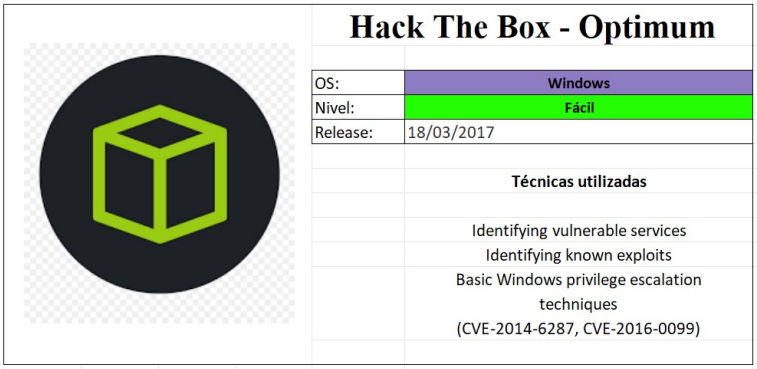
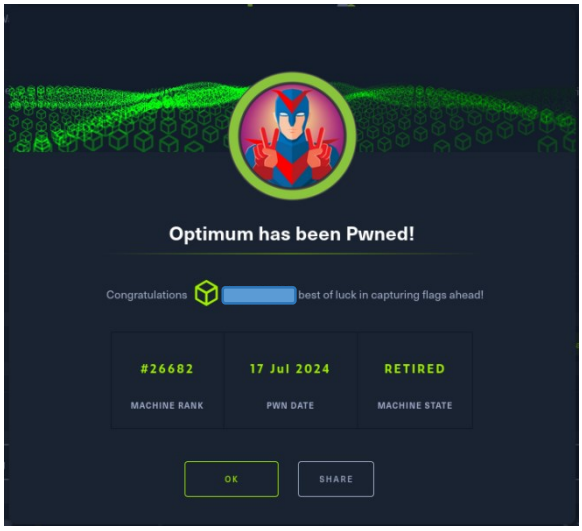


Aviso Legal

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 varios exploits 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 10.129.214.112. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
┌──(administrador㉿kali)-[~/Descargas]
└─$ ping -c 5 10.129.214.112
PING 10.129.214.112 (10.129.214.112) 56(84) bytes of data.
64 bytes from 10.129.214.112: icmp_seq=1 ttl=127 time=50.6 ms
64 bytes from 10.129.214.112: icmp_seq=2 ttl=127 time=50.4 ms
64 bytes from 10.129.214.112: icmp_seq=3 ttl=127 time=49.4 ms
64 bytes from 10.129.214.112: icmp_seq=4 ttl=127 time=50.2 ms
64 bytes from 10.129.214.112: icmp_seq=5 ttl=127 time=50.8 ms

--- 10.129.214.112 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 49.425/50.278/50.754/0.461 ms

┌──(administrador㉿kali)-[~/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 10.129.214.112 -oN scanner_optimum** para descubrir los puertos abiertos y sus versiones:

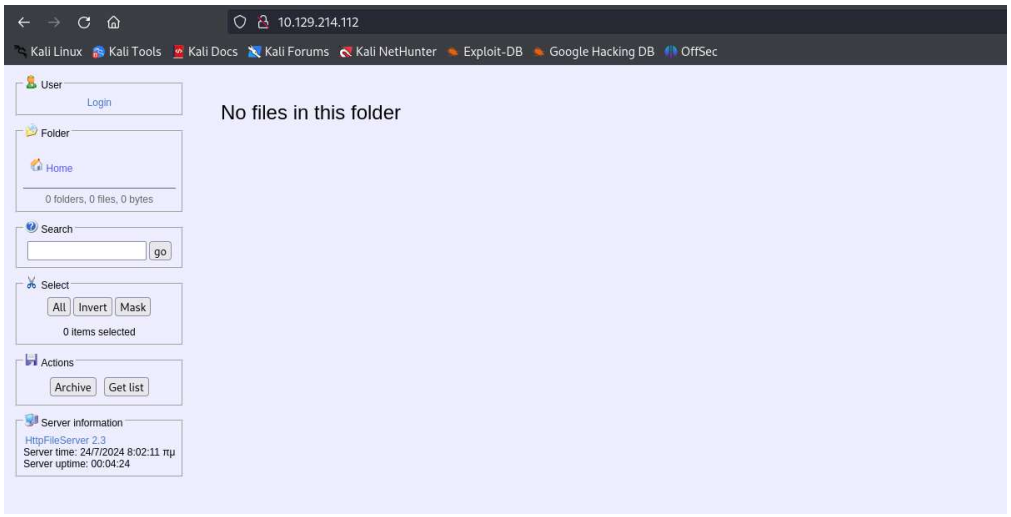
- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo 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.

```
┌──(root㉿kali)-[/home/administrador/Descargas]
└─# cat nmap/scanner_optimum
# Nmap 7.94SVN scan initiated Wed Jul 17 22:02:47 2024 as: nmap -p- -sS -sC -sV -vvv --min-rate 5000 -Pn -oN nmap/scanner_optimum 10.129.214.112
Nmap scan report for 10.129.214.112
Host is up, received user-set (0.052s latency).
Scanned at 2024-07-17 22:02:47 CEST for 38s
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-server-header: HFS 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 17 22:03:26 2024 -- 1 IP address (1 host up) scanned in 38.44 seconds
```

Análisis del puerto 80 (HTTP)

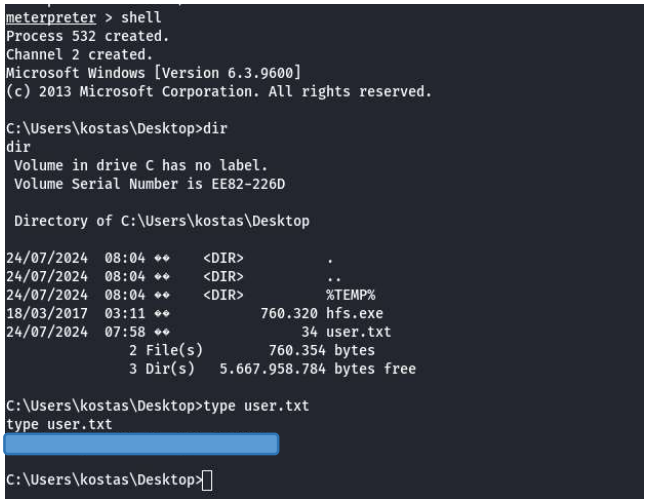
Después de realizar un escaneo de puertos abiertos con Nmap, accedí a la página web disponible en el servidor. El servidor web de la máquina víctima es HttpFileServer 2.3, que es vulnerable a CVE-2014-6287. Esta vulnerabilidad se encuentra en la función findMacroMarker en parserLib.pas en Rejetto HTTP File Server. Permite a los atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda. Esta vulnerabilidad es crítica, con una puntuación de 9.8 en CVSS v3 y 10.0 en CVSS v2.



Sabiendo esto, busqué un módulo en Metasploit que permitiera explotarla.

Encontré el módulo adecuado, lo configuré correctamente y lo utilicé para explotar la vulnerabilidad. Como resultado, obtuve acceso a la máquina objetivo a través de una consola de Meterpreter. Sin embargo, el acceso que obtuve no era de un usuario con máximos privilegios, por lo que era necesario buscar vulnerabilidades que me permitieran escalar privilegios.

En este punto, pude obtener la flag de usuario, lo que me permitió confirmar que había ganado acceso al sistema.



Para encontrar vulnerabilidades en la máquina víctima, utilicé el módulo `local_exploit_suggester` de Metasploit. Este módulo es muy útil, ya que, proporciona una lista de posibles vulnerabilidades que se pueden explotar para escalar privilegios:

```
msf6 exploit(windows/http/rejetto_hfs_exec) > search post/multi/recon/local_exploit_suggester

Matching Modules
================

   #  Name                                        Disclosure Date  Rank    Check  Description
   -  ----                                        ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester    .                normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/http/rejetto_hfs_exec) > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
```

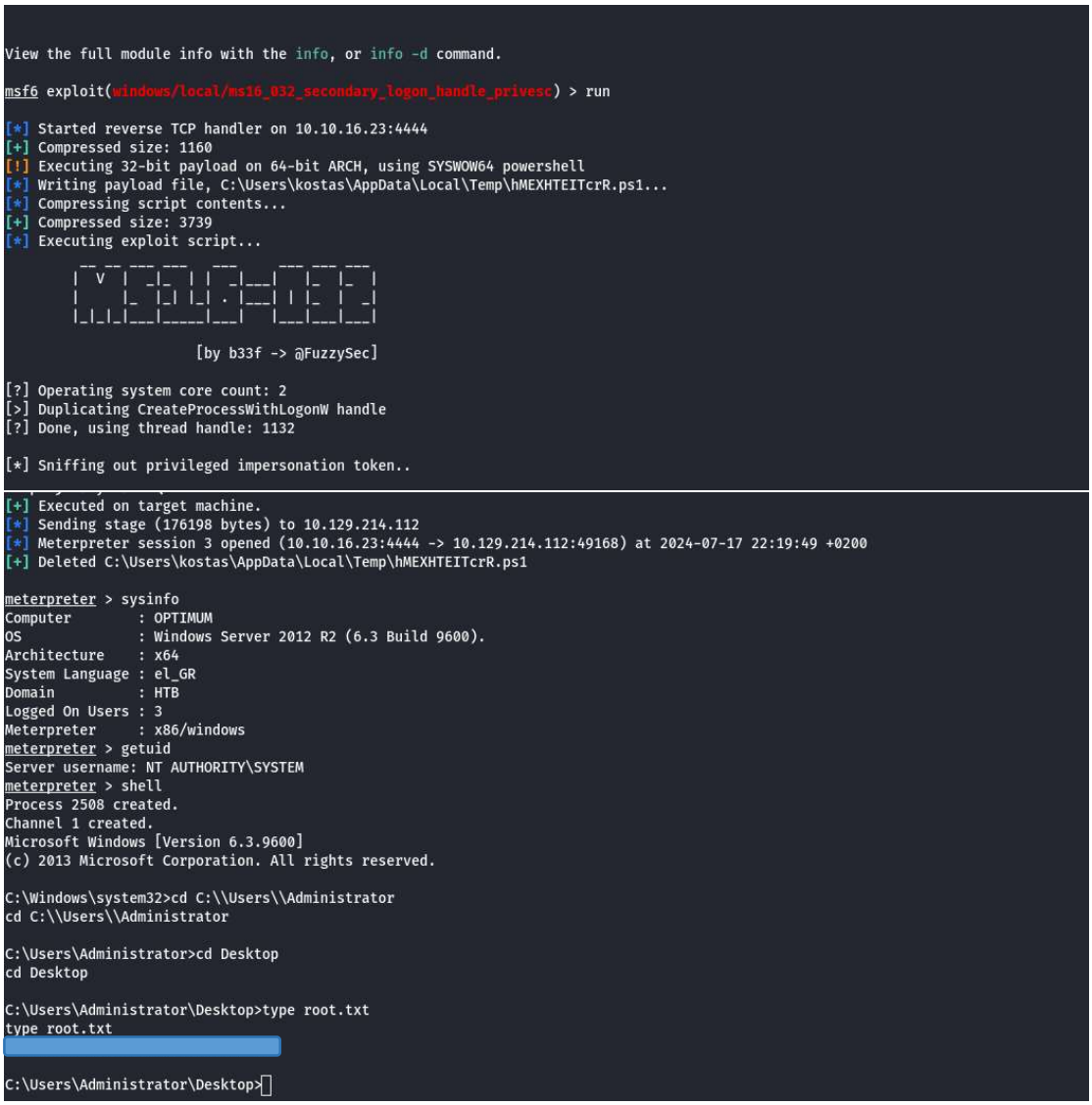
Una de las vulnerabilidades sugeridas fue MS16-032 (CVE-2016-0099), es una vulnerabilidad de escalado de privilegios que afecta al Servicio de Inicio de Sesión Secundario de Windows. Esta vulnerabilidad se debe a la falta de saneamiento de los manejadores estándar en el Servicio de Inicio de Sesión Secundario de Windows. La vulnerabilidad es conocida por afectar a las versiones de Windows 7, Windows 8, Windows 8.1, Windows 10, así como a Windows Server 2008, Windows Server 2012, tanto en sus versiones de 32 bits como de 64 bits.

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.214.112 - Collecting local exploits for x64/windows...
[*] 10.129.214.112 - 196 exploit checks are being tried...
[+] 10.129.214.112 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.129.214.112 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.129.214.112 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.129.214.112 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.129.214.112 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[+] 10.129.214.112 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
[+] 10.129.214.112 - exploit/windows/local/cve_2021_40449: The service is running, but could not be validated. Windows 8.1/Windows Server 2012 R2 build detected!
[+] 10.129.214.112 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.129.214.112 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 45 / 45
[*] 10.129.214.112 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/bypassuac_dotnet_profiler     Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr            Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/bypassuac_sdclt               Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/bypassuac_sluihijack          Yes                      The target appears to be vulnerable.
 5   exploit/windows/local/cve_2019_1458_wizardopium     Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes                      The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
 7   exploit/windows/local/cve_2021_40449                Yes                      The service is running, but could not be validated. Windows 8.1/Windows Server 2012 R2 build detected!
 8   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could not be validated.
 9   exploit/windows/local/tokenmagic                    Yes                      The target appears to be vulnerable.
```

Después de configurar y ejecutar con éxito el exploit, accedí como usuario NT Authority/system, el usuario más privilegiado del sistema, además de obtener la flag de root:



Bibliografía

https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287