

# Progetto 4

- ▀ Vulnerability Scanner  
e risoluzione delle  
criticità

# Primo scan del target: 192.168.1.65

Hosts 1 Vulnerabilities 70 Remediations 2 History 1									
Filter Search Hosts 1 Host									
Host Vulnerabilities									
192.168.1.65 11 7 24 8 135									
Sev	CVSS	VPR	Name			Family	Count		
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure			RPC	1		
CRITICAL	10.0		Unix Operating System Unsupported Version Detection			General	1		
CRITICAL	10.0 *		VNC Server 'password' Password			Gain a shell remotely	1		
CRITICAL	9.8		Bind Shell Backdoor Detection			Backdoors	1		
MIXED	...	...	Apache Tomcat (Multiple Issues)			Web Servers	4		
CRITICAL	...	...	SSL (Multiple Issues)			Gain a shell remotely	3		
MIXED	...	...	SSL (Multiple Issues)			Service detection	3		
HIGH	7.5		NFS Shares World Readable			RPC	1		
HIGH	7.5 *	6.7	rlogin Service Detection			Service detection	1		
HIGH	7.5 *	6.7	rsh Service Detection			Service detection	1		
HIGH	7.5	6.7	Samba Badlock Vulnerability			General	1		
MIXED	...	...	SSL (Multiple Issues)			General	28		
MIXED	...	...	ISC Bind (Multiple Issues)			DNS	5		
MEDIUM	6.5		TLS Version 1.0 Protocol Detection			Service detection	2		



**Come si può vedere sono state riscontrate diverse criticità.**

11 di queste sono risultate critiche e da risolvere al più presto.

Andremo a prendere in esame le prime 3 criticità riscontrate:

- **NFS Exported Share Information Disclosure**
- **VNC Server 'password' Password**
- **Bind Shell Backdoor Detection**
- **rlogin Service Detection**

# NFS Exported Share Information Disclosure

Questa criticità consiste nel problema di accesso al sistema di condivisione file.

Si può notare dalla presenza del '\*' prima della parentesi che non è specificato alcun indirizzo di accesso.

```
GNU nano 2.0.7      File: /etc/exports      Modi:
# /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)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

- Per risolvere la criticità è stato necessario specificare almeno un indirizzo di accesso. In questo caso è stato aggiunto l'indirizzo della macchina virtuale stessa.

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

# /etc/exports: the access control list for filesystems which may be
#                  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)
#
✓ 192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

# VNC Server 'password' Password


Con questa criticità è stato riscontrato un utilizzo di una password troppo debole per l'accesso al server VNC.

Nessus è riuscito ad accedere infatti tramite la password :  
'password'

Per risolvere la criticità si è dovuto intervenire sul file contenente la password di accesso e modificarla.

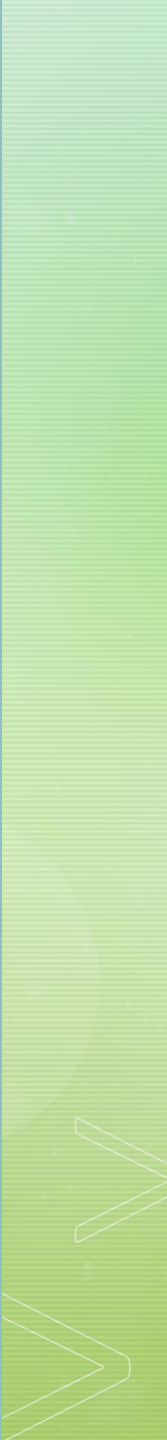
```
root@metasploitable:/usr/share# cd /
root@metasploitable:/# ls
bin      dev      initrd    lost+found  nohup.out  root  sys  var
boot     etc      initrd.img media        opt         sbin  tmp  vmlinuz
cdrom    home     lib       mnt          proc        srv   usr

root@metasploitable:/# cd root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# ls /a
ls: cannot access /a: No such file or directory
root@metasploitable:~# ls -a
.          .config      .gconf      .profile    .ssh
..         Desktop      .gconfd     .purple     .vnc
.bash_history .filezilla   .gststreamer-0.10 reset_logs.sh vnc.log
.bashrc     .fluxbox     .mozilla    .rhosts     .Xauthority
root@metasploitable:~# _
```



Per poter accedere al file contenente la password sono stati necessari i permessi di amministratore. Una volta ottenuti tramite il percorso visibile nell'immagine si può ritrovare il file contenente la password e quindi modificarla.

Una volta salvata la modifica e riavviato il servizio il problema viene risolto.





# Bind Shell Backdoor Detection

Questa particolare criticità indica la presenza di una backdoor di tipo Bind Shell (significa che consente il traffico verso la macchina su cui è aperta).

Nessus ha trovato questa Backdoor sulla porta 1524.

Provando inizialmente a risolvere il problema tramite la chiusura della porta si è riscontrato che al riavvio della macchina il problema si ripresentava. Si è visto quindi necessario intervenire tramite firewall.

È stato scelto il firewall UFW, e una volta installato sulla macchina Metasploit è stata creata la regola per impedire il traffico sulla porta incriminata.



Usage: ufw COMMAND

Commands:

enable	Enables the firewall
disable	Disables the firewall
default ARG	set default policy to ALLOW or DENY
logging ARG	set logging to ON or OFF
allow deny RULE	allow or deny RULE
delete allow deny RULE	delete the allow/deny RULE
status	show firewall status
version	display version information

root@metasploitable:/# sudo ufw deny 1524

Rules updated

Firewall loaded

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

Una volta creata la regola la macchina si può considerare risolta la criticità.

# ■ rlogin Service Detection

L'ultima minaccia presa in considerazione o il servizio rlogin.

È stata classificata dal VA Nessus come una minaccia di grado alto e non critico a differenza delle altre ma è bene cercare di risolvere anche questa nel minor tempo possibile. Infatti un possibile 'man in the middle' potrebbe sfruttarla per intercettare dati e non di meno nomi utenti e password visto che i dati che vengono trasmessi tramite questo servizio non sono criptati.


La soluzione a questo problema risiede nella disattivazione del servizio rlogin. Per far cio si è dovuto intervenire sul file stesso.

Una volta commentata la stringa interessata e riavviato il servizio il problema risulta risolto.

```
GNU nano 2.0.7          File: /etc/inetd.conf          Modified
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.tftpd$
telnet                  stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd$
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd$
tftp                   dgram  udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tftpd$
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd$
login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind$
exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd$
ingreslock stream tcp nowait root /bin/bash bash -i
```

# Scansione Finale e Report aggiornato.

Host		Vulnerabilities ▼				
<input type="checkbox"/>	192.168.1.65	8	5	24	8	141
<input type="checkbox"/> Sev ▼	CVSS ▼	VPR ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 Apache Tomcat (Multiple Issues)	Web Servers	4	🔄 ✎
<input type="checkbox"/> CRITICAL	...	...	📁 SSL (Multiple Issues)	Gain a shell remotely	3	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 SSL (Multiple Issues)	Service detection	3	🔄 ✎
<input type="checkbox"/> HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1	🔄 ✎
<input type="checkbox"/> HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 SSL (Multiple Issues)	General	28	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 ISC Bind (Multiple Issues)	DNS	5	🔄 ✎
<input type="checkbox"/> MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	🔄 ✎
<input type="checkbox"/> MEDIUM	6.5		Unencrypted Telnet Server	Misc.	1	🔄 ✎
<input type="checkbox"/> MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 SSH (Multiple Issues)	Misc.	6	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 HTTP (Multiple Issues)	Web Servers	5	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 SMB (Multiple Issues)	Misc.	2	🔄 ✎
<input type="checkbox"/> MIXED	...	...	📁 TLS (Multiple Issues)	Misc.	2	🔄 ✎



Si può apprezzare a colpo d'occhio la diminuzione delle vulnerabilità riscontrate della scansione. In particolar modo la risoluzione delle vulnerabilità critiche ad alte citate sopra. Viene allegata anche una copia dettagliata del report Nessus iniziale e finale per ulteriore completezza.

