



Blaster - THM (Done)

Try Hack Me Balster - <https://tryhackme.com/r/room/blaster>

Resources for this video:

Zero Day Initiative CVE-2019-1388 - <https://www.youtube.com/watch?v=3BQKpPNITSo>

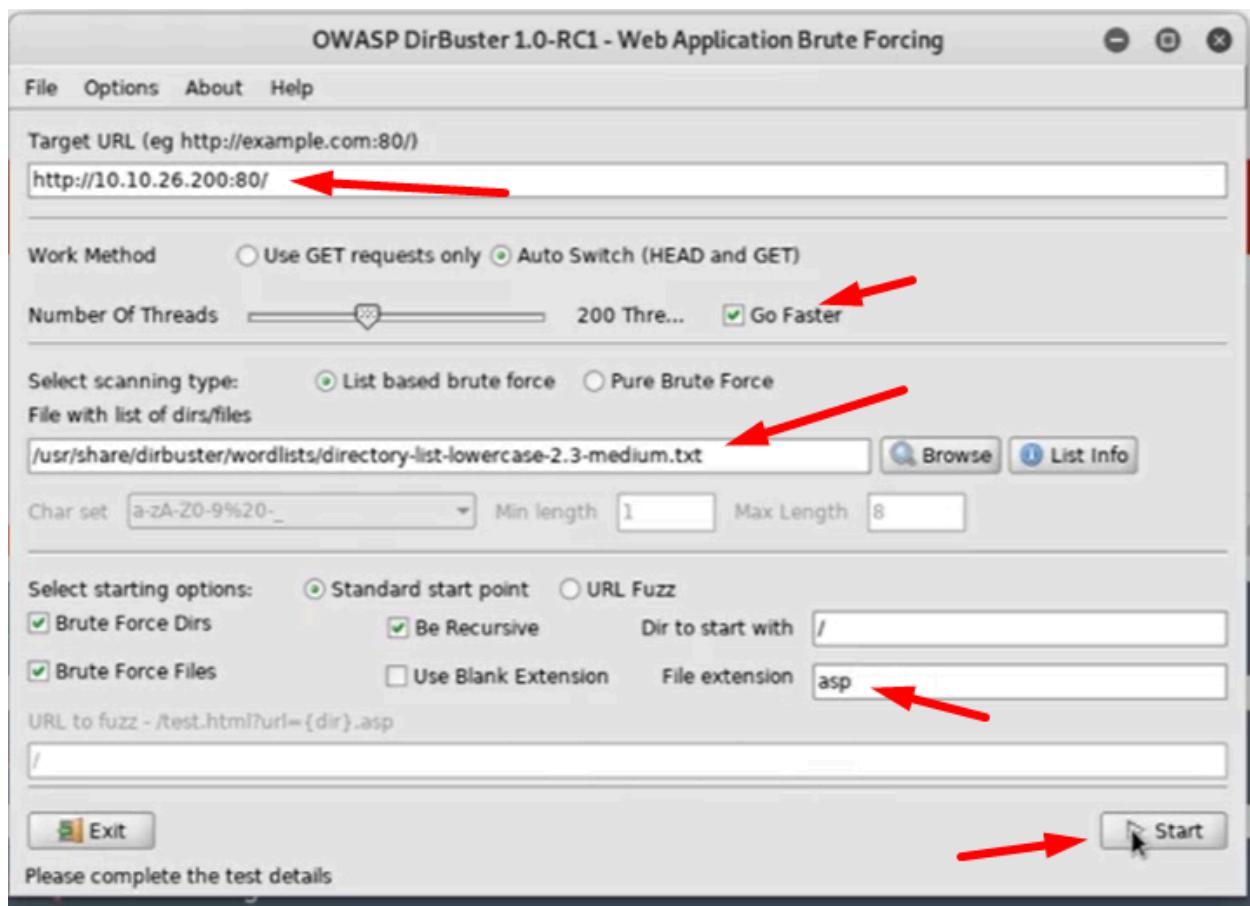
Rapid7 CVE-2019-1388 - <https://www.rapid7.com/db/vulnerabilities/msft-cve-2019-1388>

```
root@kali:~# nmap -A -T4 -p- -Pn 10.10.26.200 ←
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 02:23 EDT
Nmap scan report for 10.10.26.200
Host is up (0.12s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|_ 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: 2020-04-28T06:25:32+00:00
|   ssl-cert: Subject: commonName=RetroWeb
|     Not valid before: 2019-12-07T23:49:24
|_ Not valid after: 2020-06-07T23:49:24
|_ ssl-date: 2020-04-28T06:25:34+00:00; +2s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least
Device type: general purpose
Running (JUST GUESSTING): Microsoft Windows 2016 (80%) FreeBSD 6.2 (85%)
```

80= try dirbuster

3389 = blue keep vuln but Heath has never success this attack.

Try to get credentials using port 80 and login using 3389.



We could add asp and aspx in file extension but we will go with only asp this time.

Right click > Open in browser

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.10.26.200:80/

Scan Information | Results - List View: Dirs: 13 Files: 0 | Results - Tree View | Errors: 0 |

Type	Found	Response	Size
Dir	/	200	928
Dir	/retro/	200	31181
Dir	/retro/	200	169
Dir	/retro/	403	1371
Dir	/retro/	403	1371
Dir	/retro/	301	248
Dir	/retro/	200	169
Dir	/retro/	403	1371
Dir	/retro/	200	15477
Dir	/retro/	200	169
Dir	/retro/	200	15486
Dir	/retro/index.php/2019/12/09/	200	15489
Dir	/retro/index.php/rss/	301	361

Current speed: 6 requests/sec (Select and right click for more options)

Average speed: (T) 368, (C) 23 requests/sec

Parse Queue Size: 0 Current number of running threads: 200

Total Requests: 35702/5813669 Change

Time To Finish: 2 Days Report

Back Pause Stop Starting dir/file list based brute forcing /retro/wp-includes/source.asp

We found username 'Wade' as blog page author.

TryHackMe | HackInn | TryHackMe | blaster | cve 2019-1388 - Goo... | GitHub - jas502n/CVE... | Microsoft CVE-2019... | IIS Windows Server | Retro Fanatics – Retro Go... | Tro...

10.10.26.200/retro/index.php/2019/12/09/ready-player-one/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Hello world! 30th Anniversary of PAC-MAN → Wade on Ready Player One

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

Your email address will not be published.

ARCHIVES December 2019

CATEGORIES Uncategorized

META Log in Entries RSS Comments RSS WordPress.org

```
root@kali:~# rdesktop 10.10.26.200 ←
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerbe
?
Failed to connect, CredSSP required by server.
root@kali:~# xfreerdp --help ←
```

rdesktop does not work. CredSSP error.

```
Examples:
xfreerdp connection.rdp /p:Pwd123! /f
xfreerdp /u:CONTOSO\JohnDoe /p:Pwd123! /v:rdp.contoso.com
xfreerdp /u:JohnDoe /p:Pwd123! /w:1366 /h:768 /v:192.168.1.100:4489 ↴
xfreerdp /u:JohnDoe /p:Pwd123! /vmconnect:C824F53E-95D2-46C6-9A18-23A5BB4035
32 /v:192.168.1.100
```

```
root@kali:~# xfreerdp /u:Wade /v:10.10.26.200:3389 ←
```

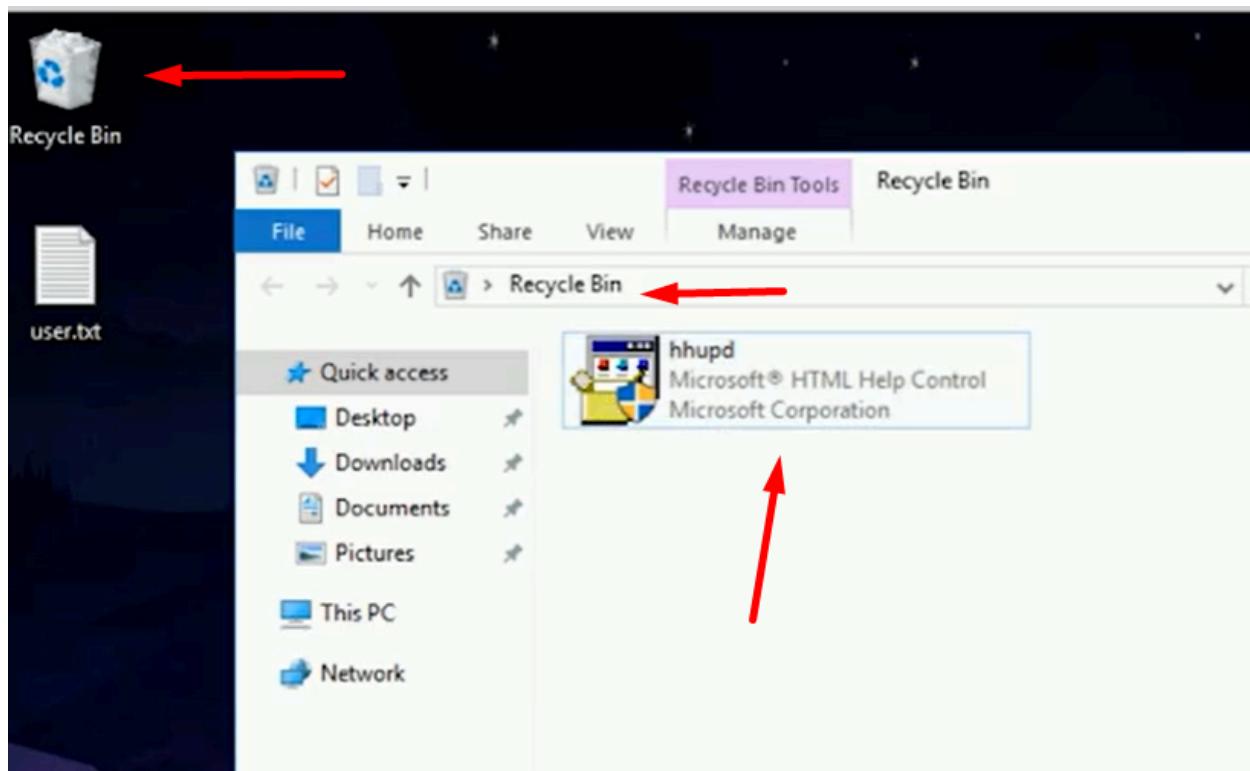
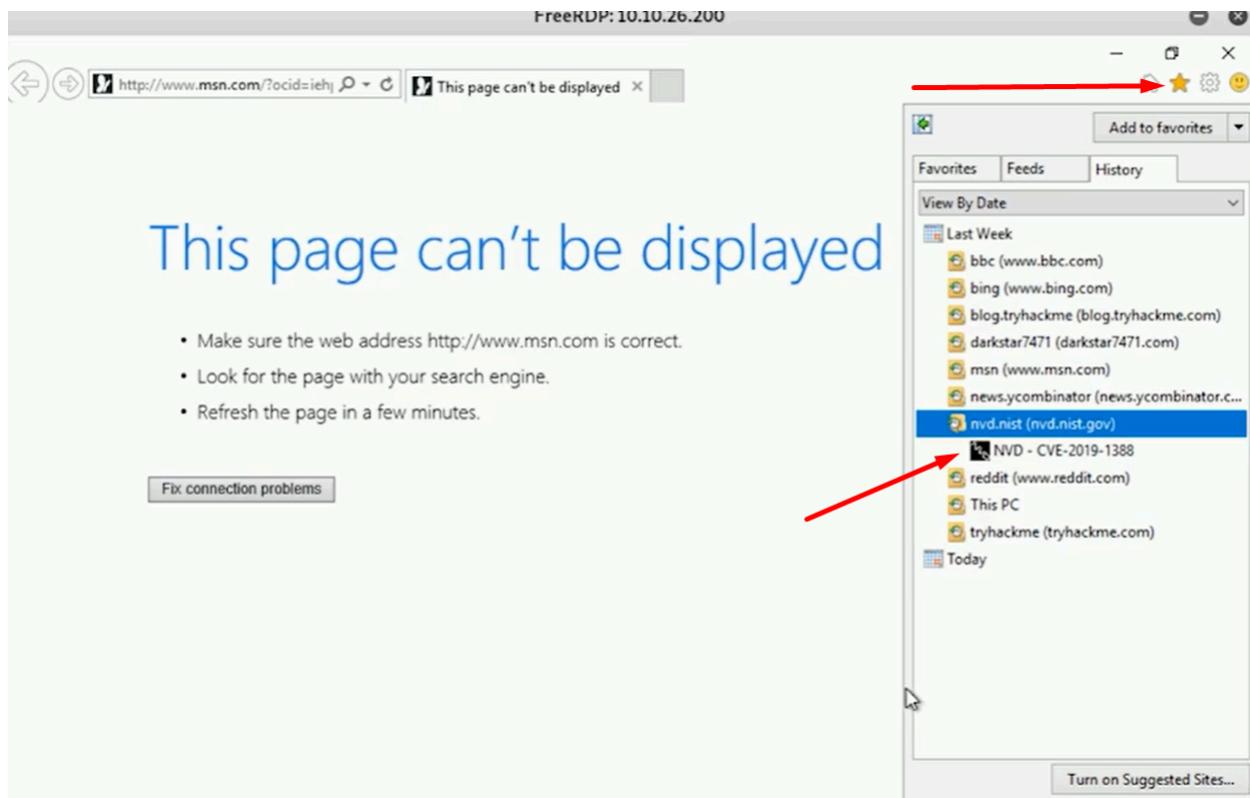
```
xfreerdp /u:JohnDoe /p:Password /w:1366 /h:768 /v:ip
#/w=width, /h=hight
```

Type password:parzival >Do you trust above certificate? Yes

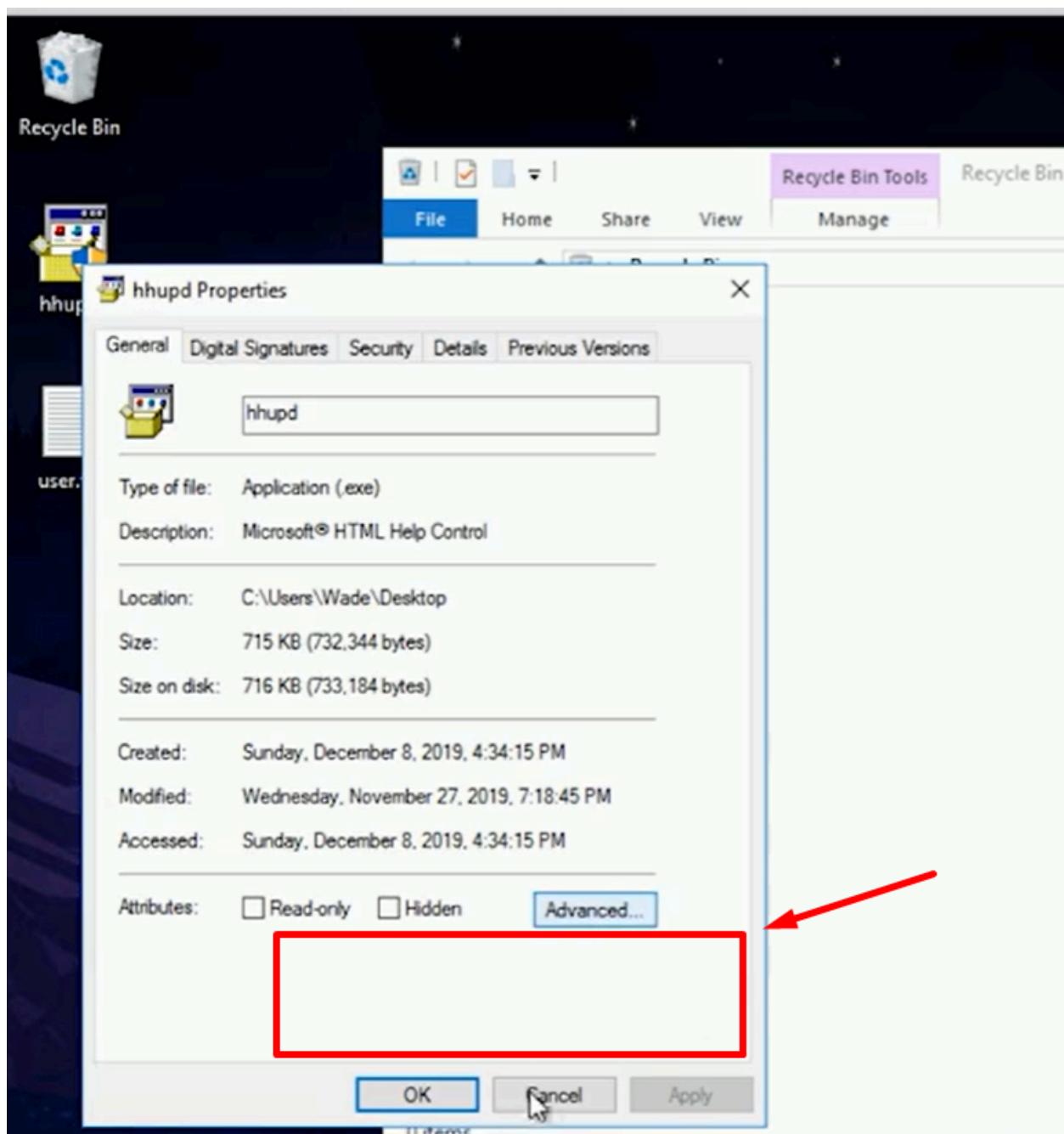
You will login rdp to the machine!

Escalation via CVE-2019-1388

Looks like the user has browsed about vuln CVE-2019-1388. And he tried this vuln using hhupd exe and he deleted it but he did not delete it completely. Thats why we are seeing that exe in recycle bin.

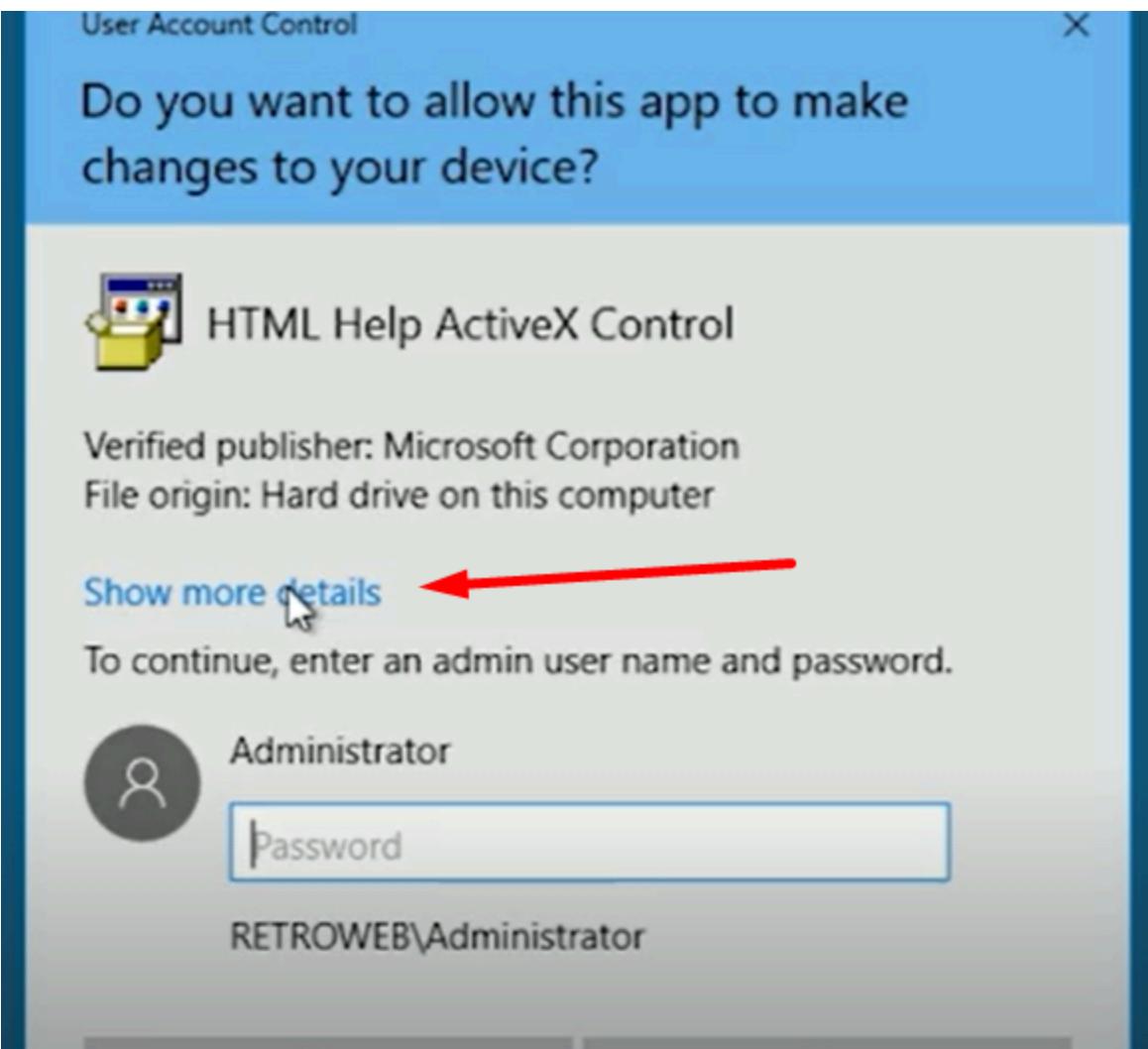


drag the exe file to desktop



If it say any security feature here. Go ahead and unblock.

And run it as administrator.



User Account Control

X

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



HTML Help ActiveX Control

Verified publisher: Microsoft Corporation

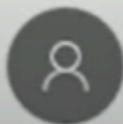
File origin: Hard drive on this computer

Program location: "C:\Users\Wade\Desktop\hhupd.exe"

Show information about the publisher's certificate 

[Hide details](#)

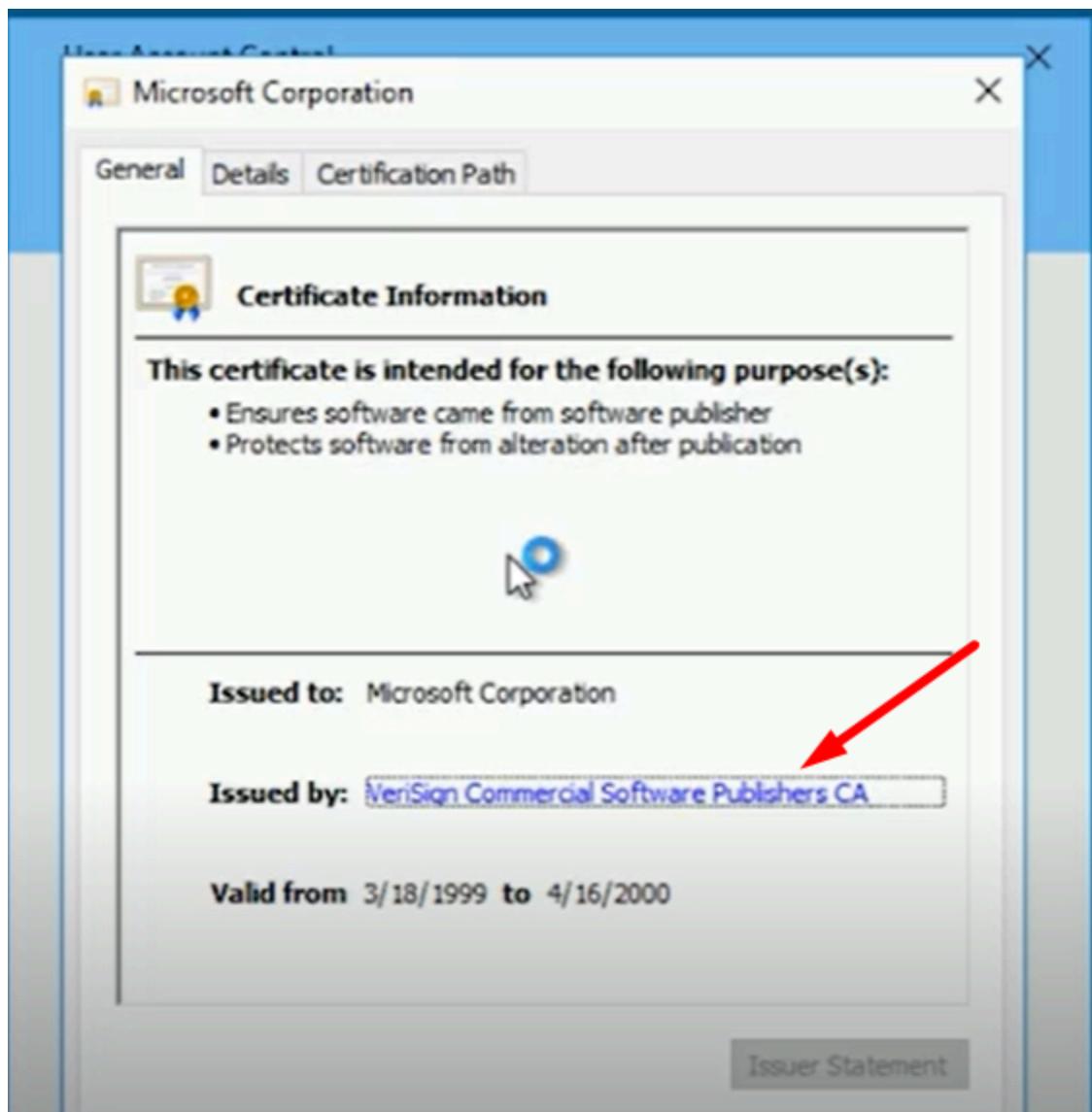
To continue, enter an admin user name and password.



Administrator

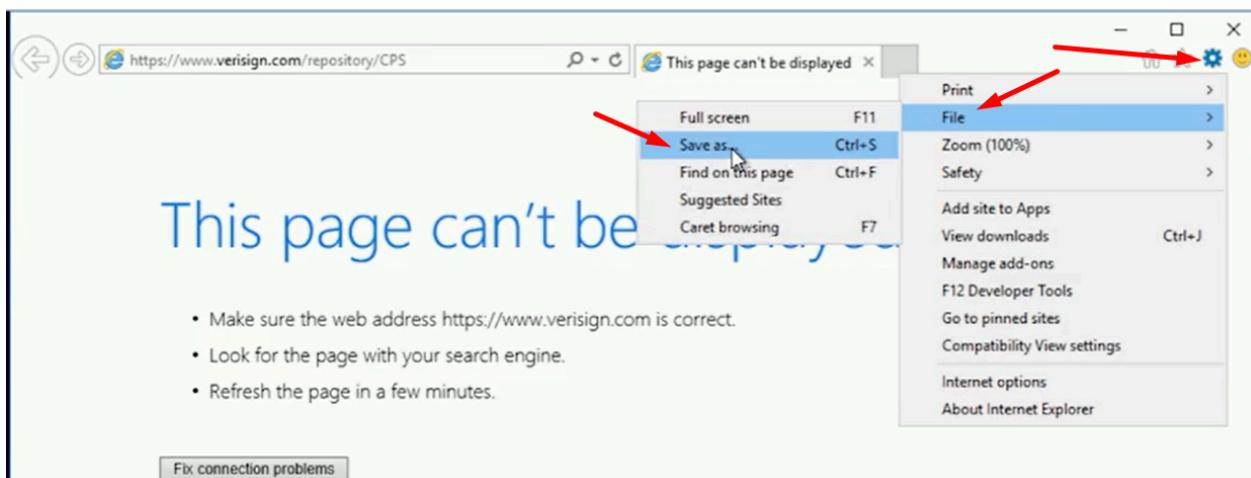
Password

RETRONWEB\Administrator

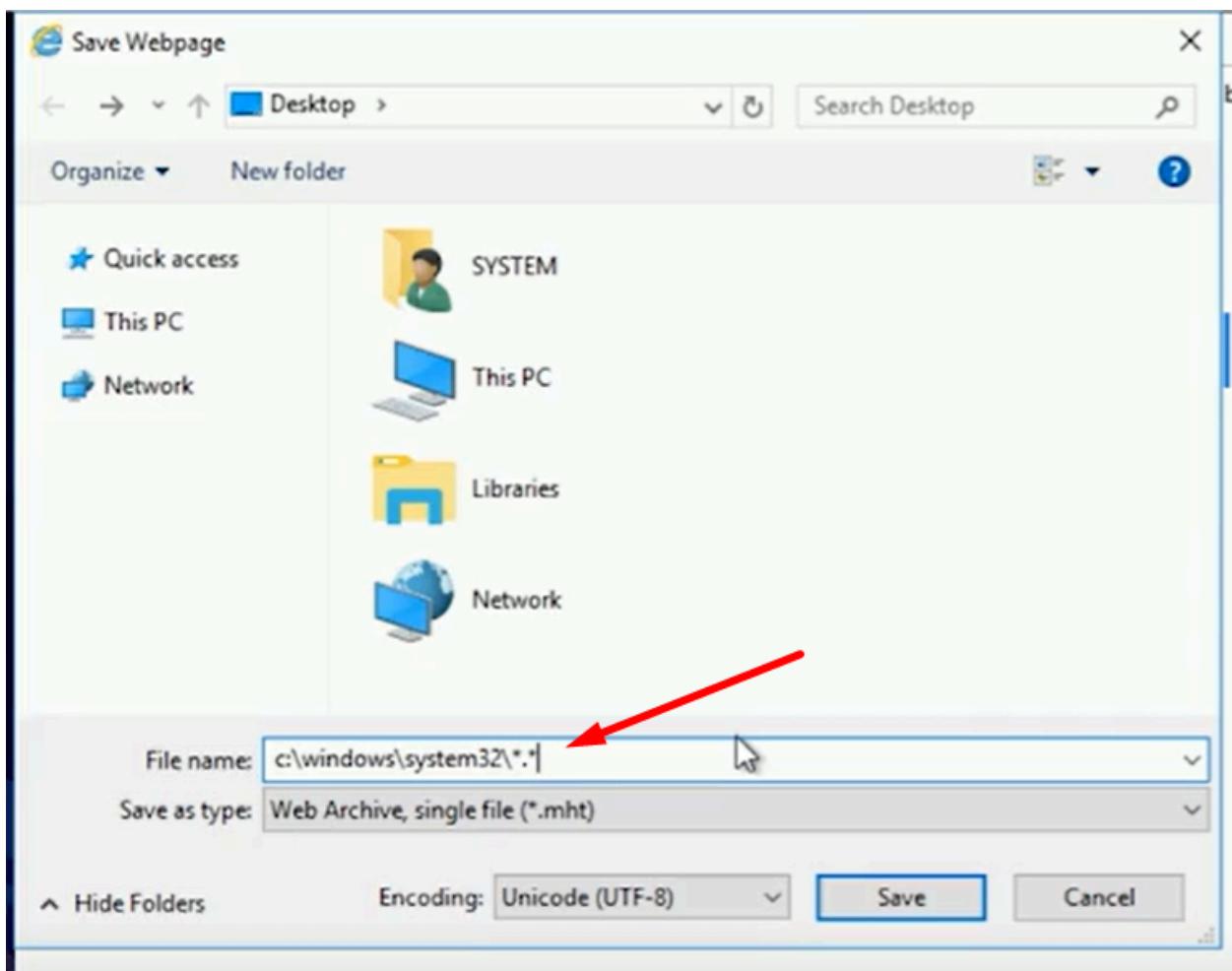


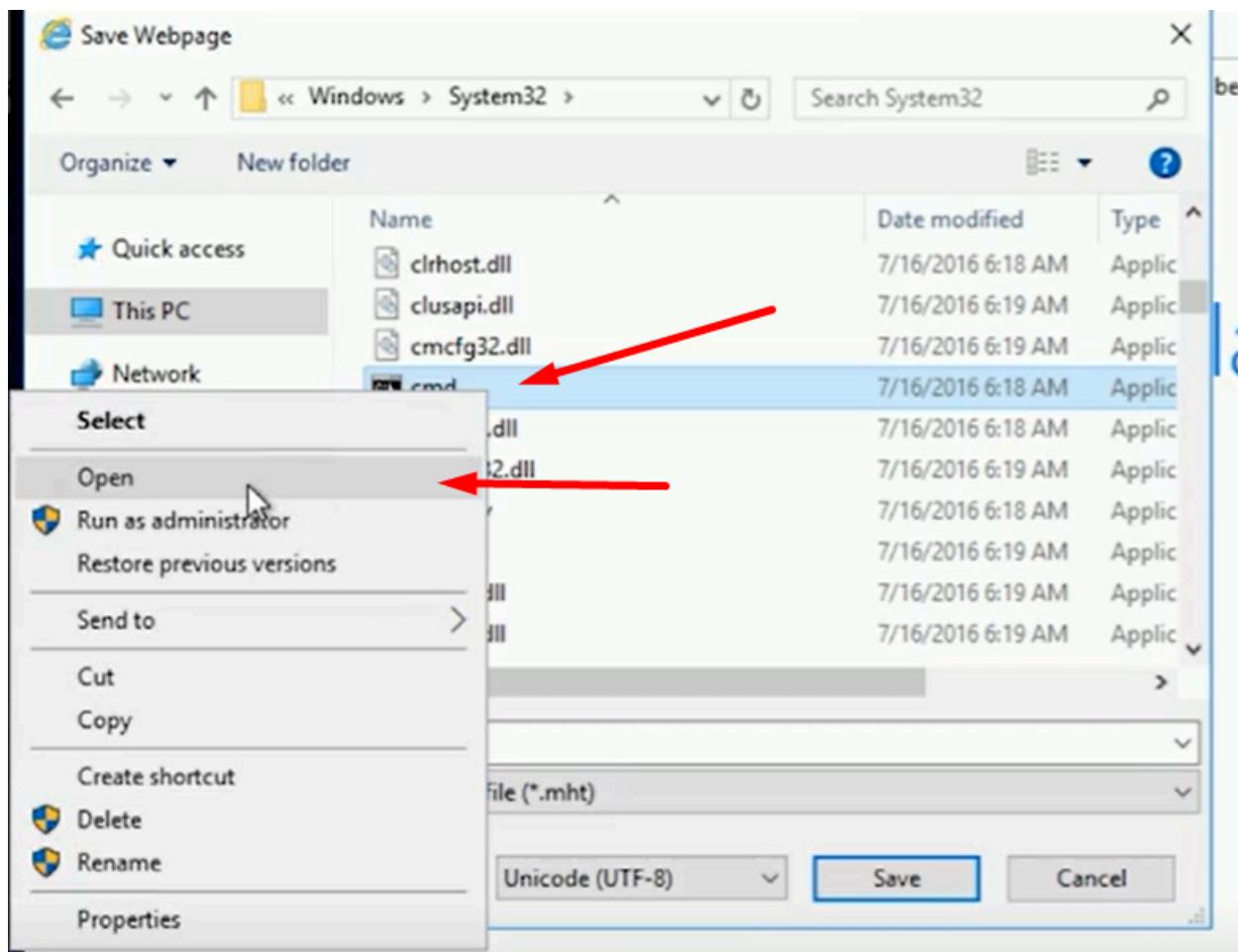
Click on this. This will open Internet explorer as system. Exit out of that exe by clicking OK or cancel or whatever.

Now Internet explorer is running as system. Go ahead and open Internet explorer.



if error pop up, just click ok and ignore.





Find cmd.exe and open.

A screenshot of a Windows Command Prompt window titled 'Administrator: C:\Windows\System32\cmd.exe'. The window shows the command 'whoami' being run, which outputs 'nt authority\system'. A red arrow points from the text 'Find cmd.exe and open.' to the 'nt authority\system' line in the command output.

```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

star C:\Windows\System32>whoami
nt authority\system
```

We are authority/system.

This is 2019 late exploit. This is relatively new. We might still see it especially in CTF.