Hack The Box - Legacy

OS:	Windows
Nivel:	Fácil
Release:	15/03/2017

Técnicas utilizadas

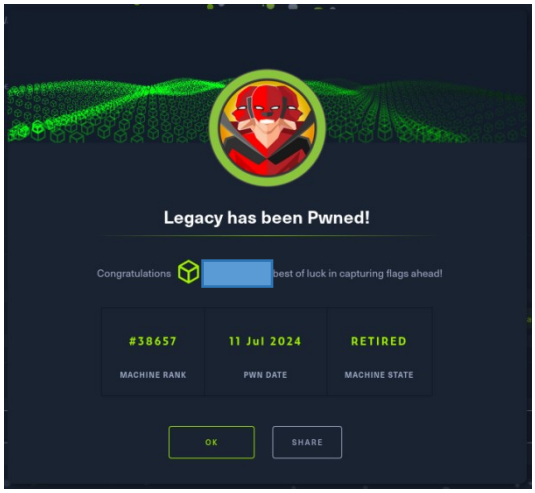
Identifying vulnerable services
Exploiting SMB (CVE-2008-4250)

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 10.129.227.181. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~]
└─$ ping -c 5 10.129.227.181 -R
PING 10.129.227.181 (10.129.227.181) 56(124) bytes of data.
64 bytes from 10.129.227.181: icmp_seq=1 ttl=127 time=54.7 ms
NOP
RR:     10.10.16.23
        10.129.0.1
        10.129.227.181
        10.10.16.1
        10.10.16.23

64 bytes from 10.129.227.181: icmp_seq=2 ttl=127 time=54.0 ms
NOP     (same route)
64 bytes from 10.129.227.181: icmp_seq=3 ttl=127 time=55.1 ms
NOP     (same route)
64 bytes from 10.129.227.181: icmp_seq=4 ttl=127 time=75.8 ms
NOP     (same route)
64 bytes from 10.129.227.181: icmp_seq=5 ttl=127 time=53.5 ms
NOP     (same route)

--- 10.129.227.181 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 53.450/58.588/75.772/8.609 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 10.129.227.181 -oN scanner_legacy** 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.

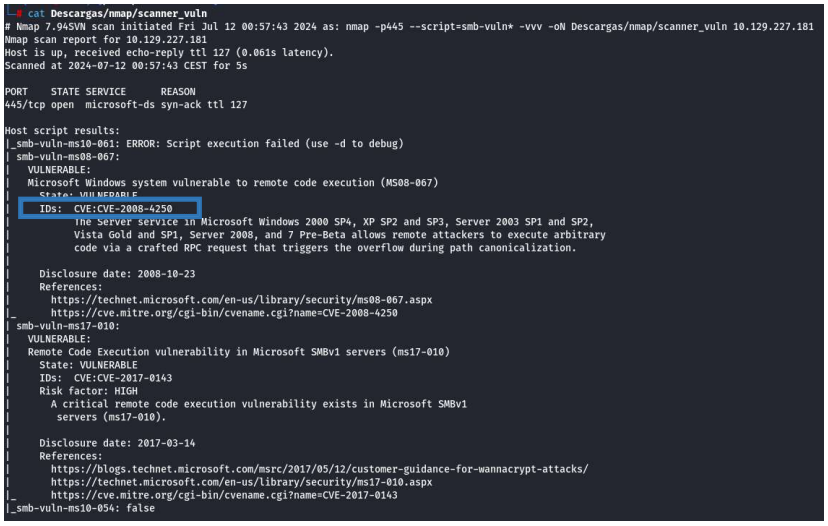
```
# Nmap 7.94SVN scan initiated Fri Jul 12 00:49:35 2024 as: nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn -oN scanner_legacy 10.129.227.181
Increasing send delay for 10.129.227.181 from 0 to 5 due to 613 out of 2041 dropped probes since last increase.
Increasing send delay for 10.129.227.181 from 5 to 10 due to 424 out of 1411 dropped probes since last increase.
Nmap scan report for 10.129.227.181
Host is up, received user-set (0.079s latency).
Scanned at 2024-07-12 00:49:35 CEST for 33s
Not shown: 65532 closed tcp ports (reset)
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 XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:94:42:f4 (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00:50:56:94:42:f4:00:00:00:00:00:00:00:00:00:00
|   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
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 16915/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 61278/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 60321/udp): CLEAN (Failed to receive data)
|   Check 4 (port 54548/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2024-07-17T03:47:37+03:00
|_clock-skew: mean: 5d00h27m39s, deviation: 2h07m16s, median: 4d22h57m39s
```

Después de realizar un escaneo de puertos abiertos con Nmap, descubrí que la máquina objetivo está ejecutando Windows XP, un sistema operativo bastante antiguo. Esto es muy importante, ya que, Windows XP es conocido por tener varias vulnerabilidades, especialmente en relación con el protocolo SMB (Server Message Block). El protocolo SMB se utiliza para compartir acceso a archivos, impresoras y otros recursos en redes. Las versiones antiguas de SMB, como las que se encuentran en Windows XP, tienen varias vulnerabilidades conocidas que pueden ser explotadas.

```
┌──(root㉿kali)-[/home/administrador]
└─# ls /usr/share/nmap/scripts/ | grep "smb-vuln"
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
```

Una vez identificado que la máquina objetivo estaba ejecutando Windows XP y que el puerto 445 estaba abierto, decidí buscar vulnerabilidades específicas relacionadas con el protocolo SMB. Para ello, utilicé el Nmap Scripting Engine (NSE), una potente herramienta que permite automatizar una amplia variedad de tareas de red y seguridad. Este comando ejecuta todos los scripts de NSE que comienzan con “smb-vuln” contra el puerto 445 de la máquina objetivo. Estos scripts están diseñados para buscar una variedad de vulnerabilidades conocidas en SMB.



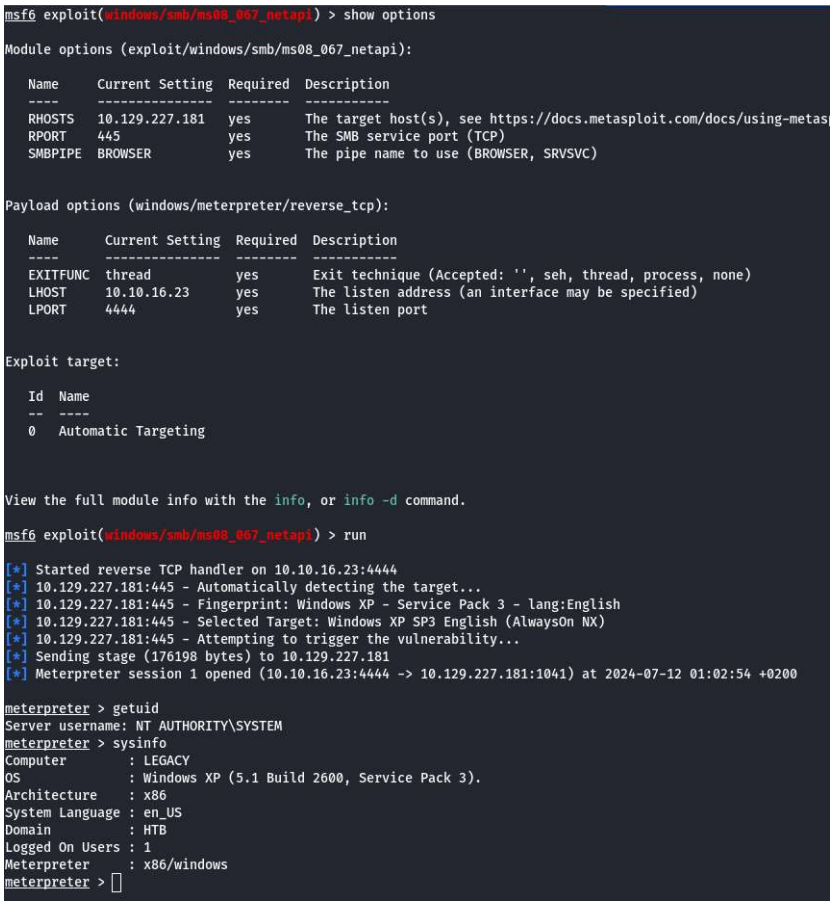
Escalada de privilegios

El escaneo con Nmap y NSE reveló que la máquina objetivo es vulnerable a MS08-067. Esta es una vulnerabilidad crítica en el servicio Server de Windows que podría permitir la ejecución remota de código si un atacante enviara una solicitud RPC especialmente diseñada a un sistema afectado.

MS08-067 es particularmente notable porque fue explotada por el gusano Conficker, que causó una cantidad significativa de daño en 2008. La existencia de esta vulnerabilidad en la máquina objetivo proporciona un vector de ataque claro que puedo explotar para ganar acceso al sistema.

Para explotar la vulnerabilidad MS08-067, utilicé la herramienta Metasploit, que es un marco de trabajo para el desarrollo y ejecución de exploits contra sistemas de destino.

Ejecuté el exploit correspondiente para MS08-067 y, como resultado, obtuve acceso a la máquina objetivo.



Bibliografía

https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067