

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

Meta / 192.168.32.101

[Back to Hosts](#)

Configure

Vulnerabilities 57


Filter Search Vulnerabilities 57 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		NFS Exported Share Information Dis...	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported...	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Apache Tomcat AJP Connector Requ...	Web Servers	1
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
MIXED	15 SSL (Multiple Issues)	General	28
MIXED	5 ISC Bind (Multiple Issues)	DNS	5

Host Details

IP: 192.168.32.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)
Start: Today at 5:37 AM

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Per risolvere la vulnerabilità sul 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)

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

Per cambiare la password sul server VNC bastano solo un paio di comandi nella shell. Prima otteniamo privilegi di root, una volta che c'abbiamo 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.

```
.gconf .profile 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
.bashrc .fluxbox .mozilla .rhosts .Xauthority
.config .gconf .profile .ssh
Desktop .gconfd .purple .vnc
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:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/.vnc# _
```

Nessus ha scoperto che la bindshell backdoor si trovava nella porta 1524, per questo possiamo inserire una regola al firewall di meta ufw.

Con il comando `ufw deny 1524` chiudiamo le comunicazione sulla porta 1524, sia TCP come UDP

```
root@metasploitable:/home/msfadmin# ufw deny 1524
Rule updated
root@metasploitable:/home/msfadmin# ufw status
Firewall loaded
```

To	Action	From
--	-----	----
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere
445:tcp	ALLOW	Anywhere
445:udp	ALLOW	Anywhere
139:tcp	ALLOW	Anywhere
139:udp	ALLOW	Anywhere

```
root@metasploitable:/home/msfadmin#
```

Per l'ultima vulnerabilità, il badlock al server Samba, esiste una soluzione consigliata per Nessus, che è 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

```
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
```

To	Action	From
--	-----	----
1524:tcp	DENY	Anywhere
1524:udp	DENY	Anywhere
445:tcp	DENY	Anywhere
445:udp	DENY	Anywhere
139:tcp	DENY	Anywhere
139:udp	DENY	Anywhere

```
root@metasploitable:/home/msfadmin#
```