

**Consegna
S5/L5**

Remediation Meta

Dopo aver scelto le vulnerabilità, le andiamo a risolvere

Hosts	1	Vulnerabilities	65	Remediations	2	Notes	2	History	1
Filter	Search Vulnerabilities		65 Vulnerabilities						
<input type="checkbox"/> Sev	CVSS	VPR	Name	Family	Count				
<input type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1				
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1				
<input type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1				
<input type="checkbox"/> CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2				
<input type="checkbox"/> CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1				
<input type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1				
<input type="checkbox"/> CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	3				
<input type="checkbox"/> HIGH	7.5		NFS Shares World Readable	RPC	1				
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1				
<input type="checkbox"/> MIXED	15 SSL (Multiple Issues)	General	28				
<input type="checkbox"/> MIXED	5 ISC Bind (Multiple Issues)	DNS	5				

```
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)
#
/mnt/newdisk 192.168.1.101(rw,sync,no_root_squash,no_subtree_check)
```

Per risolvere la vulnerabilità relativa al NFS, ci spostiamo nel file exports all'interno della directory /etc. Questo file ci consente di creare una lista degli host che possono accedere al NFS, aggiungendo l'IP di metasploitable facciamo in modo che solo questo specifico host può accedervi. (Se volessimo estendere questi privilegi ad altri host basterebbe aggiungerli in questa lista).

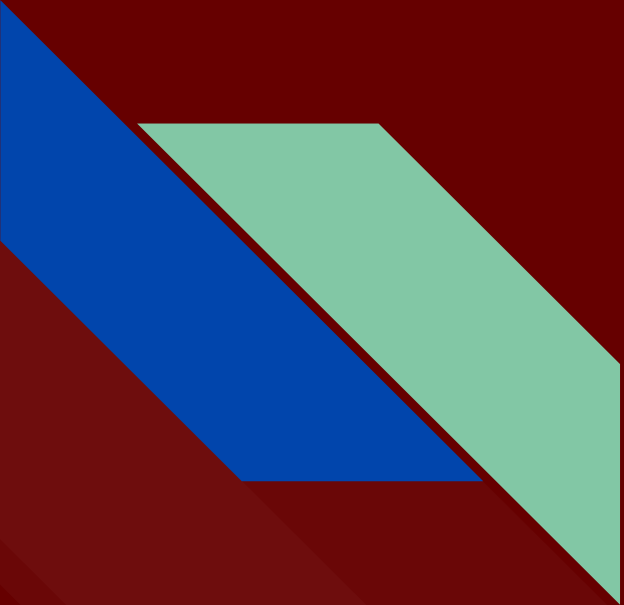
```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# cd
root@metasploitable:~# ls -A
.bash_history  .filezilla  .gstreamer-0.10  reset_logs.sh  vnc.log
.bashrc        .fluxbox    .mozilla         .rhosts        .Xauthority
.config        .gconf      .profile         .ssh
Desktop        .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# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~/vnc#
```

Per cambiare la password sul server VNC bisogna spostarsi nella directory `/home/msfadmin/.vnc` dopo aver ottenuto i privilegi di root. Eseguendo il comando `vncpasswd`, possiamo modificare la password, inserendo una a nostra scelta.

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

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

Nessus ha individuato la bindshell backdoor sulla porta 1524. Possiamo chiudere questa porta modificando una regola del firewall di meta ufw. Con il comando `ufw deny 1524` chiudiamo tutte le trasmissioni sulla porta 1524, sia TCP sia UDP.



```
root@metasploitable:/home/msfadmin# ufw deny 445
Rule added
root@metasploitable:/home/msfadmin# ufw deny 139
Rule added
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

Per la vulnerabilità relativa al server Samba, Nessus suggerisce semplicemente di aggiornare la versione del Server. Però esiste una soluzione che ci permette di evitare questo passaggio che è chiudere le trasmissioni sulle porte 445 e 139. Andremo ad utilizzare gli stessi comandi usati per la vulnerabilità precedente.