If you want to automatically load your printer list rather
# than setting them up individually then you'll need this
;   load printers = yes

# lpr(ng) printing. You may wish to override the location of the
# printcap file
;   printing = bsd
;   printcap name = /etc/printcap

# CUPS printing.  See also the cupsaddsmb(8) manpage in the
```

Da report si evince che sono risultate sistemati anche altre vulnerabilità critiche, che però non erano state prese in considerazione per l’esecuzione dell’esercizio, quali:
Apache Tomcat AJP Connector RequestInjection e Unix Operations System Unsupported Version Detection.
Metre la vulnerabità obiettivo è rimasta.