## **M3 D8**

## **ESERCIZIO**

# **GIORNO 5 – PROGETTO**

Scansione completa da Kali con tool Nessus verso la macchina virtuale Metasploitable. Diverse criticità e vulnerabilità sono state trovate, dalle più gravi alle meno importanti (raffigurate con colore rosso le principali dove porre rimedio fino alle azzurre – le più innocue).

Obiettivo: Provare ad implementare delle azioni di rimedio (remediation actions) e verificare che le vulnerabilità siano state fixate.

## **PUNTO 1:**

Elenco delle vulnerabilità trovate, specialmente le più gravi da segnalare, e riportate sul report (specialmente report tecnico dove segnalare il problema e possibile azione correttiva da implementare).

				192.168.50.10	1	
8		4		17		72
CRITI	CAL		HIGH	MEDIUM	LOW	INFO
Vulnerabilitie	es					Total: 10
SEVERITY	CVSS V3.0	VPR	PLUGIN	NAME		
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connect	or Request Injection	(Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection	1	
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol	Detection	
CRITICAL	10.0	-	33850	Unix Operating System Unsup	oported Version Dete	ection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL F Weakness	ackage Random N	umber Generator
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL F Weakness (SSL check)	Package Random N	umber Generator
CRITICAL	10.0*	5.9	11356	NFS Exported Share Informat	ion Disclosure	
CRITICAL	10.0*	-	61708	VNC Server 'password' Passw	vord	
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade	/ Reflected DoS	
HIGH	7.5	-	42256	NFS Shares World Readable		
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher	Suites Supported (S	SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability		

## **PUNTO 2:**

Analizzare le varie vulnerabilità e provare a porre azioni di rimedio su Metasploitabe. Le vulnerabilità analizzate hanno un' alta criticità e sono riportate in tabella.

□ Se	2V <b>▼</b>	Score <b>▼</b>	Name ▲
	CRITICAL	10.0 *	NFS Exported Share Information Disclosure
	CRITICAL	10.0 *	rexecd Service Detection
	CRITICAL	10.0	Unix Operating System Unsupported Version Detection
	CRITICAL	10.0 *	VNC Server 'password' Password
	CRITICAL	9.8	Bind Shell Backdoor Detection

## SETTAGGIO REGOLA FIREWALL

(scansione ci aveva dato una data porta aperta e noi col firewall Metaspl la filtriamo)

Comando da Metaspl: sudo ufw enable / sudo ufw deny

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw deny 5900
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 8009
Rule added
msfadmin@metasploitable:~$ sudo ufw status numbered
Firewall loaded
To
                            Action
                                    From
5900:tcp
                            DENY
                                    Anywhere
5900:udp
                            DENY
                                    Anywhere
8009:tcp
                            DENY
                                    Anywhere
8009:udp
                            DENY
                                    Anywhere
msfadmin@metasploitable:~$
Apri nel browser
```

#### 9.8 51988 BIND SHELL BACKDOOR DETECTION

Impostare regola firewall nella directory ETC/INIT.D tramite il seguente comando: ip tables -A INPUT -p tcp - -dport 1524 -j DROP.

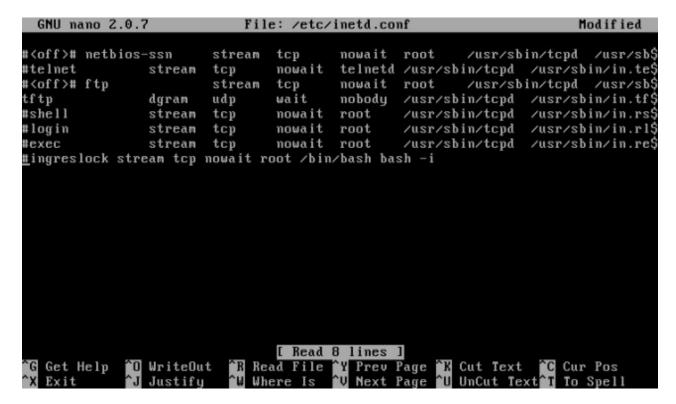
La porta segnalata dalla vulnerabilità è stata così chiusa.

Per forzare la macchina a caricare la regola al boot vado a modificare il file RC.LOCAL

```
GNU nano 2.0.7
                             File: /etc/rc.local
                                                                       Modified
 By default this script does nothing.
loadkeys it
nohup /usr/bin/rmiregistry >/dev/null Z>&1 &
nohup /usr/bin/unrealircd &
rm -f /root/.vnc/*.pid
HOME=/root LOGNAME=root USER=root nohup /usr/bin/vncserver :0 >/root/vnc.log 2>$
nohup /usr/sbin/druby_timeserver.rb &
iptables-restore < /etc/init.d/fwrules
exit 0
  Get Help
             O WriteOut
                          ^R
                             Read File 📉 Prev Page
                                                    TR Cut Text
                                                                  ^C
                                                                     Cur Pos
                             Where Is
                                          Next Page
                                                       UnCut Text
```

Aggiungere la riga iptables-restore</etc/init.d/fwrules

Per rimediare ad altri eventuali problemi di backdoor presenti nel report disattivare alcuni dei servizi in ascolto modificando il file INETD.CONF come seguente:



## 10.0\* 61708 VNC SERVER 'password' PASSWORD

```
root@metasploitable:~# sudo vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```

Per risolvere la vulnerabilità della password, vado a modificare il file PASSWD nella directory /ROOT/.VNC/ e lo applico poi eseguendo il comando: sudo passwd

#### 10.0\* 11356 NFS EXPORTED SHARE INFORMATION DISCLOSURE

```
GNU nano 2.0.7
                                                                      Modified
                            File: /etc/exports
 /etc/exports: the access control list for filesystems which may be exported
                to MFS clients. See exports(5).
 Example for NFSv2 and NFSv3:
 /srv/homes
                  hostname1(rw,sync) hostname2(ro,sync)
 Example for NFSv4:
                  gss/krb5i(rw,sync,fsid=0,crossmnt)
 /sru/nfs4
 /srv/nfs4/homes gss/krb5i(rw,sync)
       *(rw,sync,no_root_squash,no_subtree_check)
File Name to Write: /etc/exports
G Get Help
                   To Files
                                        M-M Mac Format
                                                               Prepend
                    1-D DOS Format
```

Rimuovere cartella ROOT dal file EXPORTS per risolvere la vulnerabilità.

**PUNTO 3:** 

Scansione post – remediation actions ci porterà la presenza di un numero minore di vulnerabilità.

5	3	17		72
CRITICAL	HIGH	MEDIUM	LOW	INFO

uli ici abiliuc	_			Total. 10
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability