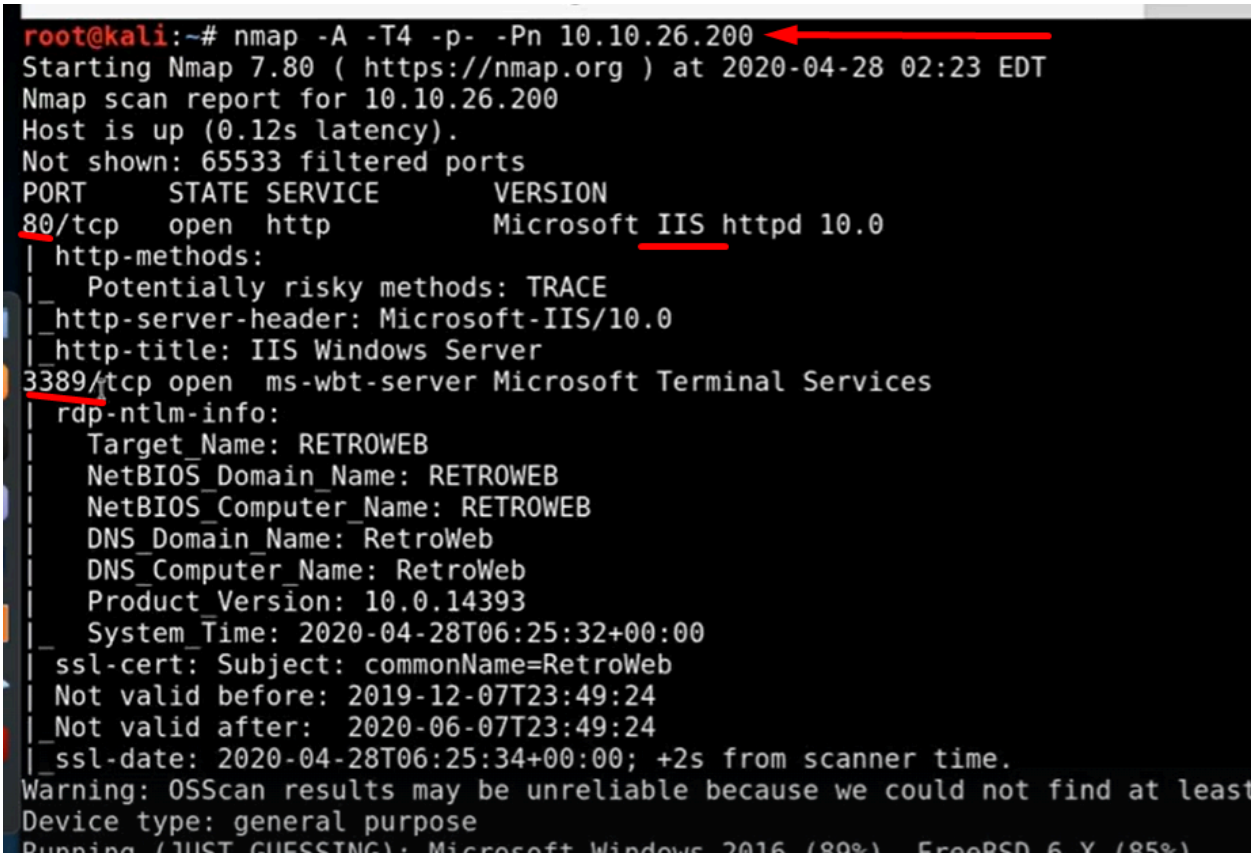
Blaster - THM (Done)

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=3BQKpPNlTSo

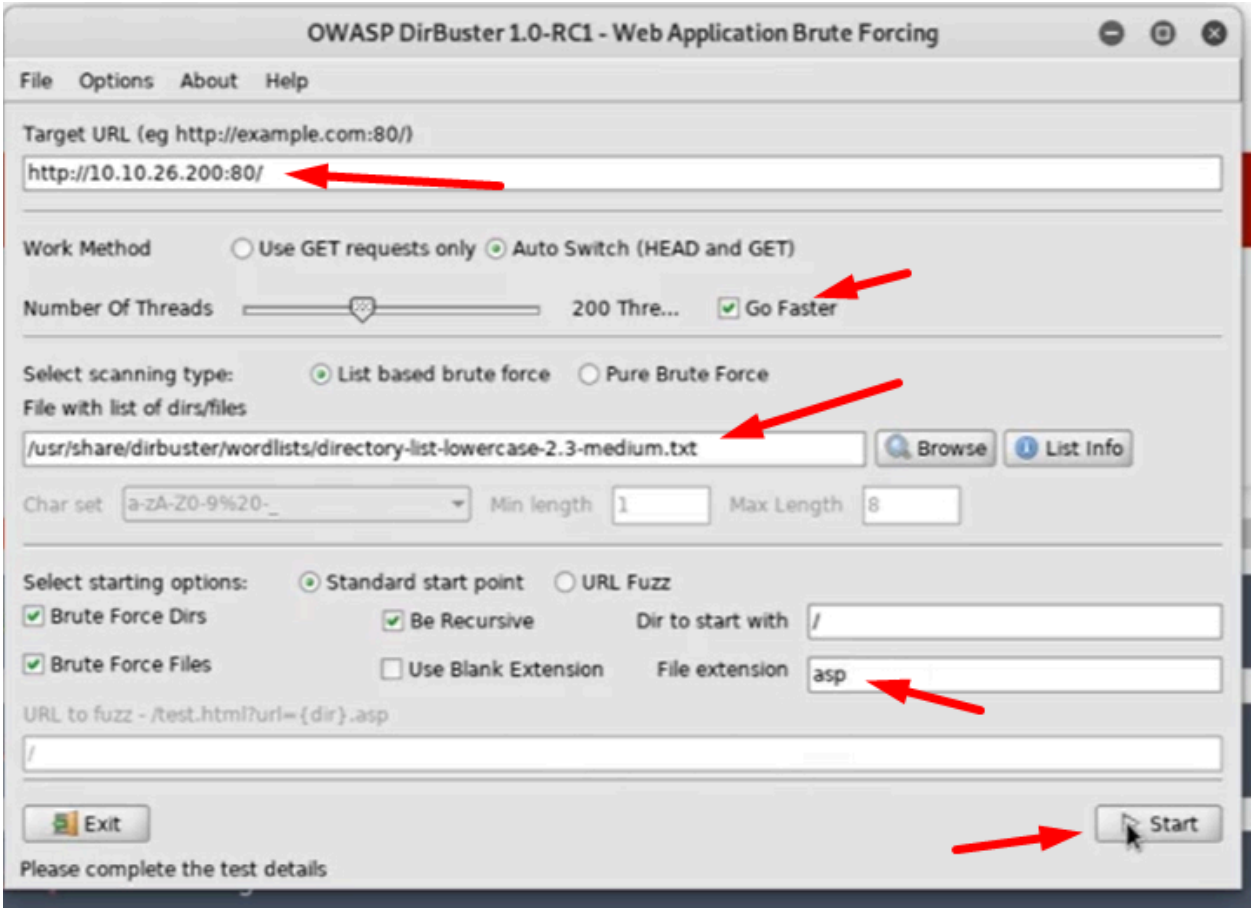
Rapid7 CVE-2019-1388 - https://www.rapid7.com/db/vulnerabilities/msft-cve-2019-1388



80= try dirbuster

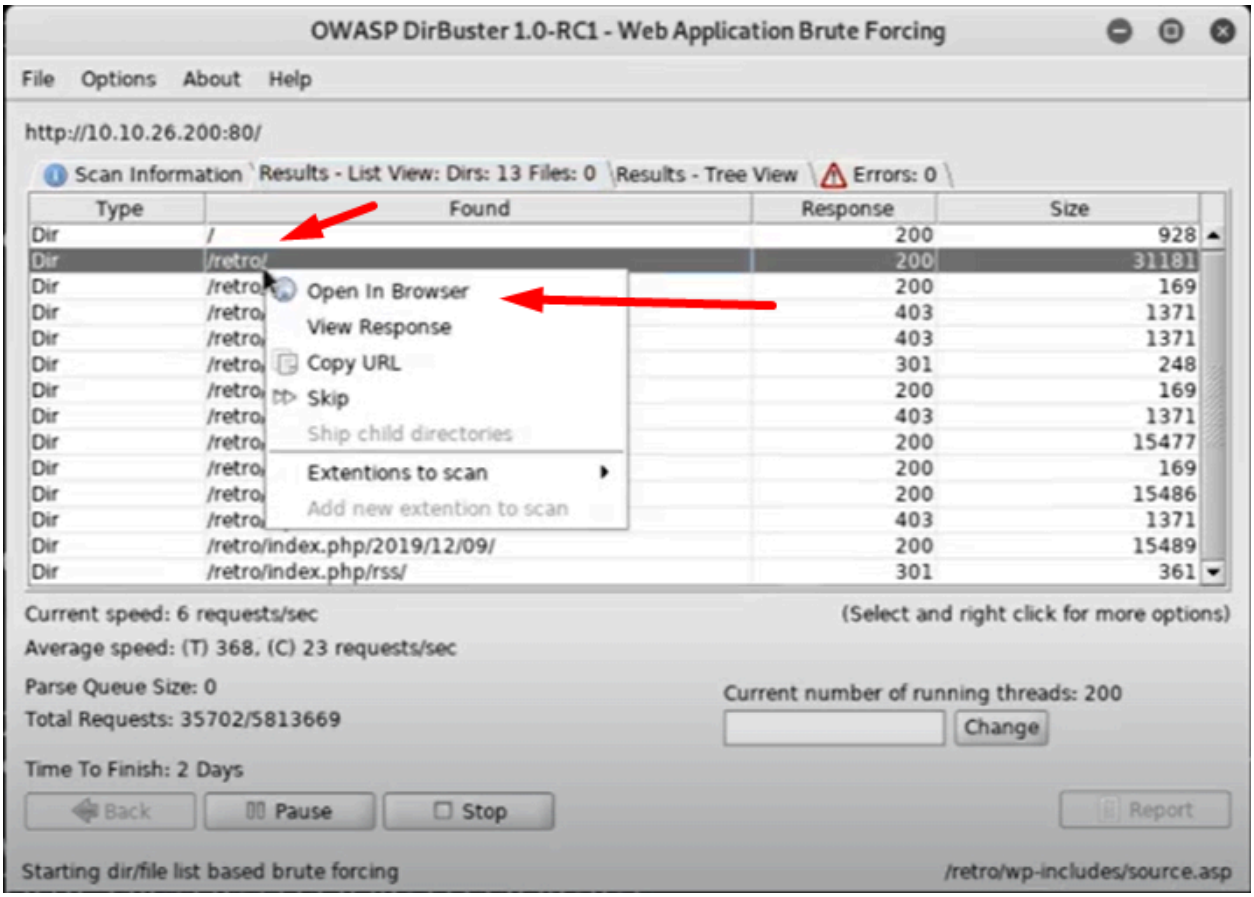
3389 = blue keep vlun but Heath has never success this attack.

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

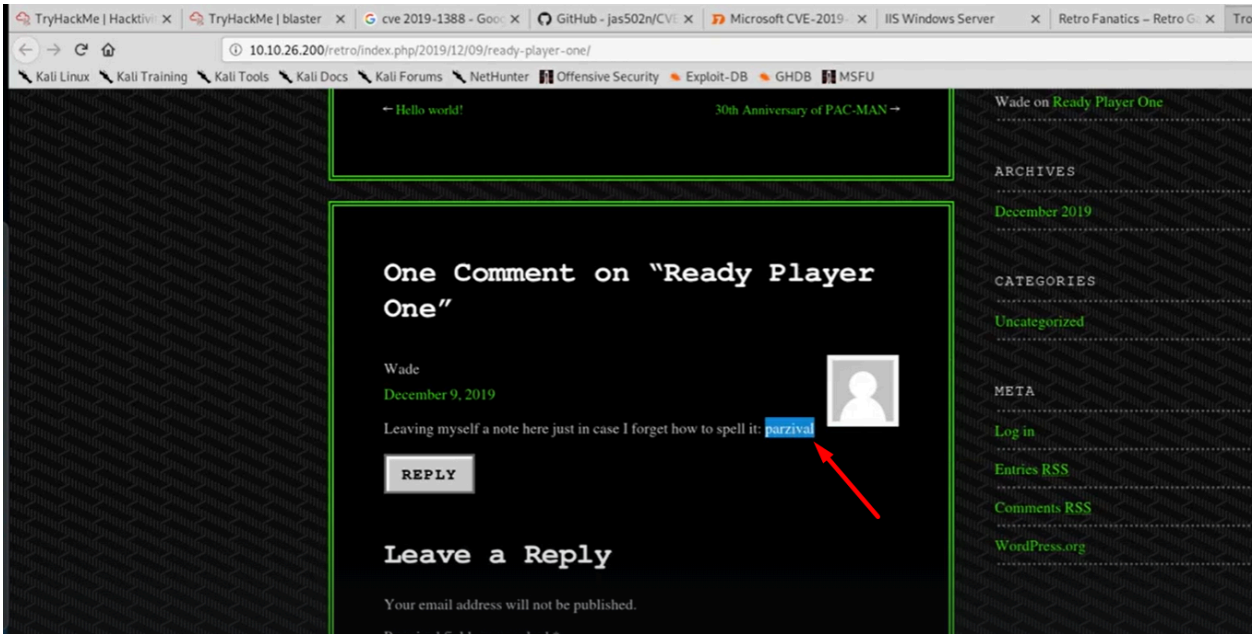


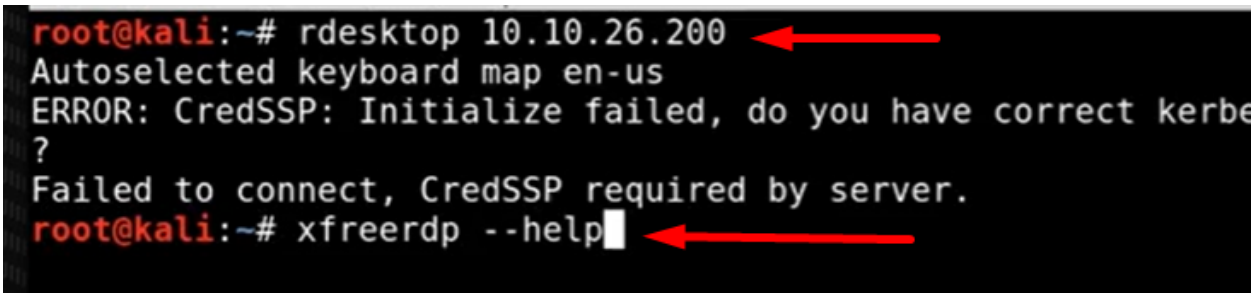
We could add asp and aspx in fille extension but we will go with only asp this time.

Right click > Open in browser

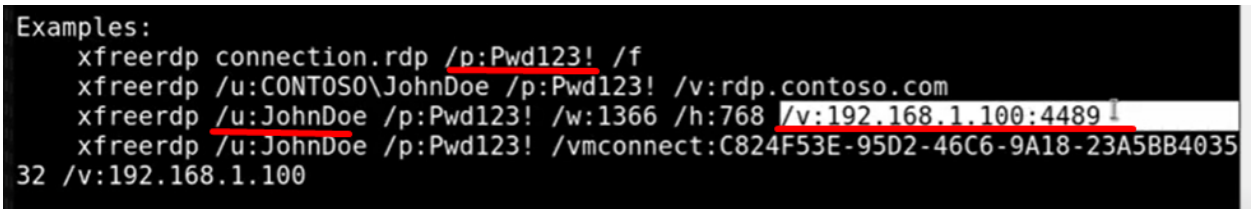


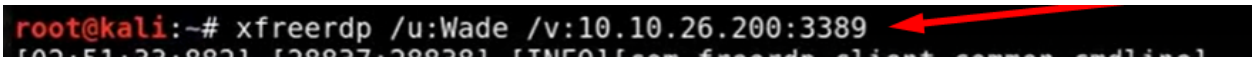
We found username ‘Wade’ as blog page author.





rdesktop does not work. CredSSP error.





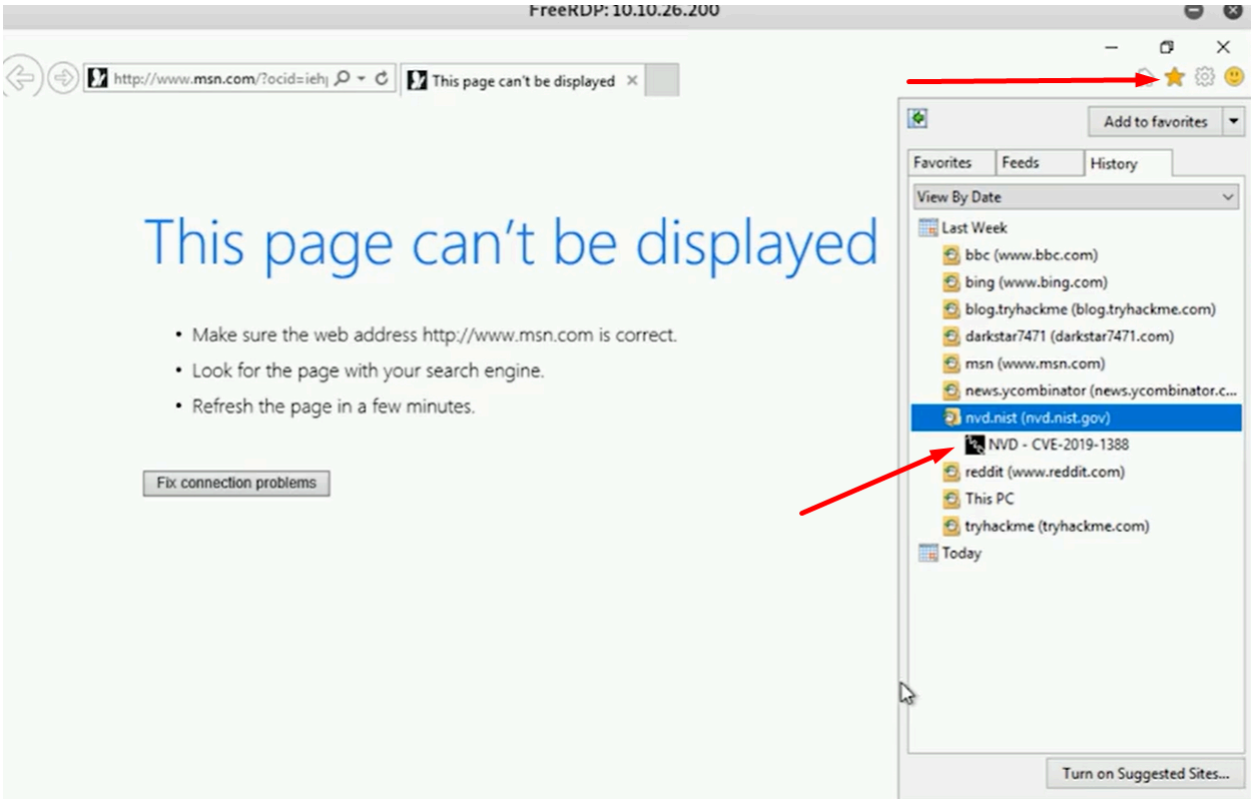

```
xfreerdp /u:JohnDoe /p:Password /w:1366 /h:768 /v:ip
#/w=width, /h=hight
```

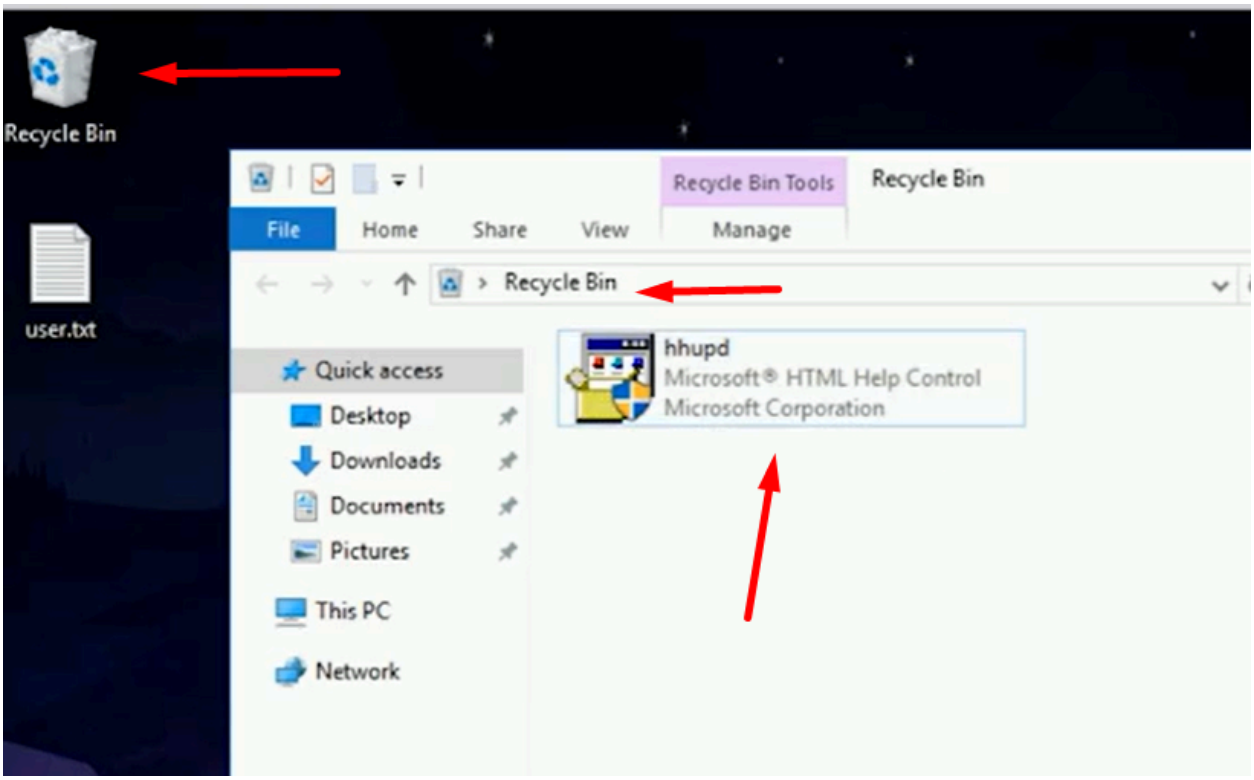
Type password:parzival >Do you trust above certificate? Yes

You will login rdp to the machine!

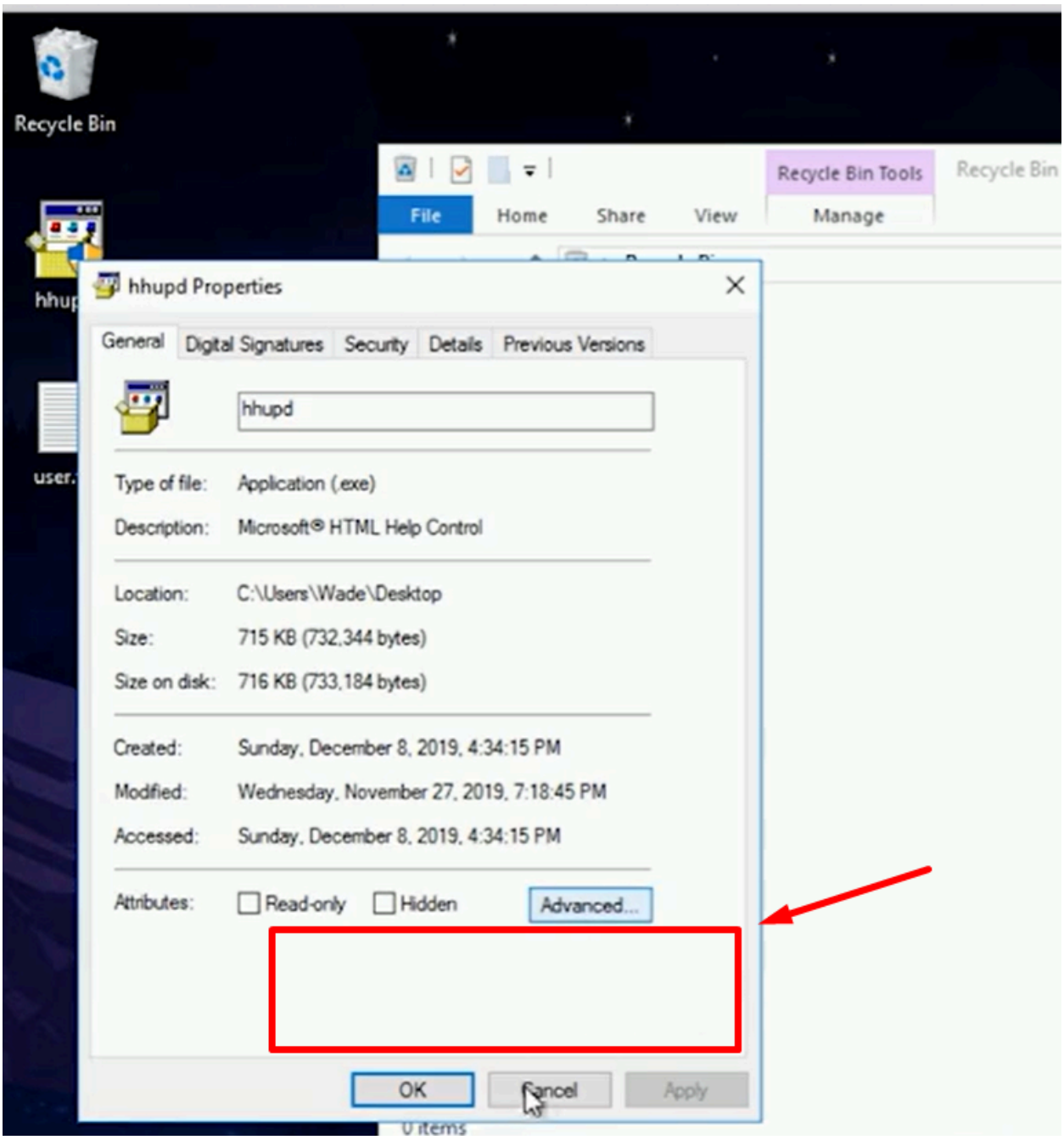
Escalation via CVE-2019-1388

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.



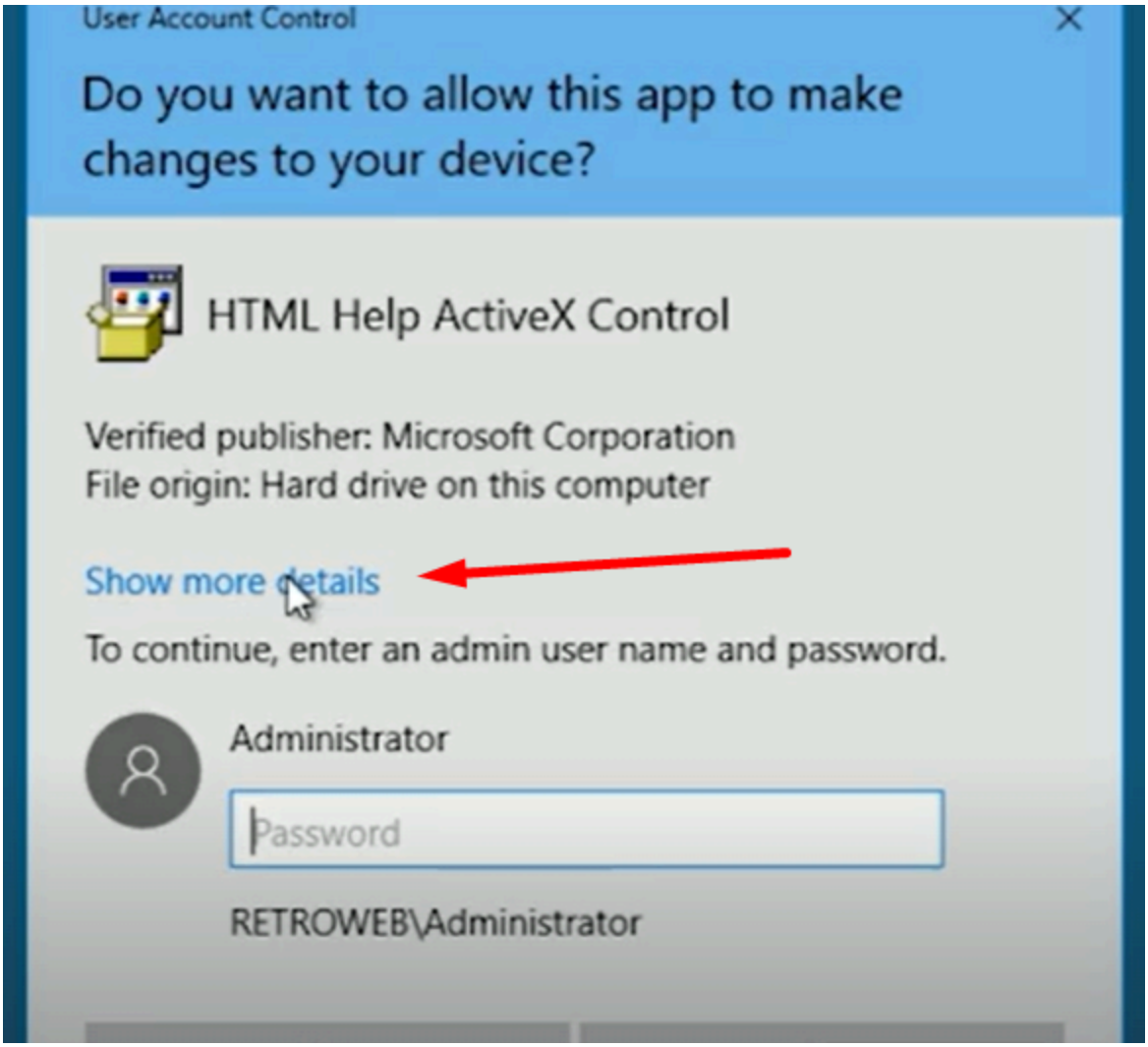


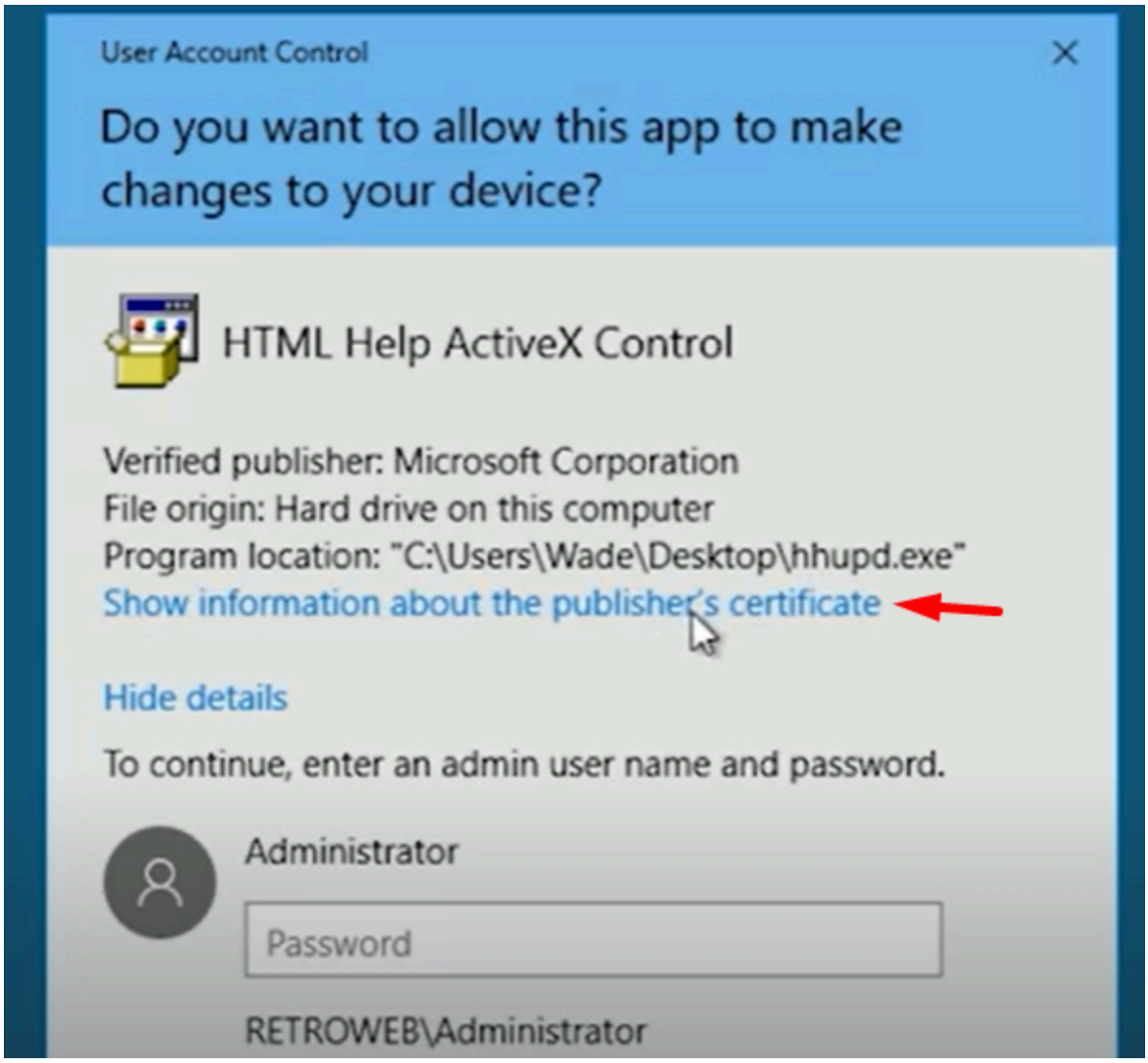
drag the exe file to desktop

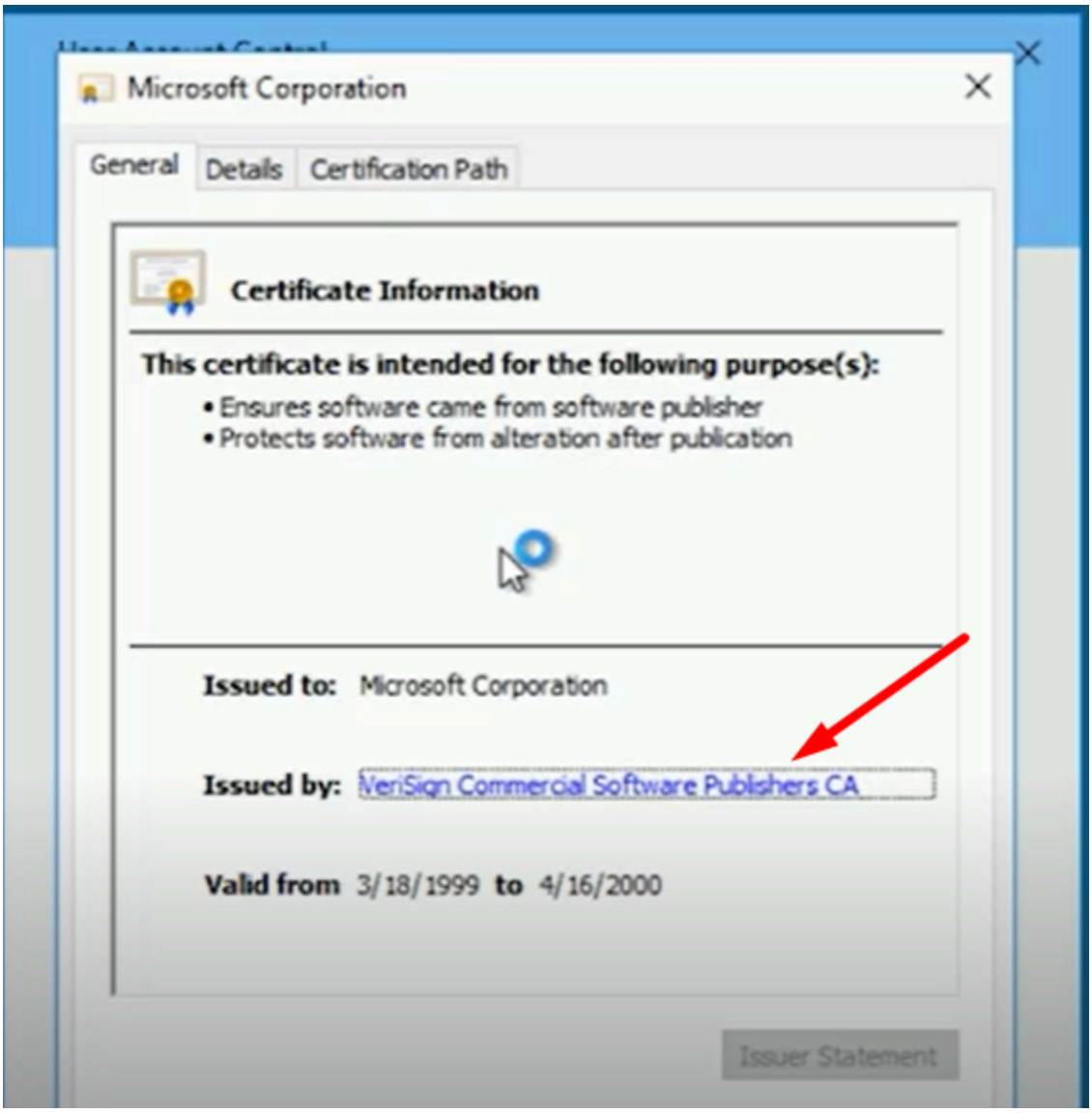


If it say any security feature here. Go ahead and unblock.

And run it as administrator.

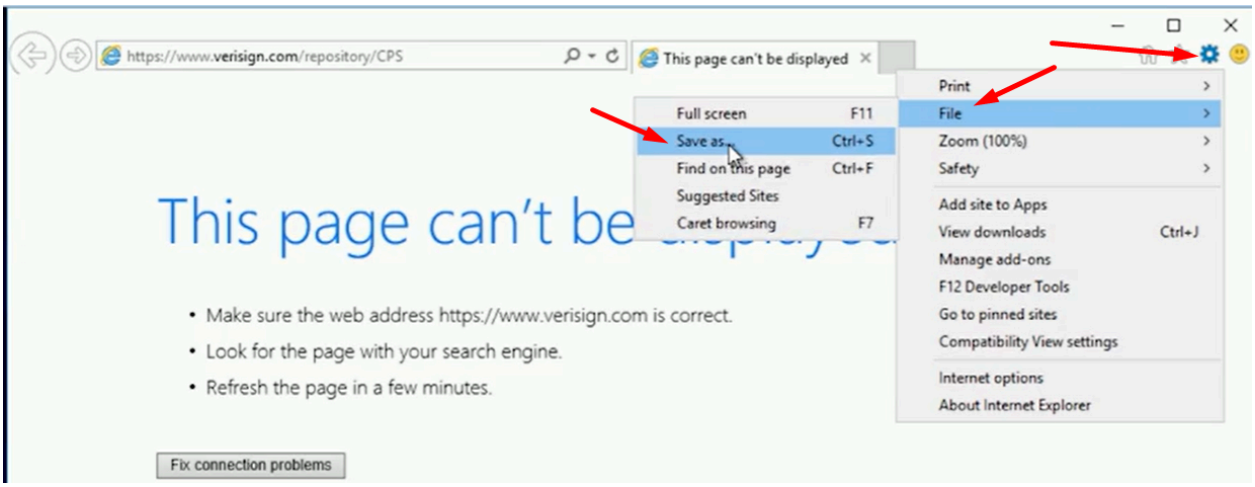

User Account Control
Do you want to allow this app to make changes to your device?
HTML Help ActiveX Control
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer
Show more details
To continue, enter an admin user name and password.
Administrator
Password
RETROWEB\Administrator


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"
Show information about the publisher's certificate
Hide details
To continue, enter an admin user name and password.
Administrator
Password
RETROWEB\Administrator

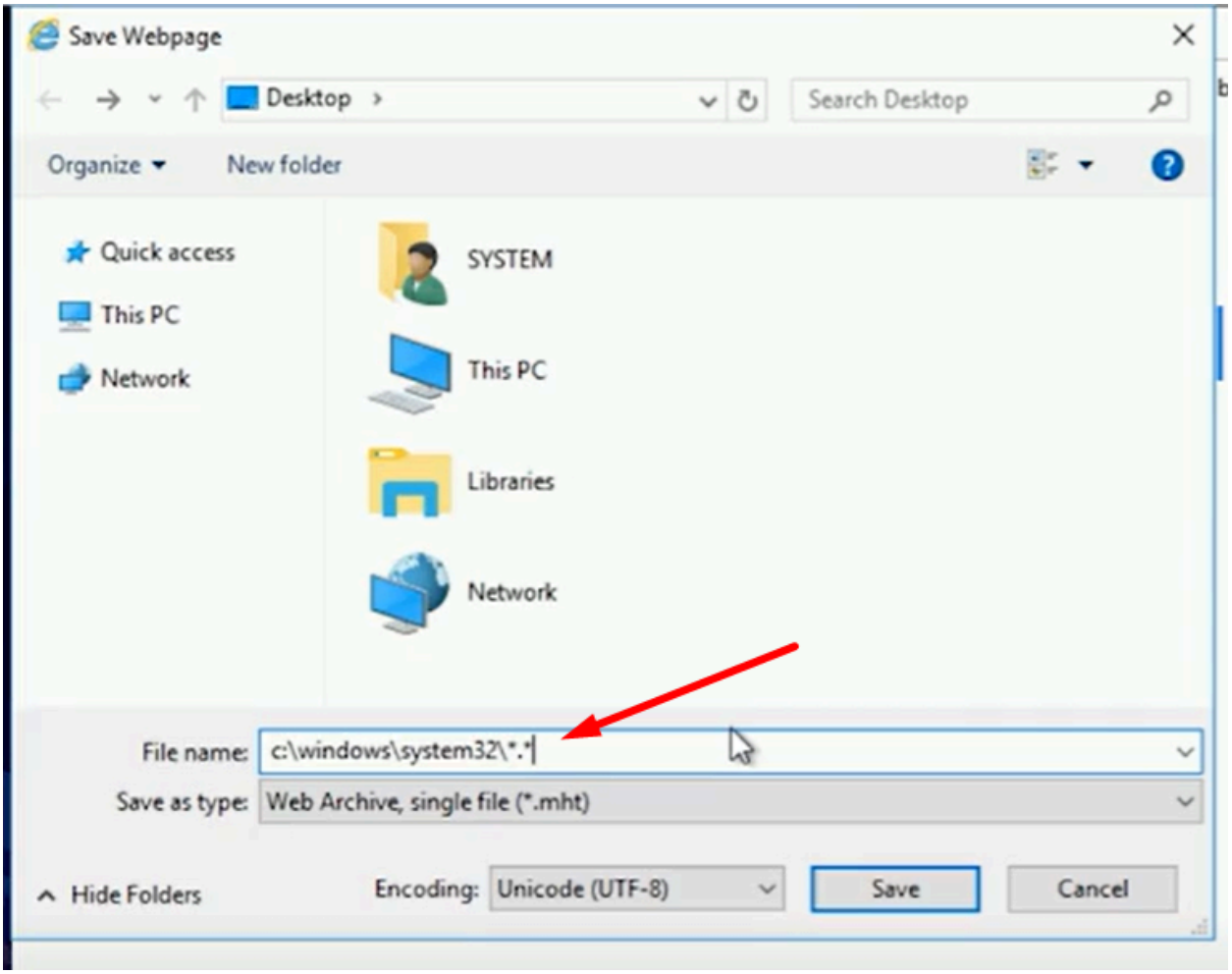


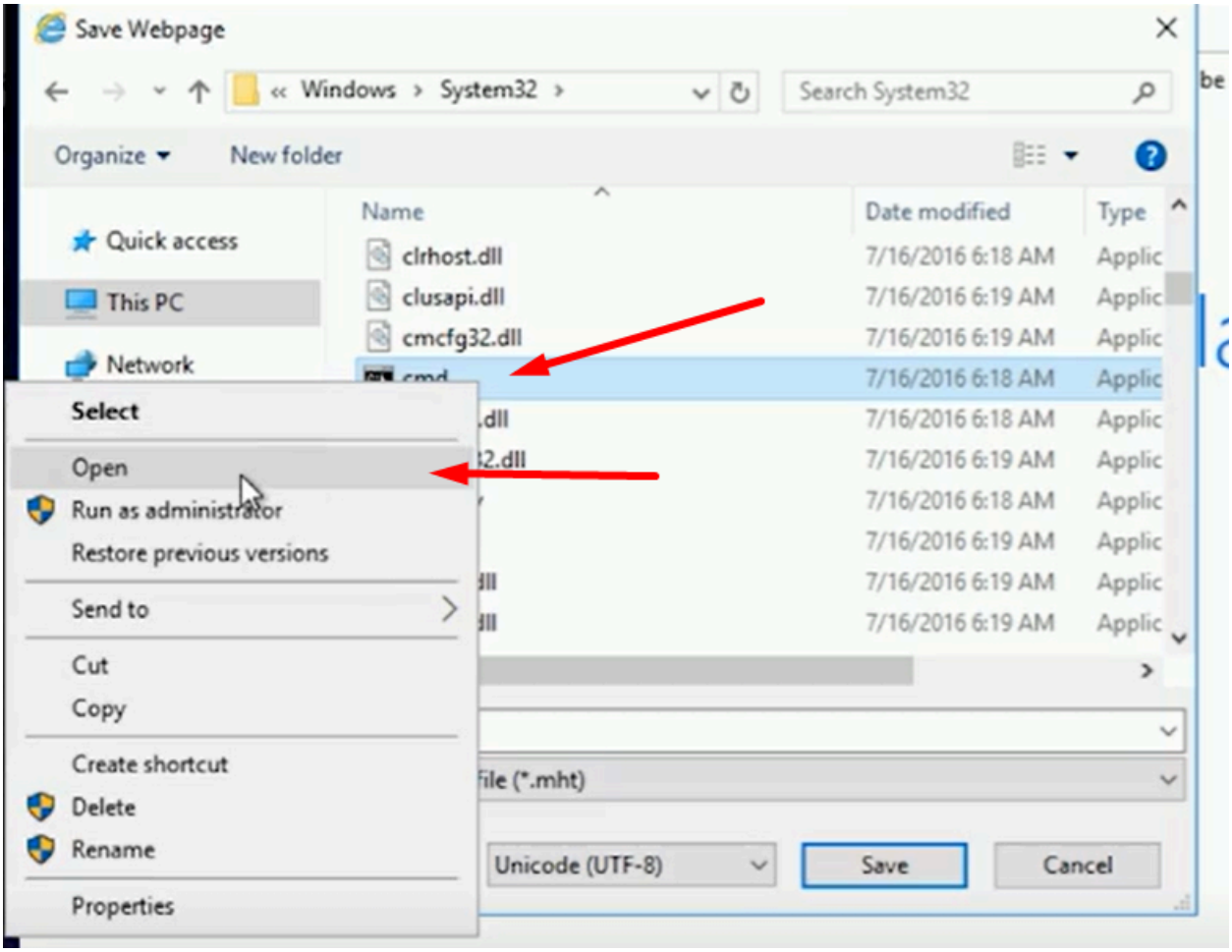
Click on this. This will open Internet explorer as system. Exit out of that exe by clicking OK or cancel or whatever.

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

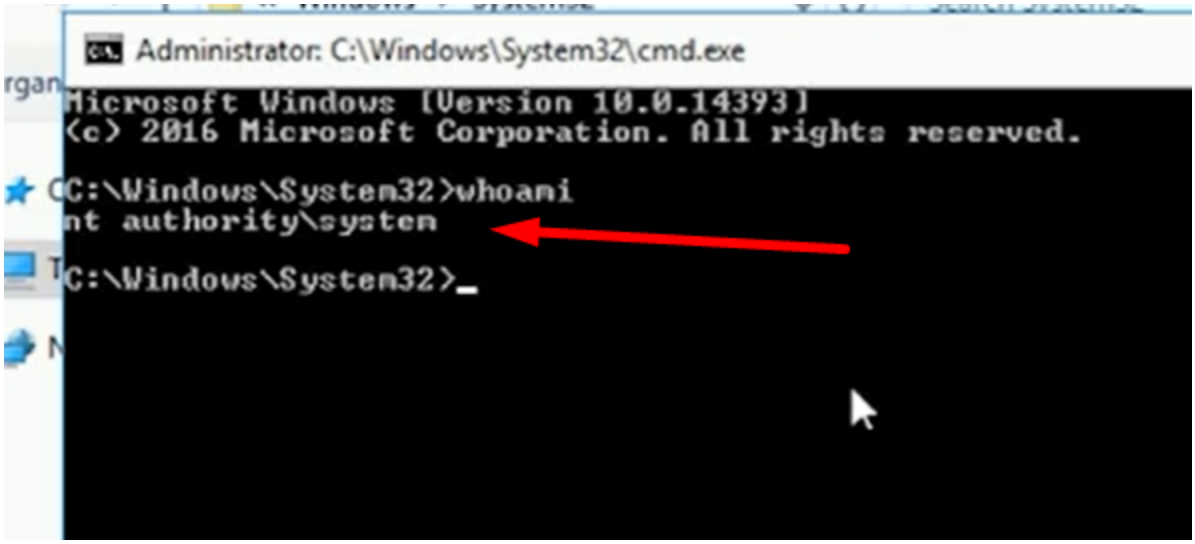


if error pop up, just click ok and ignore.





Find cmd.exe and open.



We are authority/system.

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