

M3-W12D4 – Progetto fine modulo

DATA

Cybersecurity Analyst

Studente:

Andrea Scarmagnani

Docente:

Federico Daidone

Traccia:

Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

Consegna:

1. Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - **ScansioneInizio.pdf**
2. Screenshot e spiegazione dei passaggi della remediation - **RemediationMeta.pdf**
3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - **ScansioneFine.pdf**

Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

Macchina analizzata: Metasploitable
Indirizzo IP: 192.168.50.1

Macchina attaccante: Kali
Indirizzo IP: 192.168.1.10

Qui sotto evidenza degli indirizzi IP delle due macchina:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
    inet 192.168.1.10 netmask 255.255.255.0
    inet6 fe80::27b7:8c05:3ac8:17a7 prefixlen 64
    ether 08:00:27:13:f1:7f txqueuelen 1000
    RX packets 81818 bytes 122374990 (116.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22666 bytes 1619872 (1.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0
```

Epicode-Metasploitable2 [In esecuzione] - Oracle VM

File	Macchina	Visualizza	Inserimento	Dispositivi	Aiuto
DHCP OFFER of 192.168.50.100 from 192.168.50.1					
DHCP REQUEST of 192.168.50.100 on ethernet0					
DHCP ACK of 192.168.50.100 from 192.168.50.1					
bound to 192.168.50.100 -- renewal time: 1800					
msfadmin@metasploitable:/etc/grub.d					
eth0 Link encap:Ethernet HWaddr 08:00:27:13:f1:7f					
inet addr:192.168.50.100					

Qui sotto le principali vulnerabilità trovate nella macchina:

192.168.50.100

8	4	16	6	69
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
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 (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

Per il progetto si andrà risolvere le prime 4 vulnerabilità in particolare le qui sotto citate:

Host 192.168.50.100				
Plugin ID	Risk	CVSS	Name	Synopsis
11356	Critical	10.0	NFS Exported Share Information Disclosure	It is possible to access NFS shares on the remote host.
61708	Critical	10.0	VNC Server 'password' Password	A VNC server running on the remote host is secured with a weak password.
51988	Critical	9.8	Bind Shell Backdoor Detection	The remote host may have been compromised.
32321	Critical	10.0	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	The remote SSL certificate uses a weak key. Riferita a postgresql porta 5432 + smtp 25
32314	Critical	10.0	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	The remote SSL certificate uses a weak key. Porta 22 ssh
1348622	Critical	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	There is a vulnerable AJP connector listening on the remote host.
20007	Critical	9.8	SSL Version 2 and 3 Protocol Detection Porta 25	The remote service encrypts traffic using a protocol with known weaknesses.

La vulnerabilità 20007 + 32321 + 32314 sono collegate, ho cercato di sistemarle insieme.

Vulnerabilità trovate dopo le prime sistemazioni:

Host 192.168.50.100				
Plugin ID	Risk	CVSS	Name	Synopsis
46882	Critical	10.0	UnrealIRCd Backdoor Detection	The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Plugin ID	Risk	CVSS	Name	Synopsis
11356	Critical	10.0	NFS Exported Share Information Disclosure	It is possible to access NFS shares on the remote host.

La soluzione di questa vulnerabilità sta nel sistemare il file di configurazione dei permessi situato nel

File di configurazione di NSF: >>> /etc/exports

Una volta entrati si deve commenta la riga, oppure si inserisce chi può eseguire questo tipo di controllo.

```
# /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)
```

```
msfadmin@metasploitable:/etc/init.d$ cat /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)
#
# / *(rw,sync,no_root_squash,no_subtree_check)
# / 192.168.50.99(rw,sync,no_tooy_sqasg,no_subtree_check)
msfadmin@metasploitable:/etc/init.d$ _
```

Commentando con un # oppure definendo l'Host di chi può avere i diritti.

Riavviata la macchina per rendere effettive le modifiche.

Plugin ID	Risk	CVSS	Name	Synopsis
61708	Critical	10.0	VNC Server 'password' Password	A VNC server running on the remote host is secured with a weak password.

Dopo un'attenta analisi ho scoperto che il sistema ha due account, (msfadmin e user)
Oltre a cambiare le password a questi due account va cambiata la password anche all'utente root.
Sostituita la password la vulnerabilità è stata risolta.

Porta 5900

Sostituita la password con il comando >>> vncpasswd: EpiCode2023

Plugin ID	Risk	CVSS	Name	Synopsis
51988	Critical	9.8	Bind Shell Backdoor Detection	The remote host may have been compromised.

Nella porta 1524 c'è un processo in esecuzione che rimane in ascolto.

Cerco il processo in ascolto nella porta con il comando:

`netstat -tuln | grep "1524"`

si evidenzia un processo di nome "xinetd"

```
msfadmin@metasploitable:~$ ps aux | grep "xinetd"
root      4690  0.0  0.0   2424   864 ?        Ss   04:02   0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
msfadmin  6461  0.0  0.0   3004   756 tty1    R+   04:34   0:00 grep xinetd
msfadmin@metasploitable:~$ find
```

Identificato il file termino il processo con

>>>Sudo Kill -9 4690

Una volta fatto cerco ed elimino il programma che va in esecuzione:

```
msfadmin@metasploitable:~$ sudo find / -type d -name "xinetd"
/usr/share/doc/xinetd
msfadmin@metasploitable:~$
```

Cerco ogni tipo di file:

```
msfadmin@metasploitable:~$ sudo find / -type f -name "xinetd"
/usr/sbin/xinetd
/etc/init.d/xinetd
/etc/default/xinetd
```

Elimino tutto, Nel mio caso ho spostato tutto in una cartella che non va in esecuzione automatica, così da poter analizzare il tutto.

Processi terminati:

```
msfadmin 6513  0.0  0.0   3004   756 tty1    R+   04:46   0:00 grep xinetd
[21]+  Killed                  nano /etc/init.d/xinetd (wd: ~)
(wd now: /etc/init.d)
msfadmin@metasploitable:/etc/init.d$ ps aux | grep "xinetd"
msfadmin 6515  0.0  0.0   3004   752 tty1    R+   04:46   0:00 grep xinetd
msfadmin@metasploitable:/etc/init.d$
```

Plugin ID	Risk	CVSS	Name	Synopsis
32321	Critical	10.0	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	The remote SSL certificate uses a weak key.

Porta 5432 – PostGresSQL

PostGresSql è configurato per modificare la cartella propria.

Quindi un malintenzionato può caricare un payload a proprio vantaggio.

Nel file di configurazione/etc/postgresql/8.3/main/postgresql.conf va cambiata la destinazione dei sorgenti e ho spostato i file in un'altra cartella.

```
GNU nano 2.0.7 File: /etc/postgresql/8.3/main/postgresql.conf

# take effect.

# Any parameter can also be given as a command-line option to the server, e.g.,
# "postgres -c log_connections=on". Some parameters can be changed at run time
# with the "SET" SQL command.

# Memory units: kB = kilobytes MB = megabytes GB = gigabytes
# Time units:   ms = milliseconds s = seconds min = minutes h = hours d = days

-----
# FILE LOCATIONS
-----

# The default values of these variables are driven from the -b command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/8/main'      # use data in another d
# (change requires restart)
hba_file = '/etc/postgresql/8.3/main/pg_hba.conf' # host-based authentica
```

Arginato il problema della porta 5432 ma non quella della porta 25.

Per quest'ultima porta è stato optato un filtro firewall, vedo in fondo

-È stato arginato anche il problema del Telnet dove ci si poteva connettere in tutta semplicità.
Commentando la riga.

```
GNU nano 2.0.7 File: /etc/inetd.conf

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
#telnet                 stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/
tftp                   dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf
shell                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
exec                   stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
ingreslock stream tcp nowait root /bin/bash bash -i
```

Plugin ID	Risk	CVSS	Name	Synopsis
1348622	Critical	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	There is a vulnerable AJP connector listening on the remote host.

Nota: Sistemata questa vulnerabilità si è chiusa anche la vulnerabilità

1348622 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Credo perché non essendo più accessibile la macchina dalla porta 2049 / udp / rpc-nfs

Si è arginato il problema delle altre macchine.

Vulnerabilità trovate dopo le prime sistemazioni:

Host	192.168.50.100			
Plugin ID	Risk	CVSS	Name	Synopsis
46882	Critical	10.0	UnrealIRCd Backdoor Detection	The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Con netstat controllo quale software c'è in esecuzione nella porta 6667:

```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep "6667"
tcp        0      0 0.0.0.0:6667          0.0.0.0:*            LISTEN
4796/unrealircd
```

Con ps controllo il pid e dove si trova il programma:

```
msfadmin@metasploitable:~$ ps aux | grep "unreal*"
root      4796    0.0  0.0  8540  2664 ?        S    10:02   0:00 /usr/bin/unrealircd
msfadmin  5734    0.0  0.0   3004   756 tty1    R+   10:21   0:00 grep unreal*
```

Cerco il programma all'interno del sistema:

```
msfadmin@metasploitable:~$ sudo find / -type f -name "unreal*"
/usr/bin/unrealircd
/etc/unreal/networks/unreal-test.network
/etc/unreal/unrealircd.conf
/etc/unreal/doc/unreal32docs.html
/etc/unreal/unreal
msfadmin@metasploitable:~$
```

Chiudo il processo con Kill

Sudo kill -9 4796

```
msfadmin@metasploitable:/usr/bin$ sudo kill -9 4796
msfadmin@metasploitable:/usr/bin$ ps aux | grep "unreal*"
msfadmin  5745    0.0  0.0   3004   756 tty1    R+   10:25   0:00 grep unreal*
```

Elimino il programma dall'esecuzione automatica

```
msfadmin@metasploitable:/usr/bin$ sudo rm unrealircd
msfadmin@metasploitable:/usr/bin$ sudo find / -type d -name "unreal*"
/etc/unreal
msfadmin@metasploitable:/usr/bin$ sudo find / -type f -name "unreal*"
/etc/unreal/networks/unreal-test.network
/etc/unreal/unrealircd.conf
/etc/unreal/doc/unreal32docs.html
/etc/unreal/unreal
```

Eliminato tutto riavvio la macchina e il processo non è più in esecuzione.

Host 192.168.50.100				
Plugin ID	Risk	CVSS	Name	Synopsis
20007	Critical	9.8	SSL Version 2 and 3 Protocol Detection Porta 25	The remote service encrypts traffic using a protocol with known weaknesses.

Ho bloccato la porta con il firewall, non è il massimo ma almeno provvisoriamente la vulnerabilità è stata bloccata.

Conclusione:

Molte vulnerabilità si possono risolvere aggiornando l'intero sistema operativo e installando gli aggiornamenti dei software. Volutamente ho cercato di non farlo per vedere se ci fosse la possibilità di arginare lo stesso i vari problemi. Questo perché ho provato immedesimarmi in una situazione dove la macchina deve per forza andare e un aggiornamento del sistema operativo completo potrebbe aver causato il fermo macchina, per incompatibilità dei software nuovi oppure per mancanza di tempo nel poter riconfigurare tutti i servizi.

La 32314 sembra essere un falso positivo, anche se ad oggi non ho modo di verificare.

192.168.50.100



Vulnerabilities

Total: 66

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled

Cybersecurity Analyst 2023