



Riccardo Agostino
Monti

S7 L2

HACKING CON

METASPLOIT

Scopo del test

Nell'esercizio di oggi ci viene chiesto di collegarci alla macchina Metasploitable utilizzando telnet dal framework di metasploit.

afeSEH	ASLR	NXCompat	OS DLL	Version	Path
True	False	False	True	5.1.2600	... (C:\WINDOWS\Files\Audio.dll)
True	False	False	False	-1.0- [SDL.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	6.00.2900.	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512	(C:\WINDOWS\SYSTEM32)
True	False	False	True	8.00.6001.18702	(C:\WINDOWS\SYSTEM32)
False	False	False	False	1.2.12.0 [SDL.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [InetAPI.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [RPCRT4.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [xpsp2.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	False	1.0.0.402 [SysInfo.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	7.0.2600.5512 [msvcrtd.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	False	0.0.22.5506 [AudioCoder.exe]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [RPCRT4.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [ntdll.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	False	-1.0- [libxml2.dll]	(C:\Program Files)
True	False	False	True	5.1.2600.5512 [wshtcpip.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	8.00.6001.18702 [ieframe.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [sensapi.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [RASAPI32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	8.00.6001.18702 [iertutil.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [IMAGEHELP.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [rasadhlp.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [Secur32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [WSOCK32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	6.00.2900.5512 [shdocvw.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [WS2HELP.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [ole32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [IMM32.DLL]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [hnetcfg.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [USER32.dll]	(C:\WINDOWS\SYSTEM32)
False	False	False	False	1.18 [libiconv-2.dll]	(C:\Program Files)
False	True	False	False	5.1.2600.5512 [CRYPTUI.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [rtutils.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [IPHLPPAPI.DLL]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [WINTRUST.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	2001.12.4414.700 [COMRes.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [OLEAUT32.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [rasman.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	6.00.2900.5512 [SHELL32.dll]	(C:\WINDOWS\SYSTEM32)
True	True	False	False	-1.0- [mores.dll]	(C:\Program Files\AU)
False	True	False	True	5.1.2600.5512 [DNSAPI.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	2001.12.4414.700 [CLBCATQ.DLL]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	6.0 [comctl32.dll]	(C:\WINDOWS\WinSxS)
False	True	False	True	5.1.2600.5512 [MSACM32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	False	1.1.0.0 [dsp_chmx.dll]	(C:\Program Files)
False	True	False	True	8.00.6001.18702 [WININET.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	6.00.2900.5512 [SHLWAPI.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [AVIFIL32.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [Msctfimeime]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [MSCTF.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	False	-1.0- [dsp_zsc.dll]	(C:\Program Files)
False	True	False	True	5.82 [COMCTL32.dll]	(C:\WINDOWS\system)
False	True	False	True	5.1.2600.5512 [USERENU.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [WINMM.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [kerne132.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [GDI32.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	False	-1.0- [mocommon.dll]	(C:\Program Files)
False	True	False	True	6.00.2900.5512 [wxtheme.dll]	(C:\WINDOWS\SYSTEM32)
True	True	False	False	-1.0- [jpeg.dll]	(C:\Program Files\AU)
False	True	False	True	5.1.2600.5512 [WLDAP32.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [msv1_0.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [VERSTION.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [ADUAPI32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [PSAPI.DLL]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [WS2_32.dll]	(C:\WINDOWS\SYSTEM32)
True	False	False	True	5.1.2600.5512 [mswsock.dll]	(C:\WINDOWS\SYSTEM32)
True	True	False	True	6.0.5441.0 [Normaliz.dll]	(C:\WINDOWS\SYSTEM32)
False	True	False	True	5.1.2600.5512 [TAPI32.dll]	(C:\WINDOWS\SYSTEM32)

Passo 1

Setup dell'exploit di scanning del telnet.

```
msf6 > search telnet_version
Matching Modules
=====
#  Name
0  auxiliary/scanner/telnet/lantronix_telnet_version
1  auxiliary/scanner/telnet_telnet_version

To boldly go where no shell has gone before

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
follow the white rabbit.
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > info

    Name: Telnet Service Banner Detection
    Module: auxiliary/scanner/telnet/telnet_version
    License: Metasploit Framework License (BSD)
    Rank: Normal

    Provided by:
        hdm <x@hdm.io>

    Check supported:
        No

    Basic options:
      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

    Description:
        Detect telnet services

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

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

Passo 2

Collegamento tramite telnet metasploitable2.

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

[+] 192.168.50.101:23      - 192.168.50.101:23 TELNET
[*] 192.168.50.101:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101. WARNING ! WARNING !
Escape character is '^]'. FILE TO WWW.NODISTRIBUTE.COM

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

PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD YOUR BACKDOOR FILE TO WWW.NODISTRIBUTE.COM

metasploitable login: [REDACTED]
```

Exploit

Un exploit informatico è un programma, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità in un software, hardware o qualsiasi dispositivo elettronico. Questo può provocare un comportamento non previsto o imprevisto.

Gli exploit sono spesso utilizzati per scopi malevoli.

Gli exploit informatici funzionano identificando una vulnerabilità o un difetto nel software o nell'hardware. Una volta identificata questa vulnerabilità, un hacker può scrivere un exploit con il preciso scopo di sfruttarla. Molti hacker utilizzano gli exploit per diffondere malware.

Protocollo TELNET

Il protocollo Telnet è un protocollo client-server che si basa sullo scambio di dati tramite connessioni TCP, permettendo la trasmissione di segnali. Consente il controllo remoto dei computer tramite input e output testuali. Viene stabilita una connessione client-server per impostazione predefinita tramite il protocollo di trasmissione TCP e la porta TCP 23.

	safeSEH	ASLR	NXCompat	OS DLL	Version	Path
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\kernel32.dll (C:\WINDOWS)
	True	False	False	False	-1.0- [ISDN.dll]	C:\WINDOWS\system32\ISDN.dll (C:\WINDOWS)
	True	False	True	True	6.00.2900.5512	C:\WINDOWS\system32\ole32.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\RPCRT4.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\RPCRT4.dll (C:\WINDOWS)
	True	False	False	True	8.00.6001.18702	C:\WINDOWS\system32\ieframe.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\msvcr70.dll (C:\WINDOWS)
	True	False	False	False	0.8.22.5506	C:\WINDOWS\system32\AudioCoder.exe (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\RPCRT4.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\RPCRT4.dll (C:\WINDOWS)
	True	False	False	False	1.0.0.402	C:\WINDOWS\system32\SysInfo.dll (C:\WINDOWS)
	True	False	True	True	7.0.2600.5512	C:\WINDOWS\system32\msvrt.dll (C:\WINDOWS)
	True	False	False	True	8.00.6001.18702	C:\WINDOWS\system32\ieframe.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\sensapi.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\RASAPI32.dll (C:\WINDOWS)
	True	False	True	True	8.00.6001.18702	C:\WINDOWS\system32\iertutil.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\IMAGEHELP.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\rasadhlp.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\Secur32.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\WSOCK32.dll (C:\WINDOWS)
	True	False	True	True	6.00.2900.5512	C:\WINDOWS\system32\shdocvw.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\WS2HELP.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\ole32.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\IMM32.DLL (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\Inetcfg.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\USER32.dll (C:\WINDOWS)
	True	False	False	False	1.13	C:\WINDOWS\system32\libiconv-2.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\CRYPTUI.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\Irtutils.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\IPHLPAPI.DLL (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\WINTRUST.dll (C:\WINDOWS)
	True	False	True	True	2001.12.4414.700	C:\WINDOWS\system32\COMRes.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\OLEAUT32.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\rasman.dll (C:\WINDOWS)
	True	False	True	True	6.00.2900.5512	C:\WINDOWS\system32\SHELL32.dll (C:\WINDOWS)
	True	False	False	False	-1.0- [mcres.dll]	C:\WINDOWS\system32\mcres.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\DNSAPI.dll (C:\WINDOWS)
	True	False	False	True	2001.12.4414.700	C:\WINDOWS\system32\CLBCATQ.dll (C:\WINDOWS)
	True	False	False	True	6.0	C:\WINDOWS\system32\comctl32.dll (C:\WINDOWS)
	True	False	True	True	5.1.2600.5512	C:\WINDOWS\system32\MSACM32.dll (C:\WINDOWS)
	True	False	False	False	1.1.0.0	C:\WINDOWS\system32\dsp_chmx.dll (C:\WINDOWS)
	True	False	False	True	8.00.6001.18702	C:\WINDOWS\system32\WININET.dll (C:\WINDOWS)
	True	False	False	True	6.00.2900.5512	C:\WINDOWS\system32\SHLWAPI.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\AVIFIL32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\msctftimeime.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\MSCTF.dll (C:\WINDOWS)
	True	False	False	False	-1.0- [dsp_zsc.dll]	C:\WINDOWS\system32\dsp_zsc.dll (C:\WINDOWS)
	True	False	False	True	5.8.2	C:\WINDOWS\system32\COMCTL32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\USERENV.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\WINMM.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\kernel32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\GDI32.dll (C:\WINDOWS)
	True	False	False	True	-1.0- [mccommon.dll]	C:\WINDOWS\system32\mccommon.dll (C:\WINDOWS)
	True	False	False	True	6.00.2900.5512	C:\WINDOWS\system32\uxtheme.dll (C:\WINDOWS)
	True	False	False	False	-1.0- [jpeg.dll]	C:\WINDOWS\system32\jpeg.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\WLDAP32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\msv1_0.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\VERSION.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\ADVAPI32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\PSAPI.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\WS2_32.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\mswsock.dll (C:\WINDOWS)
	True	False	False	True	6.0.5441.0	C:\WINDOWS\system32\Normaliz.dll (C:\WINDOWS)
	True	False	False	True	5.1.2600.5512	C:\WINDOWS\system32\TAPI32.dll (C:\WINDOWS)