Progetto Week 5 - Remediation Meta + Scansione Fine su Nessus

1- Remediation Bind Shell Detection

Con Nmap e inserendo l'indice -sV, ho scansionato la macchina Metasploitable, in cerca della backdoor. Dopo averla trovata ho utilizzato il comando netcat per stabilire una connessione TCP sulla porta 1524 dell'indirizzo IP 192.168.50.101, che corrisponde, appunto, all'istanza di Metasploitable trovata. Una volta stabilita la connessione, ho inserito alcuni comandi per verificare la connessione e per eseguire alcune operazioni sul sistema remoto.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 12:47 EST
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 12:50 (0:00:07 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 12:50 (0:00:00 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql?
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linu

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 185.93 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ netcat 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# hostname
metasploitable
```

Ps. Ho provato a giocare un pò sulla backdoor fino a trovare il file /root/.vnc/metasploitable:0.log. Leggendolo mi escono una serie infinite di informazioni, tra le quali noto che il server VNC sta ascoltando le connessioni sulla porta tcp 5900

```
root@metasploitable:/root# cd /root/.vnc/metasploitable:0.log
bash: cd: /root/.vnc/metasploitable:0.log: Not a directory
root@metasploitable:/root# cat /root/.vnc/metasploitable:0.log
27/02/23 11:18:14 Xvnc version 3.3.tight1.2.9
27/02/23 11:18:14 Copyright (C) 1999 AT&T Laboratories Cambridge.
27/02/23 11:18:14 Copyright (C) 2000-2002 Constantin Kaplinsky.
27/02/23 11:18:14 All Rights Reserved.
27/02/23 11:18:14 See http://www.uk.research.att.com/vnc for information on VNC
27/02/23 11:18:14 See http://www.tightvnc.com for TightVNC-specific information
27/02/23 11:18:14 Desktop name 'X' (metasploitable:0)
27/02/23 11:18:14 Protocol version supported 3.3
27/02/23 11:18:14 Listening for VNC connections on TCP port 5900
Font directory '/usr/X11R6/lib/X11/fonts/Type1/' not found - ignoring
```

Ad ogni modo il mio obiettivo è quello di eliminare la vulnerabilità, dunque, andando sul terminale di Meta, vado a cercare la backdoor:
[Dopo aver mandato il comando **sudo netstat -tuln** che mi elenca tutte le porte in ascolto, identifico il processo accanto alla porta 1524 e il relativo PID che inserisco nel seguente codice al posto dell'asterisco: **sudo ps -p <*> -o cmd**. Nella colonna cmd mi esce il nome del file contenente la backdoor /etc/inetd.conf, che vado dunque a cercare da terminale meta nella directory /etc].
Modifico il file inetd.conf con nano utilizzando #, rendendo vuoto il file, come di seguito:

```
  GNU nano 2.0.7              File: inetd.conf                          Modified

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
#telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb$
#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
```

2- Remediation Nfs Exported Share Information Disclosure

Sulla directory /etc cerco il file exports e lo apro con l'editor di testo per visualizzare il suo contenuto.

```
-r--r-----  1 root     root      470 2010-03-16 19:13 sudoers
-rw-r--r--  1 root     root       19 2008-03-06 04:31 su-to-rootrc
-rw-r--r--  1 root     root     2405 2008-03-13 18:24 sysctl.conf
-rw-r--r--  1 root     root     1614 2007-11-23 04:06 syslog.conf
drwxr-xr-x  2 root     root     4096 2010-03-16 18:59 terminfo
-rw-r--r--  1 root     root       11 2010-03-16 19:01 timezone
drwxr-x---  4 tomcat55 adm      4096 2023-02-27 11:18 tomcat5.5
-rw-r--r--  1 root     root     1260 2008-02-21 02:22 ucf.conf
drwxr-xr-x  3 root     root     4096 2010-03-16 19:01 udev
drwxr-xr-x  2 root     root     4096 2010-03-16 19:11 ufw
drwx------  7 root     root     4096 2012-05-20 14:17 unreal
-rw-r--r--  1 root     root      214 2008-03-08 13:22 updatedb.conf
drwxr-xr-x  2 root     root     4096 2010-03-16 19:11 update-manager
drwxr-xr-x  2 root     root     4096 2010-03-16 19:00 vim
-rw-r--r--  1 root     root     4430 2012-05-20 14:19 vsftpd.conf
drwxr-xr-x  2 root     root     4096 2010-03-16 19:11 w3m
```

```
-rw-r--r--  1 root     root     4221 2007-06-18 05:45 wgetrc
drwxr-xr-x  2 root     root     4096 2010-03-16 19:01 wpa_supplicant
drwxr-xr-x 10 root     root     4096 2012-05-20 14:44 X11
-rw-r--r--  1 root     root      289 2012-05-20 14:14 xinetd.conf
drwxr-xr-x  2 root     root     4096 2012-05-20 14:17 xinetd.d
-rw-r--r--  1 root     root      461 2008-04-03 15:33 zsh_command_not_found
msfadmin@metasploitable:/etc$ find exports
exports
msfadmin@metasploitable:/etc$
```

```
  GNU nano 2.0.7                File: 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)
```

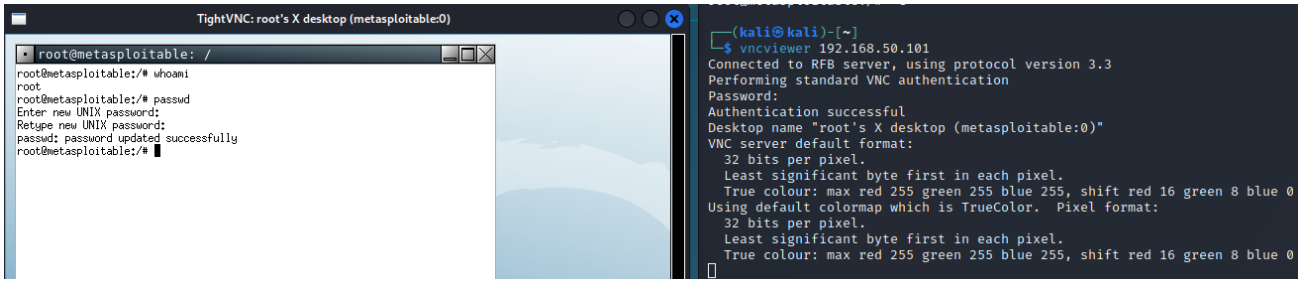
Sulla riga dove ho inserito una x rossa, vi è un codice che indica che il filesystem deve essere montato nella root del client, il quale avrà permessi di lettura e scrittura sul filesystem. Inoltre, l'utente root ha gli stessi privilegi del root sul server.
Piu precisamente:

- "rw" sta per "read-write", ovvero il client può leggere e scrivere su questo filesystem.
- "sync" indica che le operazioni di scrittura sono eseguite in modo sincrono.
- "no_root_squash" indica che l'utente root sul client ha gli stessi privilegi dell'utente root sul server
- "no_subtree_check" evita di controllare se file o directory siano già sottodirectory di un altro filesystem.

Rendendo la riga un commento, con l'utilizzo del #, il codice diventa inefficace.

3- Remediation VNC Server 'password' Password

Da terminale kali (lato attaccante), con il comando vncviewer seguito dall'ip di meta riesco a connettermi al server usando la password "password". Automaticamente si apre la finestra del root che appare a sinistra, dalla quale procedo, anzitutto, a identificarmi, per poi cambiare la password. La nuova password è 0CHpaSsR4!



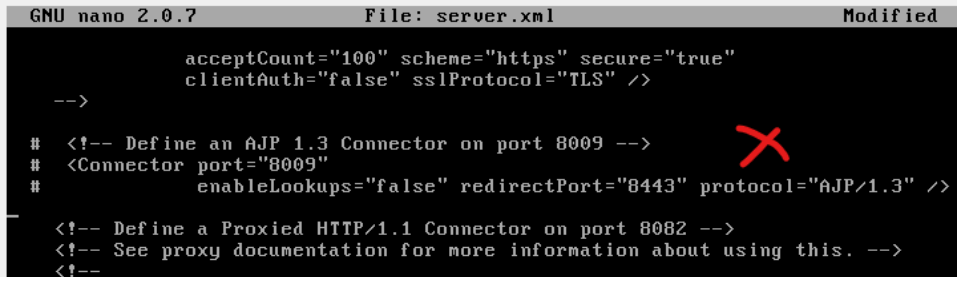
L'ho modificata anche da terminale meta (lato difensore), dove sarebbe stato saggio cambiare la pass nel seguente modo:

```
root@metasploitable:/# cd home
root@metasploitable:/home# ls
ftp  msfadmin  service  user
root@metasploitable:/home# cd msfadmin
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin#
```

4- Remediation Apache Tomcat AJP Connector Request Injection (Ghostcat)

Dopo aver trovato il file server.xml sulla directory tomcat5.5, lo apro con editor di testo. Al suo interno ci sono circa 400 righe, all'interno delle quali, ho cercato l'ajp Connector, per disattivarlo.

```
tomcat5.5/Catalina/localhost/balancer.xml
tomcat5.5/Catalina/localhost/webdav.xml
tomcat5.5/Catalina/localhost/host-manager.xml
tomcat5.5/Catalina/localhost/manager.xml
tomcat5.5/Catalina/localhost/ROOT.xml
tomcat5.5/tomcat5.5
tomcat5.5/context.xml
tomcat5.5/web.xml
tomcat5.5/policy.d
tomcat5.5/policy.d/10admin.policy
tomcat5.5/policy.d/02debian.policy
tomcat5.5/policy.d/04webapps.policy
tomcat5.5/policy.d/50user.policy
tomcat5.5/policy.d/01system.policy
tomcat5.5/policy.d/03catalina.policy
tomcat5.5/catalina.policy
tomcat5.5/tomcat-users.xml
tomcat5.5/logging.properties
tomcat5.5/server-minimal.xml
root@metasploitable:/etc# find server.xml
find: server.xml: No such file or directory
root@metasploitable:/etc# cd tomcat5.5
root@metasploitable:/etc/tomcat5.5# find server.xml
server.xml
root@metasploitable:/etc/tomcat5.5# sudo nano server.xml
```



```
<Connector port="8082"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

Scansione finale su Nessus

Si evidenzia infine come le 4 vulnerabilità risolte, non siano piu presenti nella scansione.