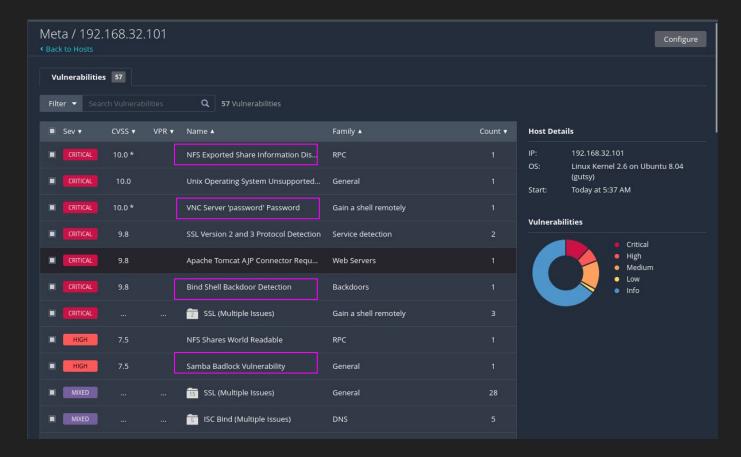
Dopo aver scelto e ricercato cuatri tipi di vulnerabilitá, adesso andiamo a risolvere ogni uno.



Per risolvere la vulnerabilit<u>à sul</u> NFS, andiamo dentro il file exports sul directory /etc. Questo file ci consente di creare una whitelist dei host che possono accedere al NFS. aggiungendo l'ip di metasploitable specifichiamo che solo questo host puo accedere al NFS. Se volessimo che altri host possano accedere a questa lista possiamo aggiungere anche a loro.

```
GNU nano 2.0.7
                            File: /etc/exports
                                                                     Modified
 /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)
/mnt/newdisk
               192.168.32.101(rw,sync,no_root_squash,no_subtree_check)
            TO WriteOut TR Read File Trev Page K Cut Text C Cur Pos
                         "W Where Is "V Next Page "U UnCut Text" To Spell
            1 Justifu
```

Per cambiare la password sul server VNC bastano solo un paio di comandi nella shell. Prima otteniamo privilegi di root, una volta che c'labbiamo possiamo andare al directorio /home/msfadmin/.vnc. e qua che con il comando vncpasswd che possiamo modificare la password, inserendo una alfanumerica randomizzata molto più sicura che non vi dirò.

```
.profile
.gconf
                              sudo
root@metasploitable:/home/msfadmin# systemctl --state
bash: systemctl: command not found
root@metasploitable:/home/msfadmin# sudo .gconf
sudo: .gconf: command not found
root@metasploitable:/home/msfadmin# cd
root@metasploitable: "# ls -A
.bash_history .filezilla .gstreamer-0.10 reset_logs.sh vnc.log
              fluxbox
                          mozilla
                                                          .Xauthority
.hashrc
                                           rhosts
.config
              .gconf .profile
                                           ssh
              gconfd purple
Desktop
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log metasploitable:1.log passwd
metasploitable:0.pid metasploitable:2.log xstartup
root@metasploitable:~/.vnc# vnc Wd
bash: vnc: command not found
root@metasploitable:~/.vnc# vnc passwd
bash: vnc: command not found
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verifu:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc#
```

Nessus ha root@metasploitable:/home/msfadmin# ufw deny 1524 scoperto che la Rule updated bindshell root@metasploitable:/home/msfadmin# ufw status backdoor si Firewall loaded trovava nella porta 1524, per questo possiamo To Action From inserire una regola al firewall 1524:tcp DENY Anywhere di meta *ufw*. 1524:udp DENY Anywhere Con il comando 445:tcp ALLOW Anywhere ufw deny 1524 445:udp ALLOW Anywhere chiudiamo le 139:tcp ALLOW Anywhere comunicazione 139:udp ALLOW Anywhere sulla porta 1524, sia TCP come UDP root@metasploitable:/home/msfadmin#

Per l'ultima vulnerabilità, il badlock al server Samba, esiste una soluzione consigliata per Nessus, che é semplicemente aggiornare la versione del server Samba. Tuttavia. collegare la VM metasploitable a internet potrebbe essere un gran rischio, perciò ho deciso che sarebbe meglio creare una regola

di firewall di

negare la comunicazione sulle porte 445 e 139 139:udp

root@metasploitable:/home/msfadmin# ufw deny 445 Rule updated root@metasploitable:/home/msfadmin# ufw deny 139 Rule updated root@metasploitable:/home/msfadmin# ufw status Firewall loaded Action From To 1524:tcp DENY Anywhere 1524:udp DENY Anywhere DENY 445:tcp Anywhere DENY 445:udp Anywhere 139:tcp DENY Anywhere

Anywhere

DENY

root@metasploitable:/home/msfadmin#