BOSSI ALESSANDRO

REPORT REMEDY ACTIONS

ELENCO CRITICITÀ RISOLTE

01

NFS EXPORTED SHARE INFORMATION DISCLOSURE

02

REXECD SERVICE DETECTION

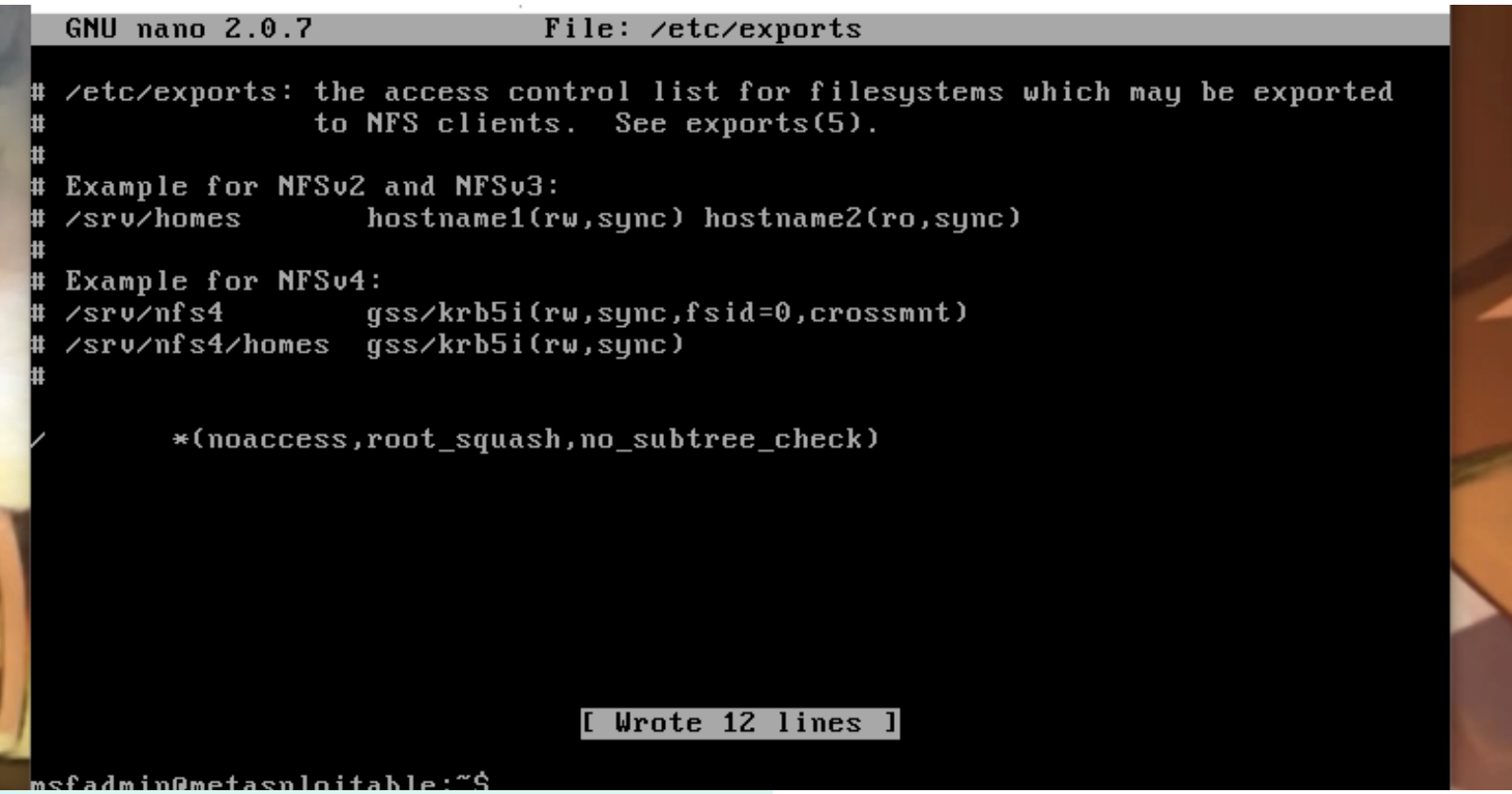
03

VNC SERVICE PASSWORD

04

BIND SHELL BACKDOOR DETECTION

NFS EXPORTED SHARE INFORMATION DISCLOSURE



DESCRIZIONE CRITICITA'

LA CRITICITÀ PERMETTEVA AD UN HOST REMOTO DI ACCEDERE CON PRIVILEGI DI ROOT E DI SCRITTURA TRAMITE L' NFS, CREANDO COSÌ LA POSSIBILITÀ DI LEGGERE E MODIFICARE I FILE SULLA MACCHINA SCANSIONATA.

RISOLUZIONE CRITICITA'

ACCEDENDO AL FILE DI CONFIGURAZIONE PER L'NFS SONO STATI MODIFICATI I PRIVILEGI IN MANIERA TALE DA NON PERMETTERE DI POTERVI ACCEDERE, IN QUESTA MANIERA NON POSSONO ESSERE NE' LETTI NE' MODIFICATI FILE ALL'INTERNO DELLA MACCHINA.

REXECD SERVICE DETECTION

DESCRIZIONE CRITICITA'

SULLA MACCHINA È STATO RILEVATO ATTIVO IL SERVIZIO REXECD CHE PERMETTE DI ESEGUIRE COMANDI DA REMOTO SULLA MACCHINA, TUTTAVIA NON DISPONENDO DI CONTROLLI SULL' AUTENTICAZIONE POTREBBE ESSERE USATO DA UN ATTACCANTE PER CAUSARE DANNI ALLA MACCHINA

RISOLUZIONE CRITICITA'

MODIFICANDO IL FILE DI CONFIGURAZIONE DI INETD È STATO DISTATTIVATO IL SERVIZIO COMMENTANDO LA RIGA DI EXEC.

VNC SERVICE PASSWORD

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  ?R    srv  usr
boot   etc   initrd.img  media       opt        root  sys  var
cdrom  home  lib         mnt         proc       sbin  tmp  vmlinuz
msfadmin@metasploitable:/$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/# cd /root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls
metasploitable:0.log  metasploitable:1.log  metasploitable:2.log  xstartup
```

DESCRIZIONE CRITICITA'

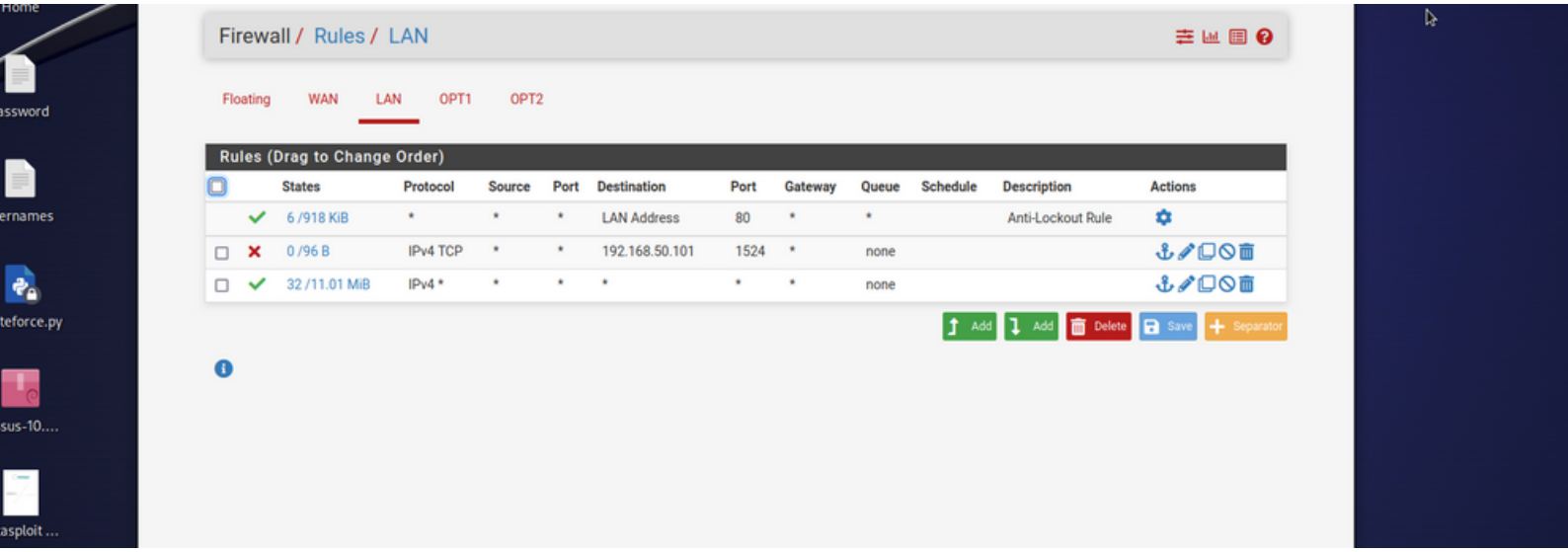
IL SERVER VNC ATTIVO SULLA MACCHINA SCANSIONATA ERA PROVVISTO DI UNA PASSWORD DEBOLE, QUESTO POTEVA PERMETTERE AD UN ATTACCANTE DI ACCEDERVI FACILMENTE

RISOLUZIONE CRITICITA'

ACCEDENDO AL FILE DI CONFIGURAZIONE DEL SERVER VNC CON PRIVILEGI ROOT È STATO POSSIBILE ELIMINARE LA PASSWORD DEBOLE, SUCCESSIVAMENTE È STATA CREATA UNA NUOVA PASSWORD

```
To access official Ubuntu documentation, please vis
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo vncpasswd
[sudo] password for msfadmin:
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)?
msfadmin@metasploitable:~$ sudo vcnpasswd
sudo: vcnpasswd: command not found
msfadmin@metasploitable:~$ sudo vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
```

BIND SHELL BACKDOOR DETECTION



DESCRIZIONE CRITICITA'

LA SCANSIONE HA RILEVATO UNA BACKDOOR ATTIVA SULLA PORTA 1524, COMPROMETTENDO LA SICUREZZA DELLA MACCHINA

RISOLUZIONE CRITICITA'

È STATA CREATA UNA REGOLA DI FIREWALL CHE BLOCCA L'ACCESSO DA QUALSIASI SORGENTE ALLA PORTA 1524 SULLA MACCHINA SCANSIONATA