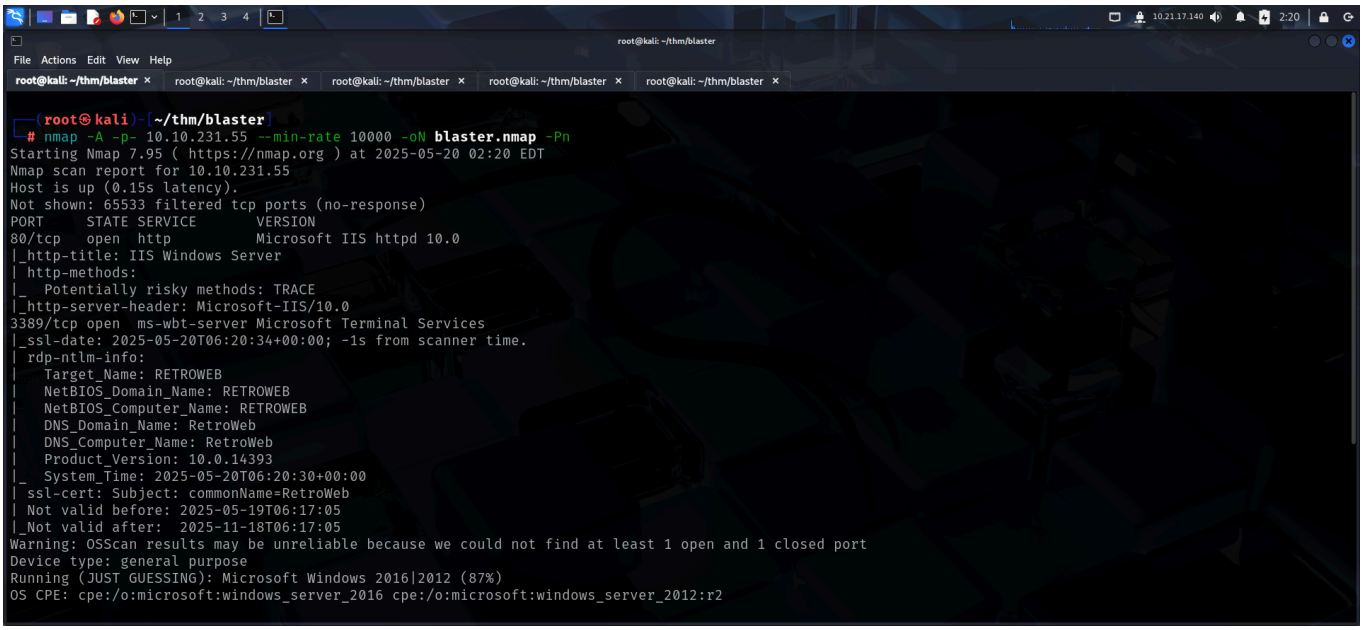
BLASTER

To access the machine, click on the link given below:

- https://tryhackme.com/room/blaster

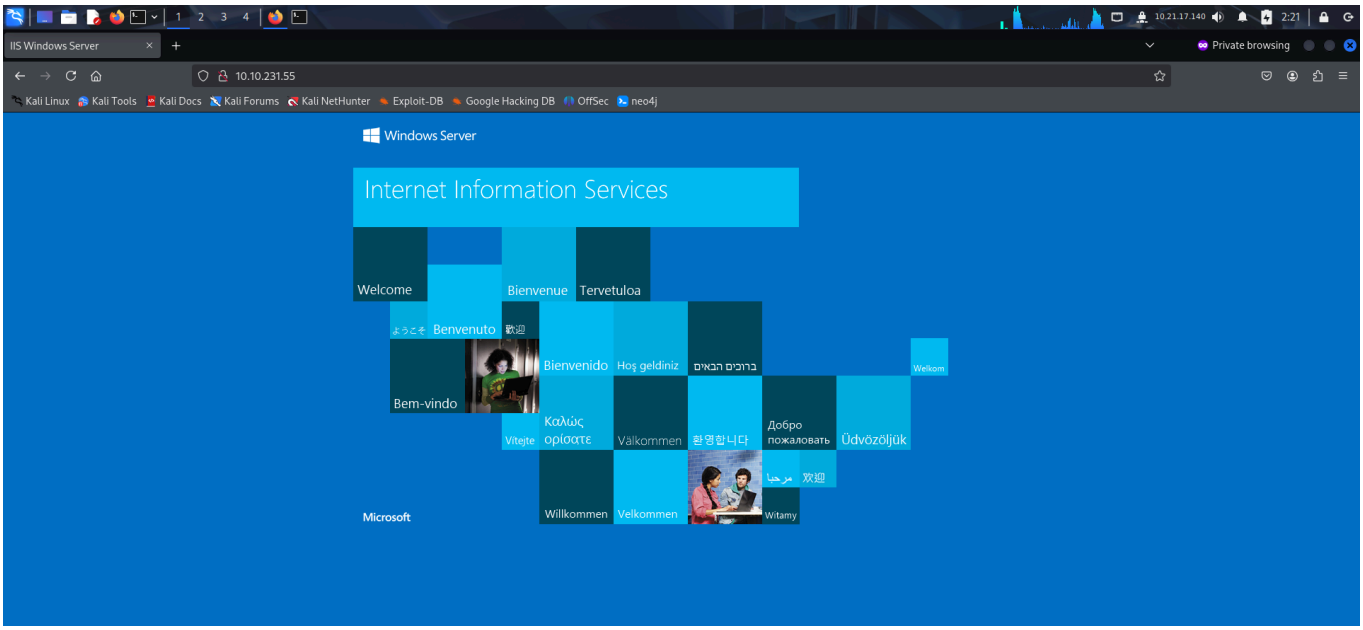
RECONNAISSANCE

I performed an **nmap** aggressive scan on the target to find open ports and the services running on them.

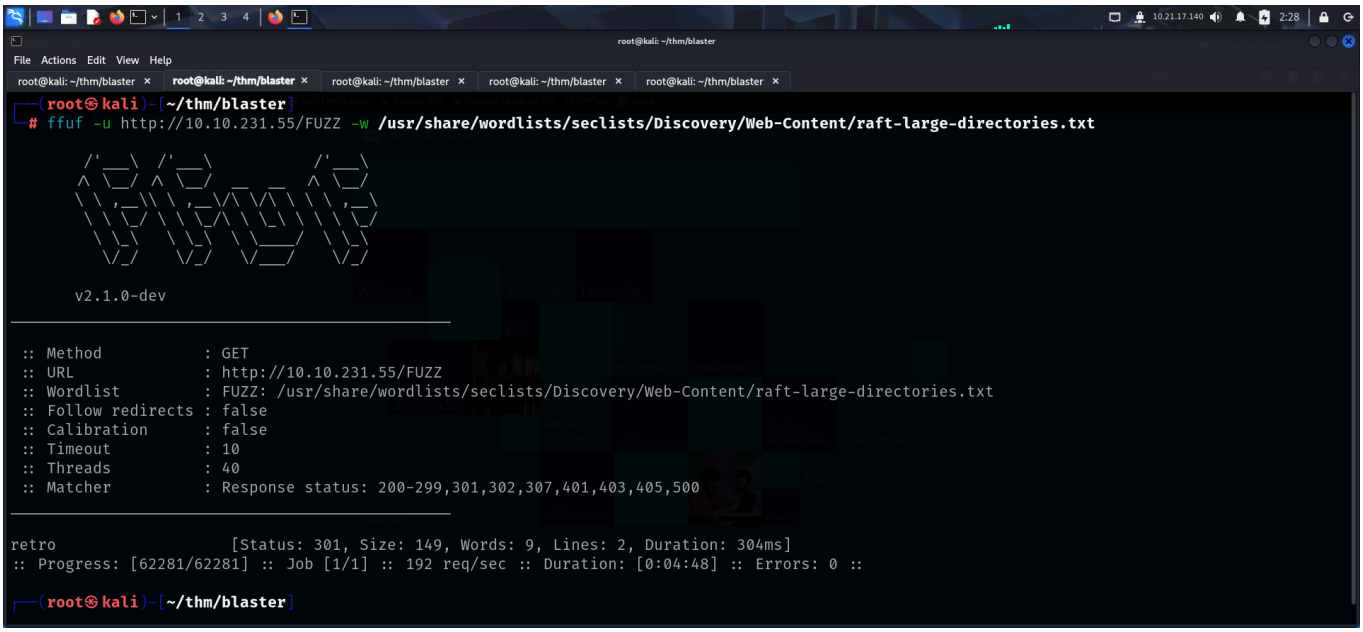


FOOTHOLD

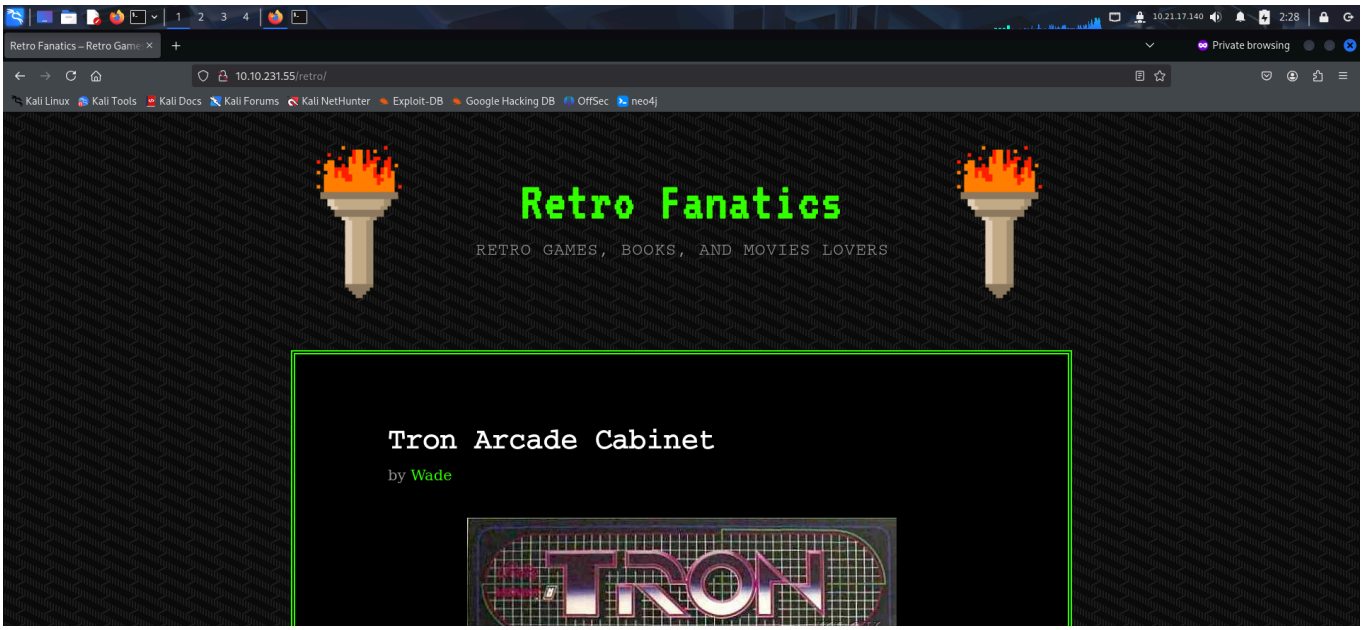
The nmap scan revealed a web application to be running on port 80, so I accessed it on my browser.



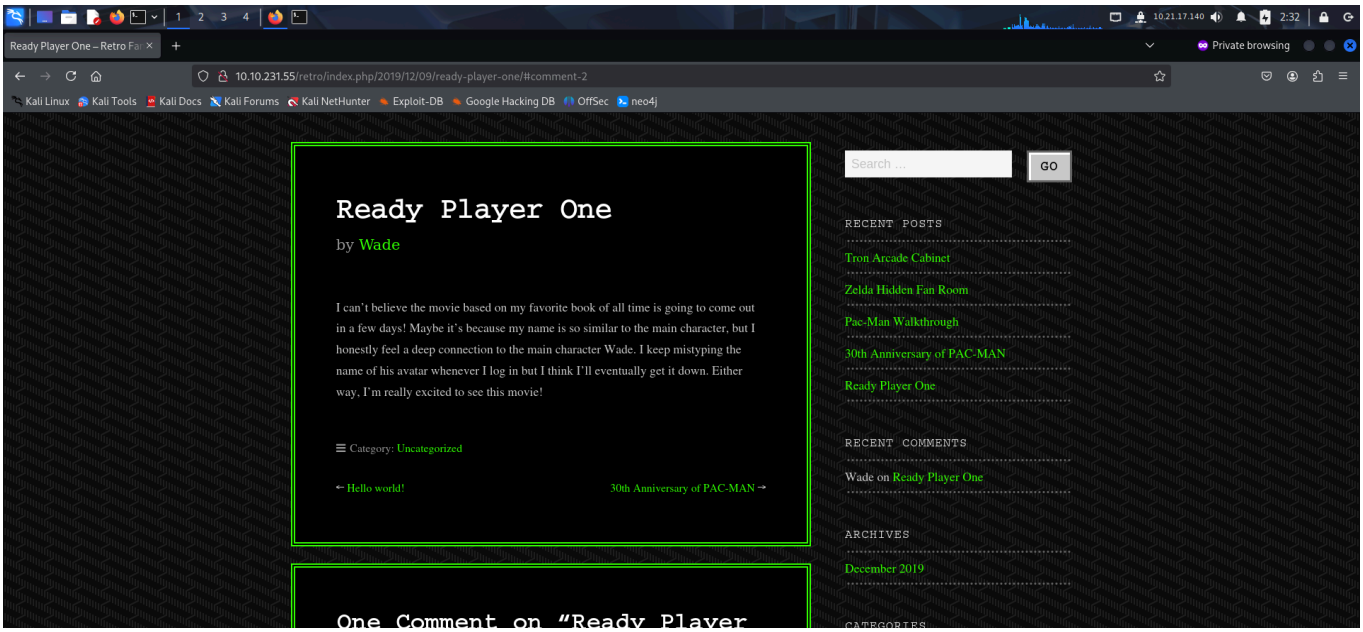
It was a default IIS landing page so I fuzzed for hidden directories and found one called *retro*.



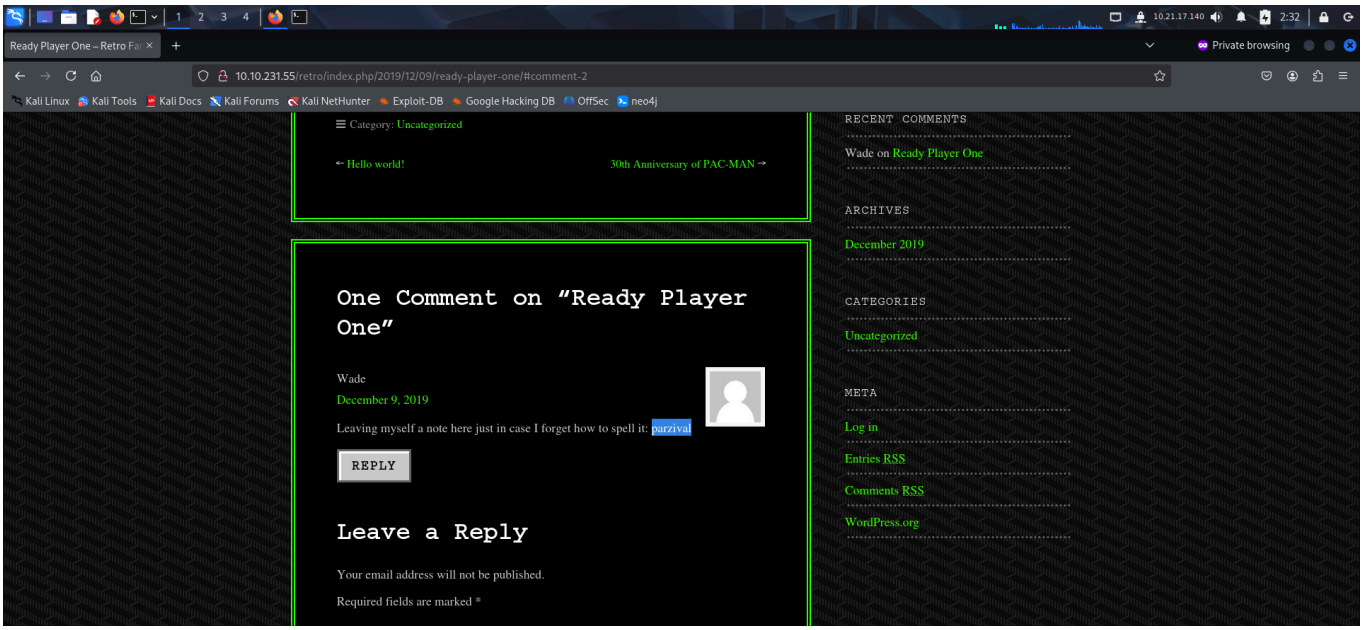
I visited the directory and found a blogging application.



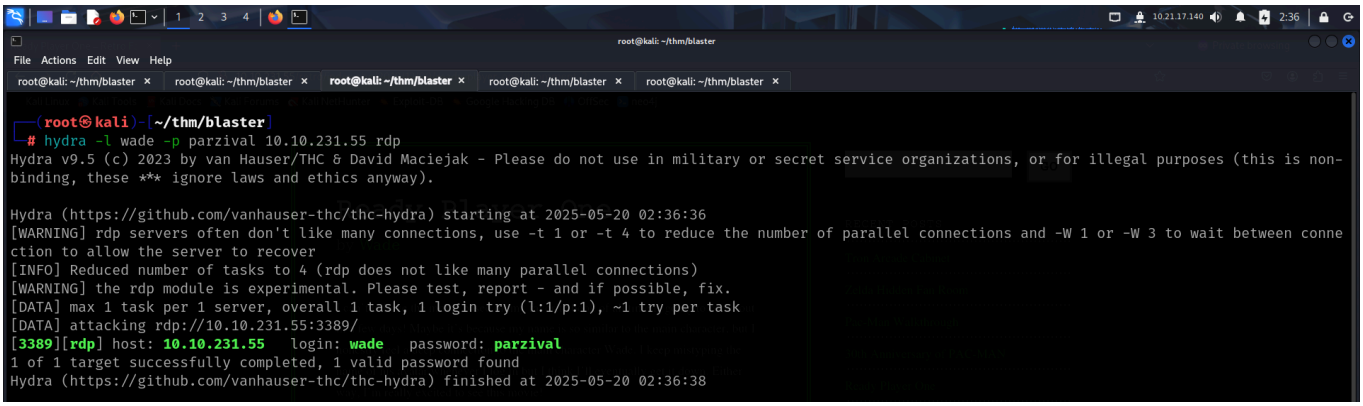
The author of the blog could be a user in the system so I kept note of it.



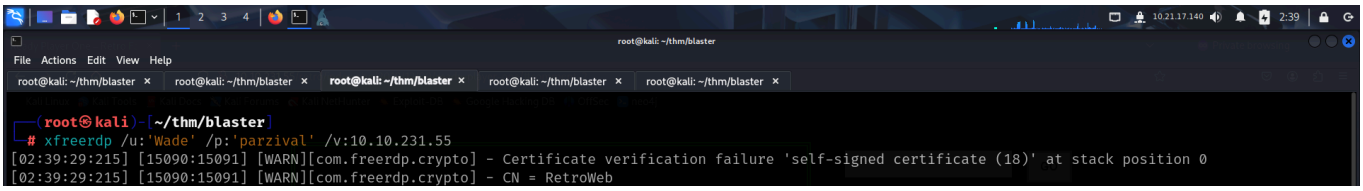
A comment on one of the blogs had a potential password.

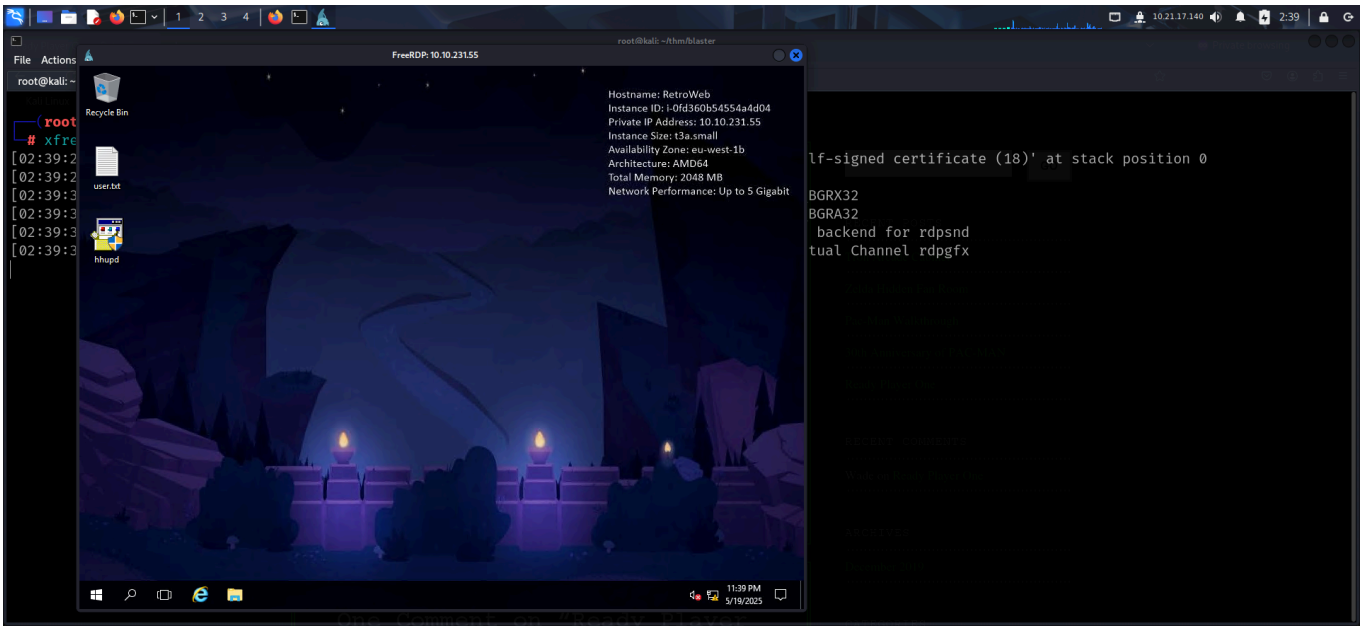


I checked if the username and password were valid and found that I could use them to access the target through **rdp**.

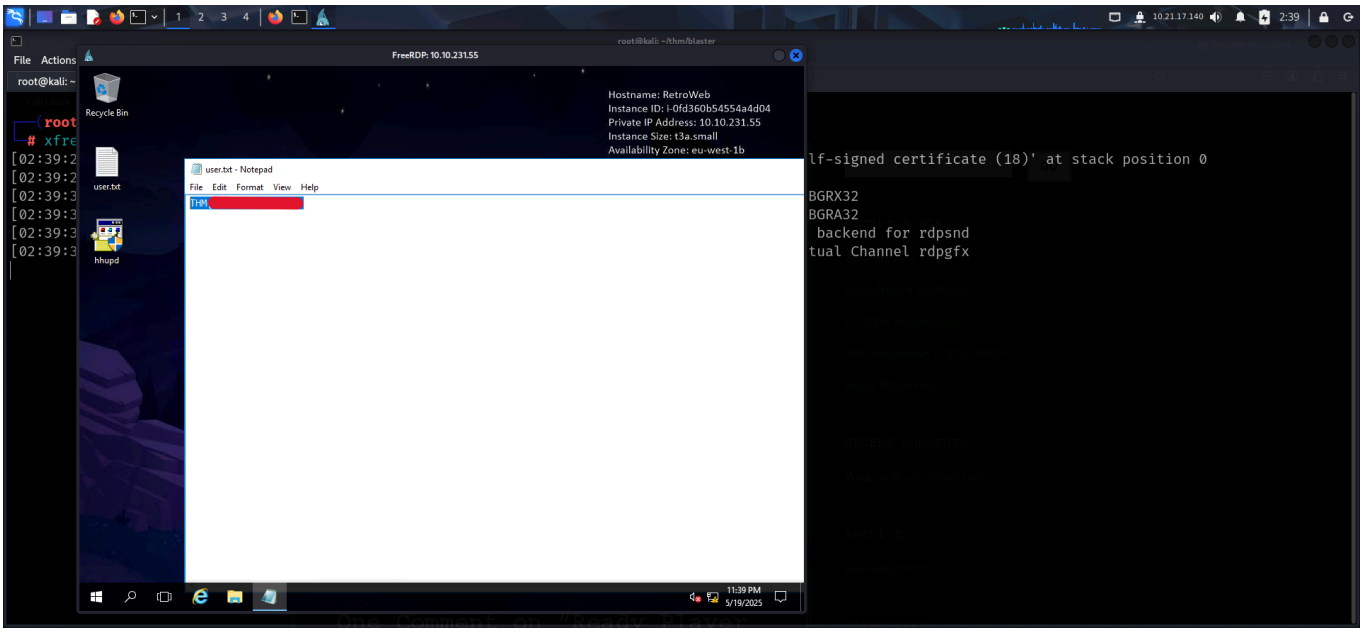


I used **xfreerdp** to access the machine.



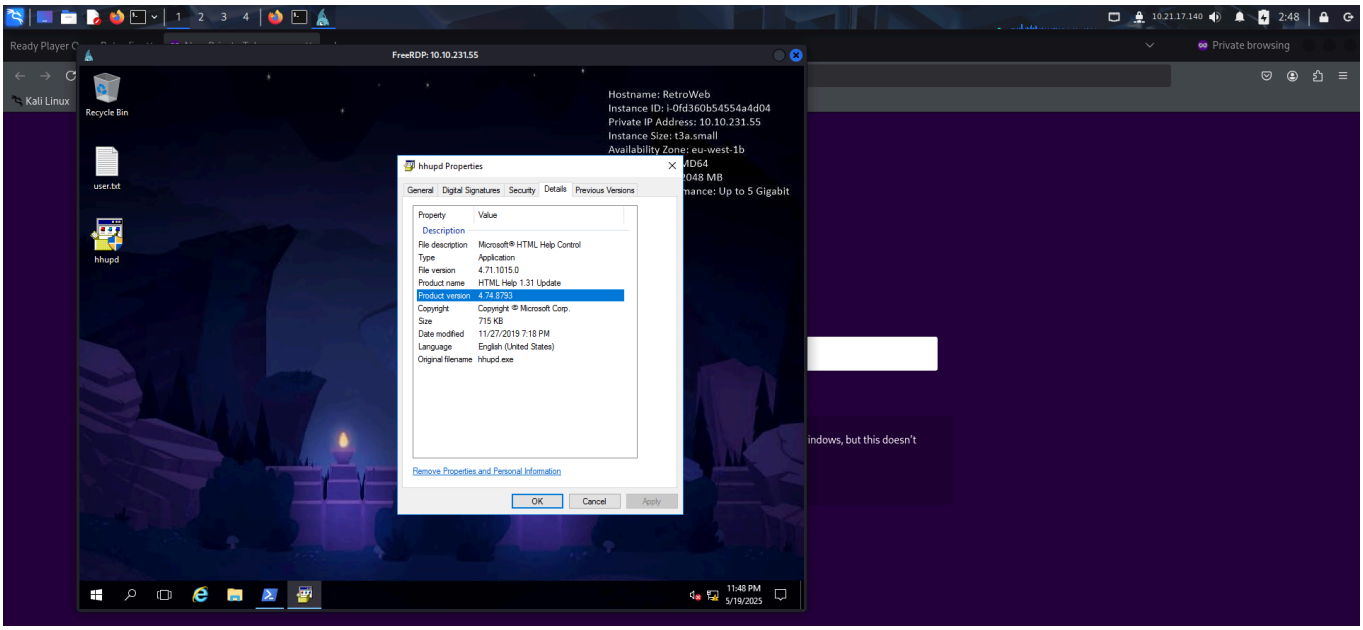


I found user.txt in the Desktop.

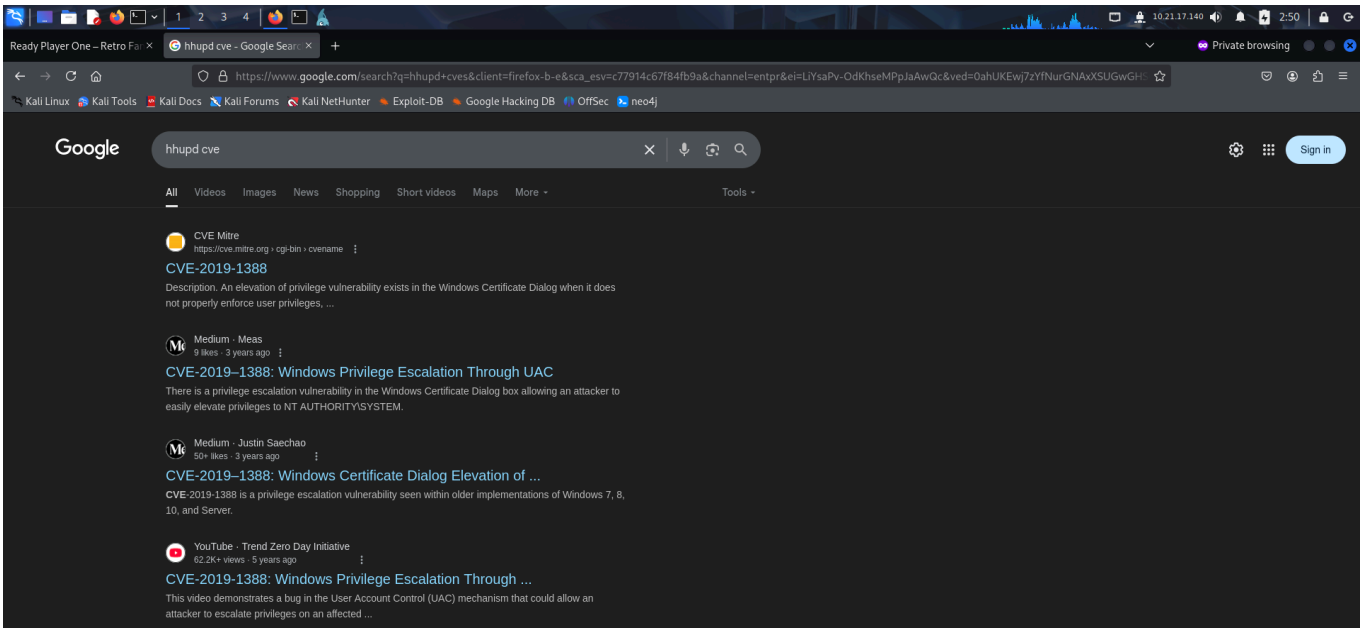


PRIVILEGE ESCALATION

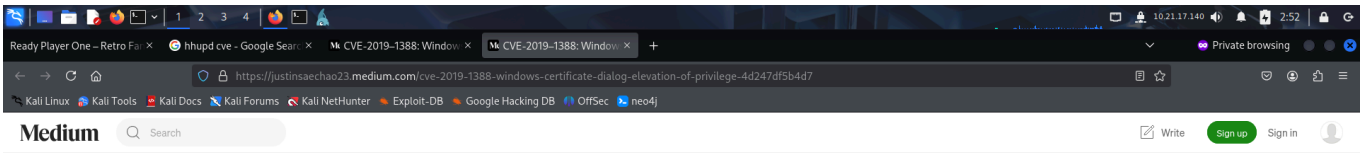
The Desktop had another application called hhupd.



I searched online for exploits and found articles for privilege escalation through UAC bypass.



link to article: https://justinsaechao23.medium.com/cve-2019-1388-windows-certificate-dialog-elevation-of-privilege-4d247df5b4d7



CVE-2019–1388: Windows Certificate Dialog Elevation of Privilege

Justin Saechao Follow 7 min read · Jun 10, 2021

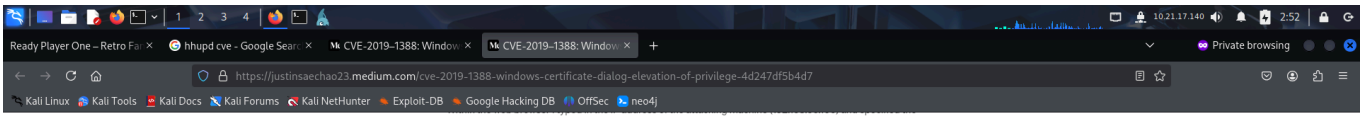
55

Overview:

CVE-2019-1388 is a privilege escalation vulnerability seen within older implementations of Windows 7, 8, 10, and Server. It is a low complexity vulnerability, meaning exploitation is relativity simple/low level. It is not complex to take advantage of and does not require any 'deep diving' into the system. As a privilege escalation vulnerability it allows a standard low level user to escalate their privileges to that of an administrator which would allow free reign over the target machine. In terms of requirements to

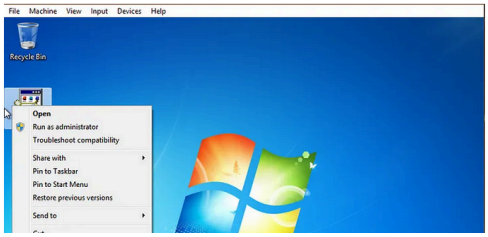
I followed the steps given in the article to escalate my privilege to administrator:

- Right click on the application and select run as Administrator

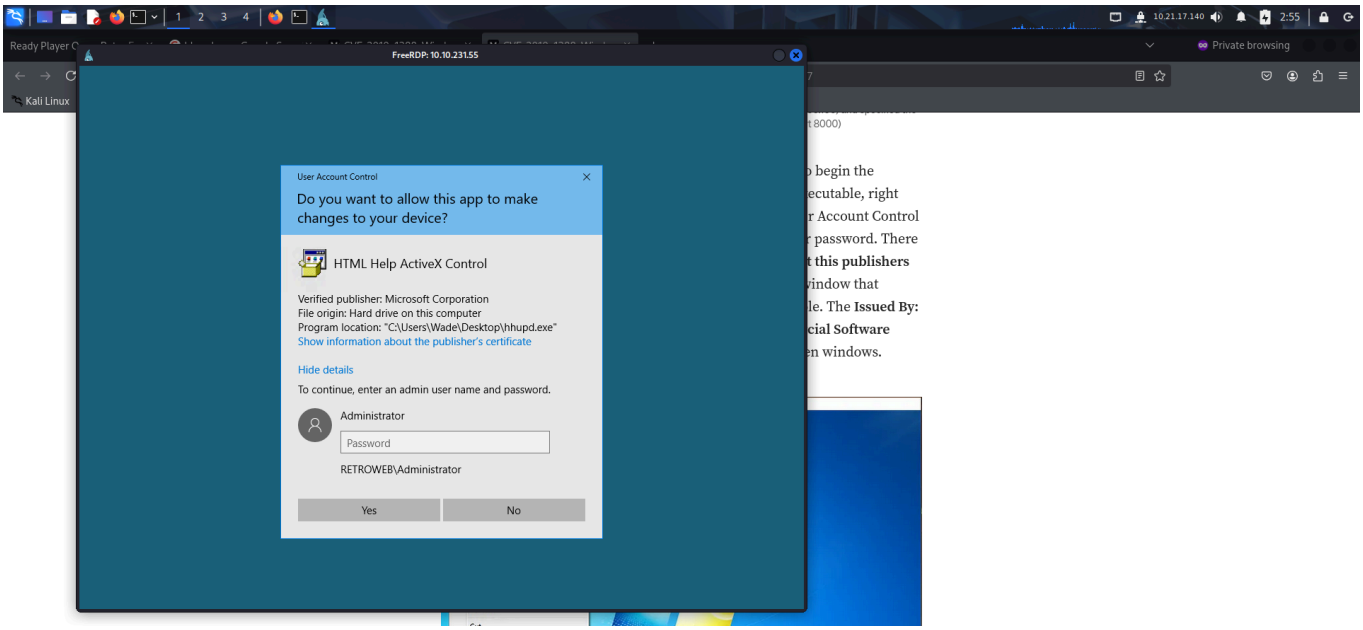


port the HTTP server was on (Python HTTP Server defaults to port 8000)

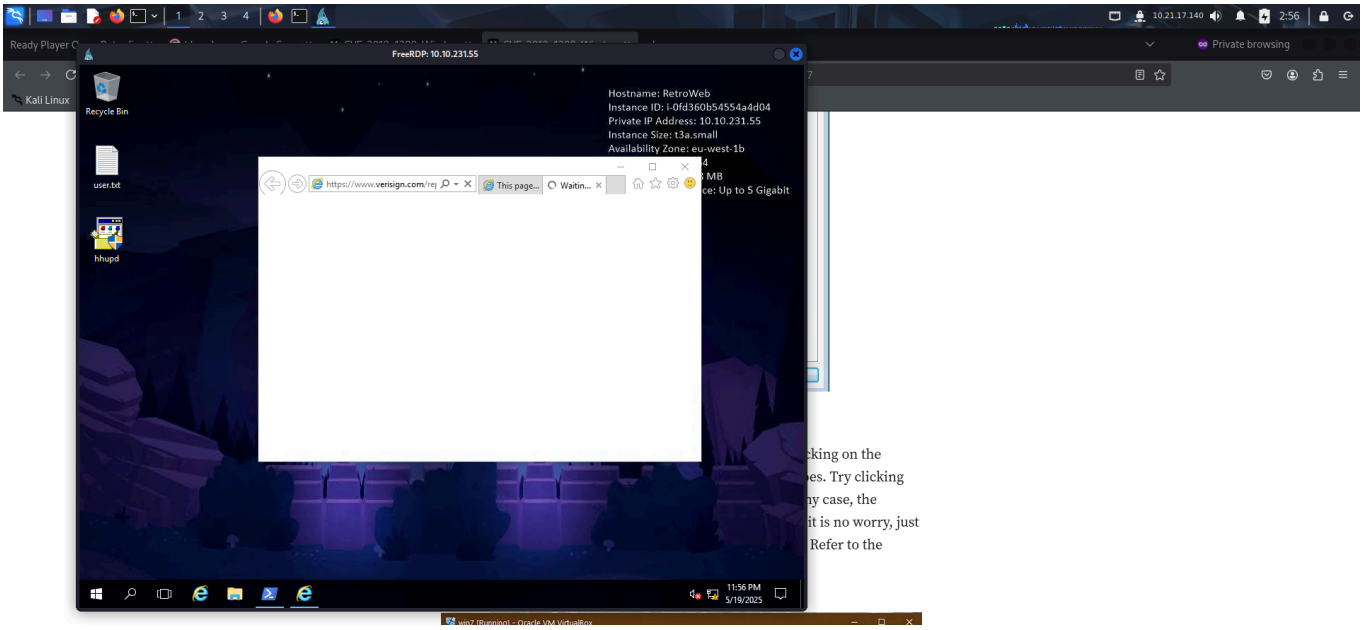
4. All the right strings are now in place and it is now time to begin the escalation phase. Navigate over to the newly transferred executable, right click on it, and click **Run as administrator**. A Windows User Account Control (UAC) window will pop up and prompt for an administrator password. There will be a highlighted link that says **Show information about this publishers certificate**. Click on that and you will be taken to another window that displays certificate information for the particular executable. The **Issued By:** line will display a highlighted hyperlink: **Verisign Commercial Software Publishers CA** which you can click on and then exit the open windows.

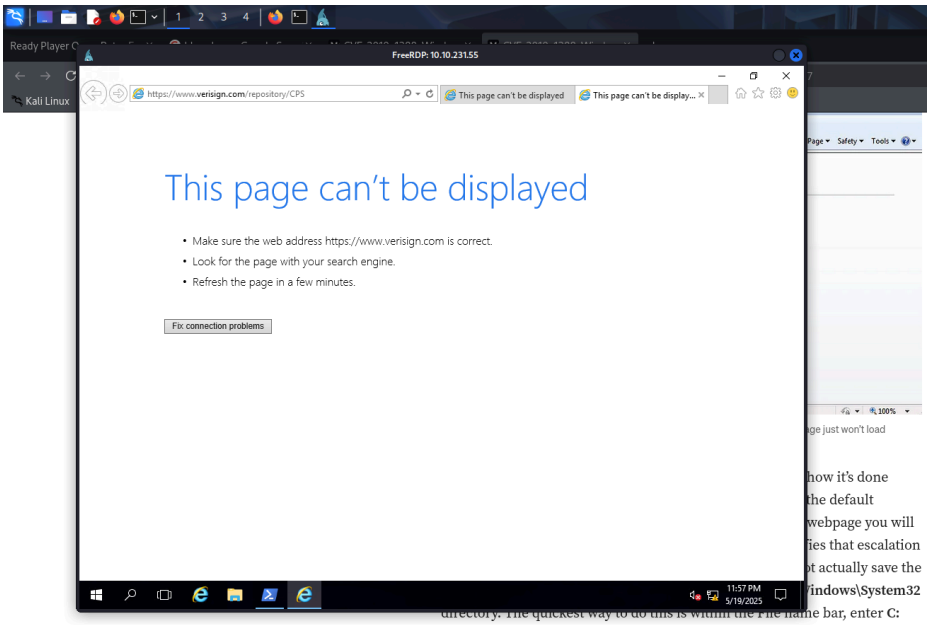


- A dialogue box appears. Click the *show information...* link.

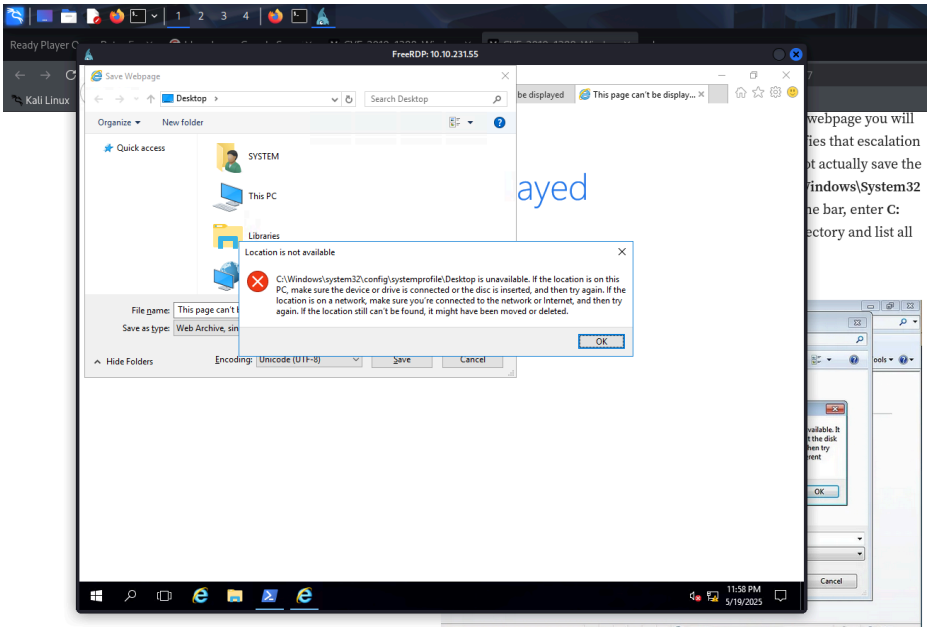


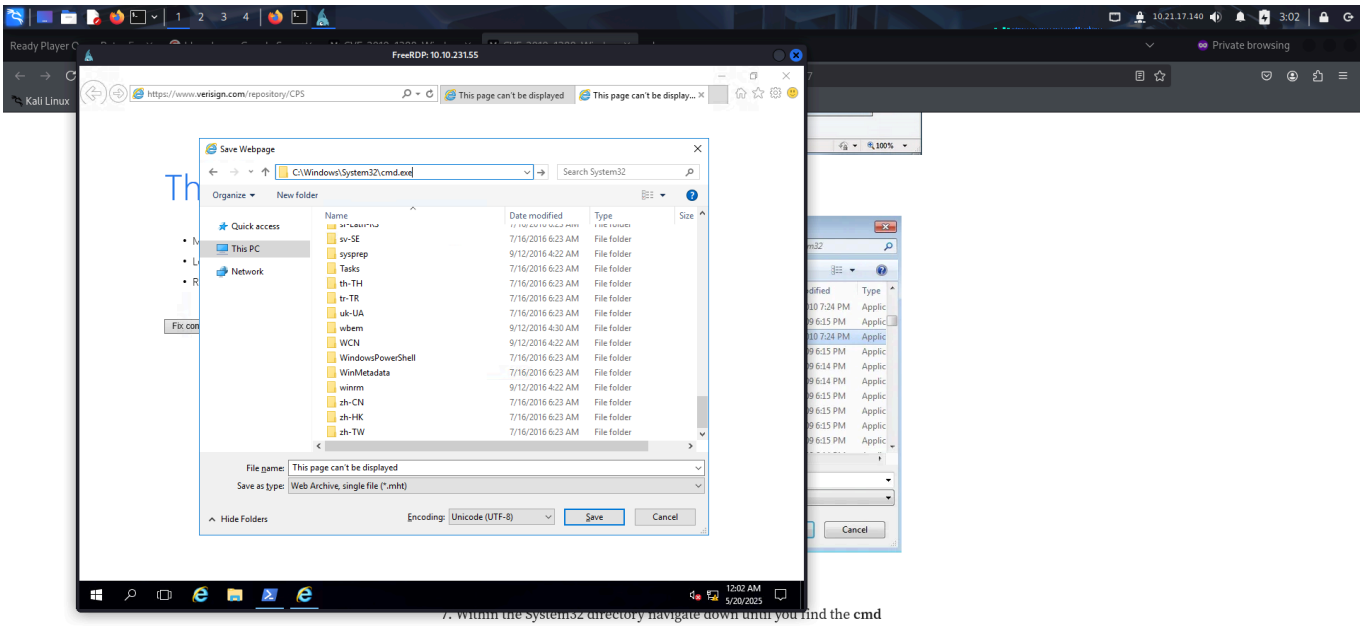
- A web browser will automatically open after clicking on the hyperlink. If not, click on the link again. The url should be of Verisign.



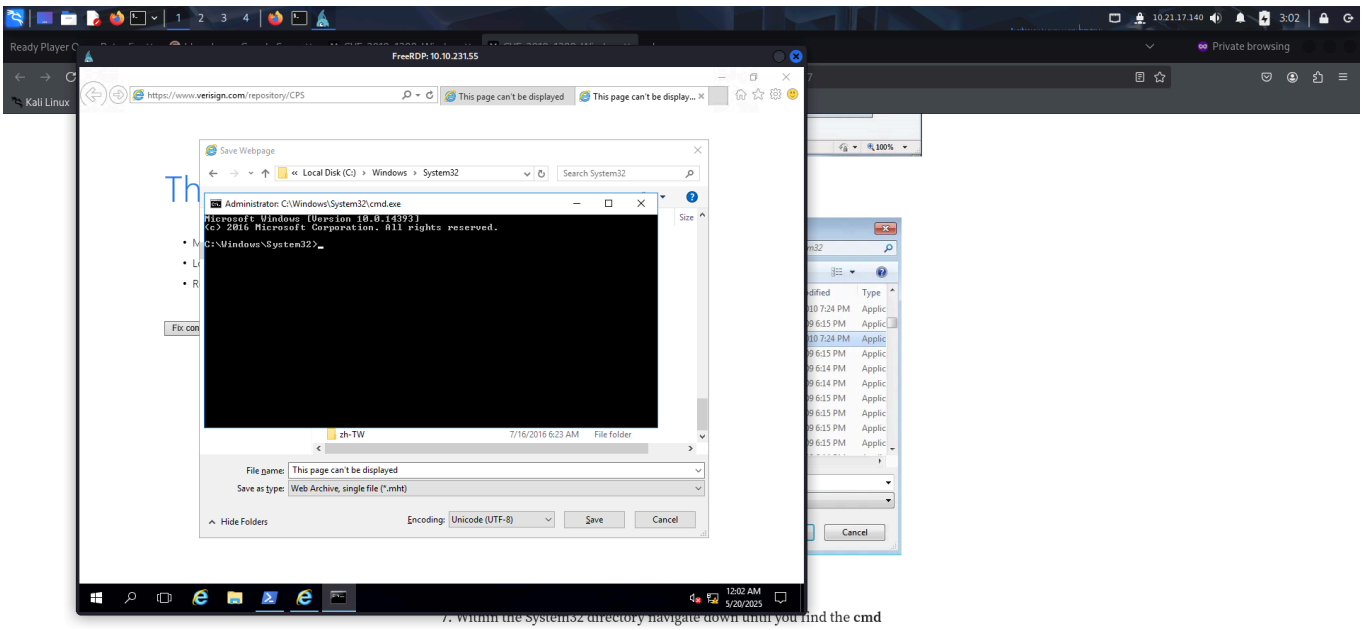


- Save the page in the following way:
  - click on save
  - ignore any warnings
  - a dialogue box will appear
  - within the file explorer, navigate to `C:\Windows\System32` and open `cmd.exe`



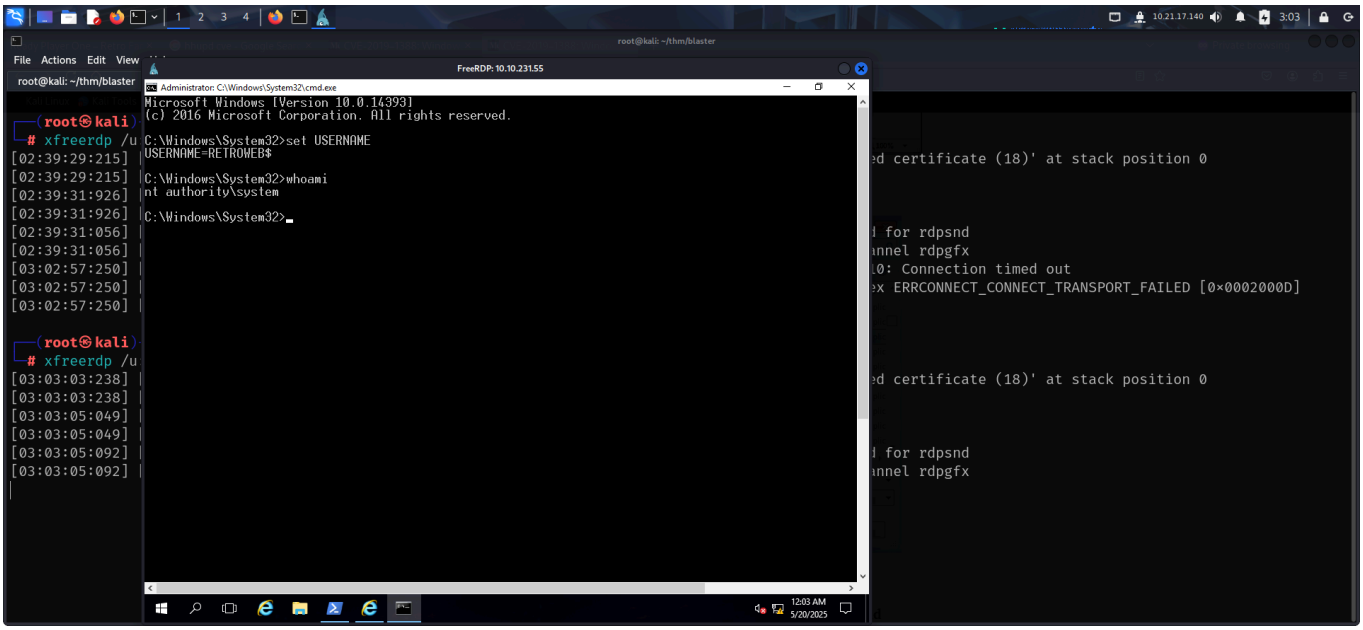


7. Within the System32 directory navigate down until you find the **cmd**

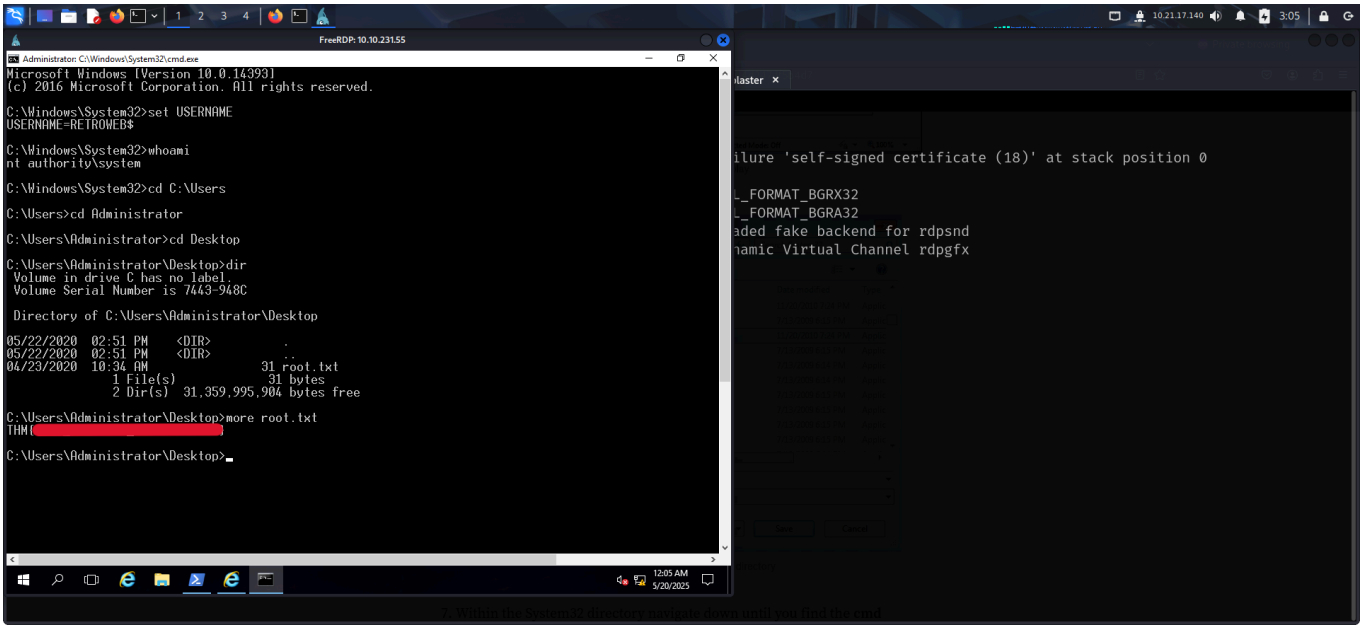


7. Within the System32 directory navigate down until you find the **cmd**

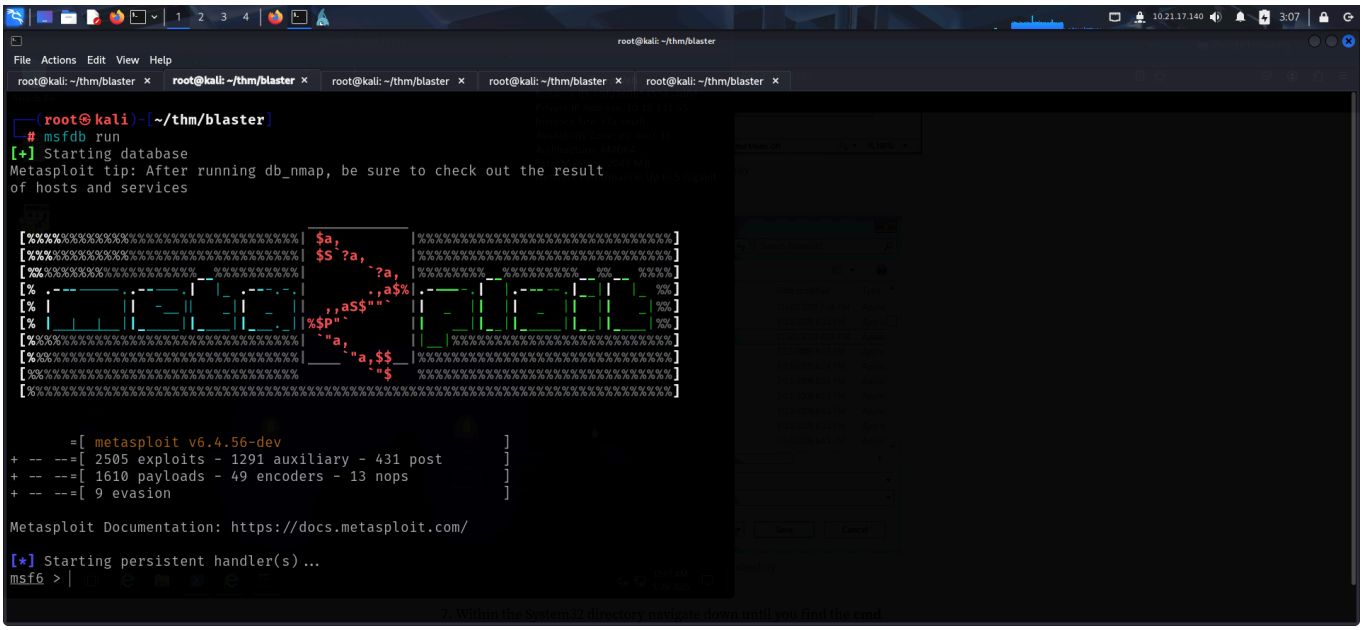
- I spawned a shell as NT Authority System.



- I then captured the root flag from Administrator's Desktop.

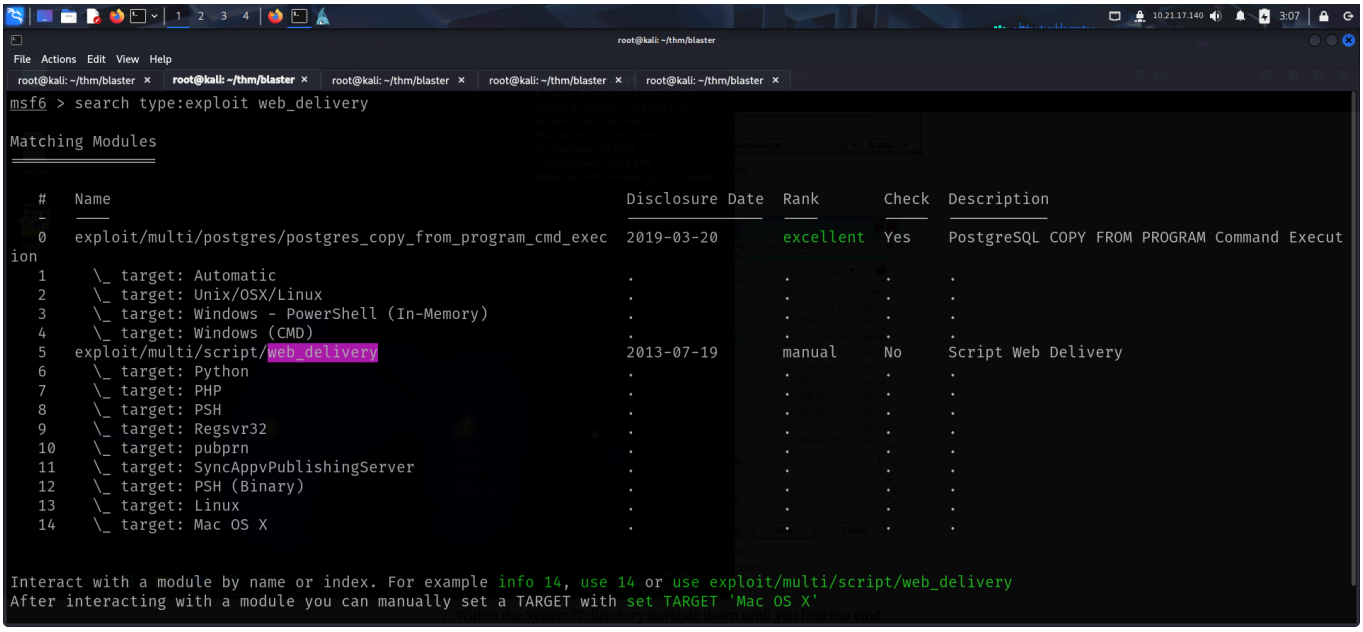


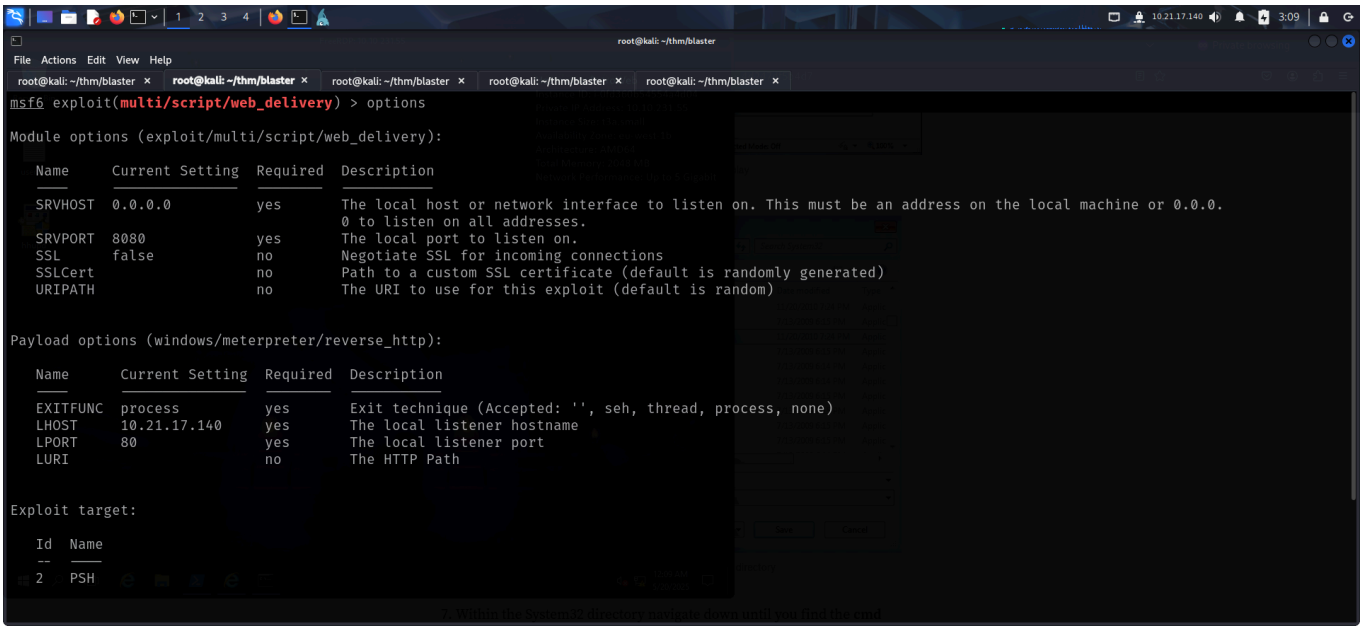
I wanted to get a meterpreter shell. So I started the **metasploit** framework.



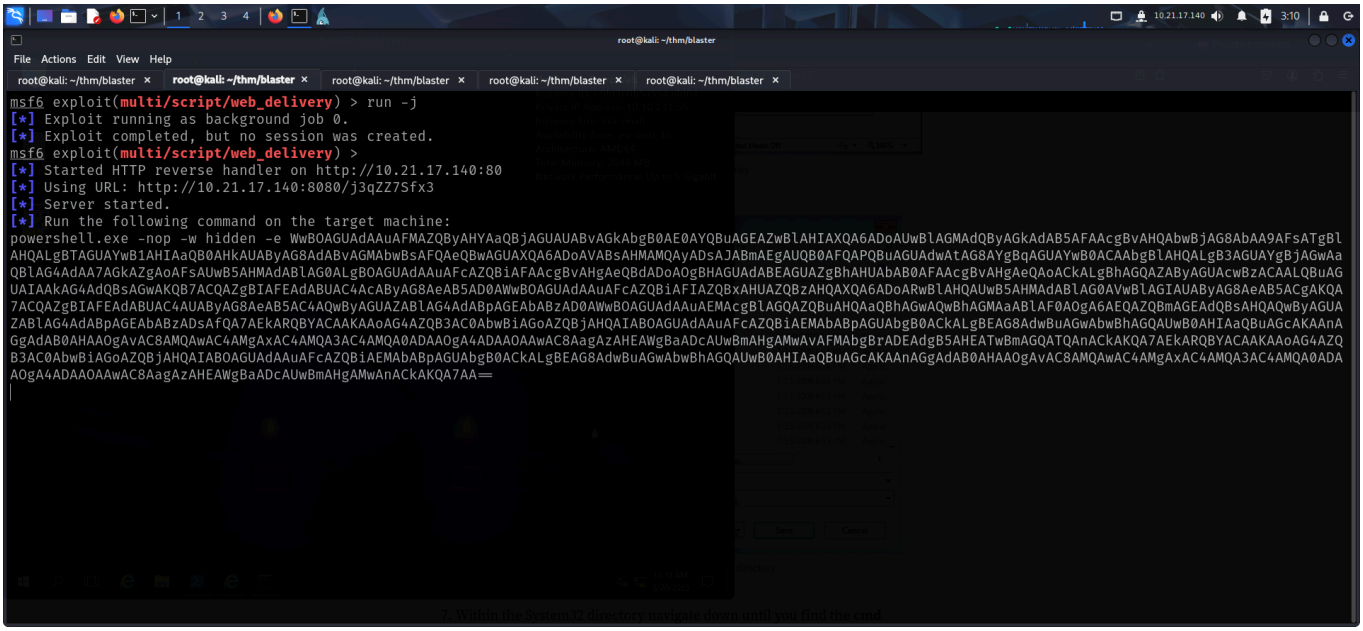
I used the following exploit to get a reverse meterpreter shell by executing a payload on the target:

`exploit/multi/script/web_delivery`

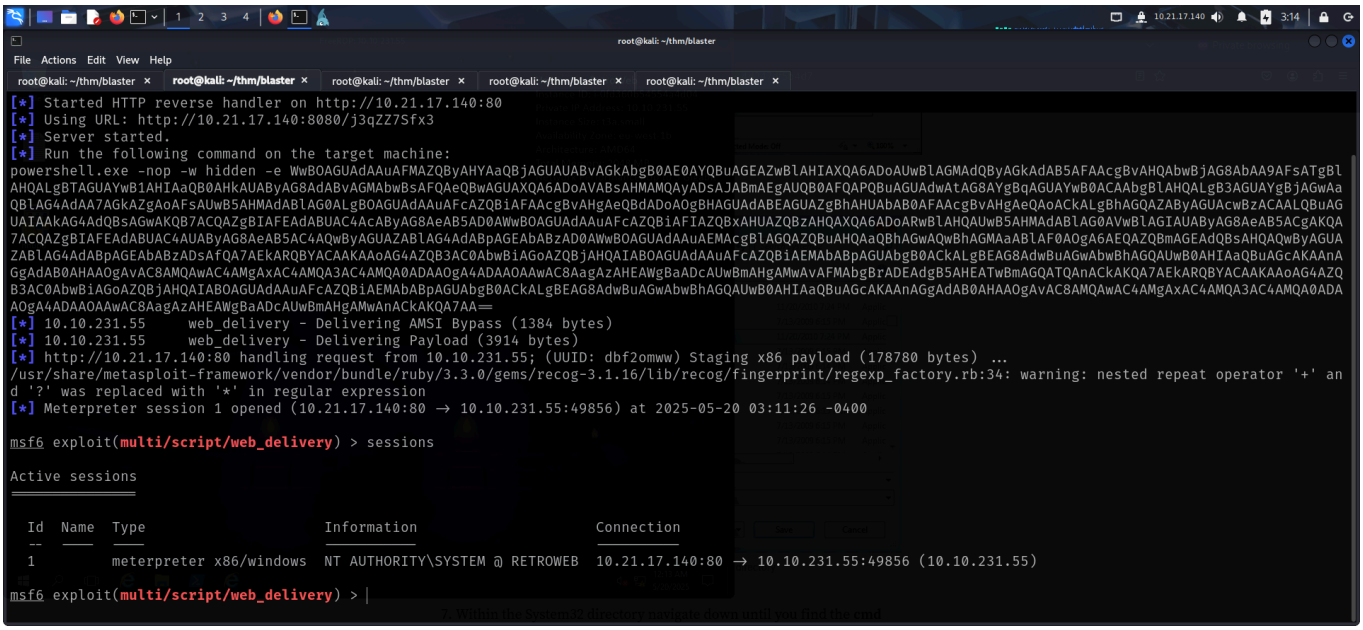


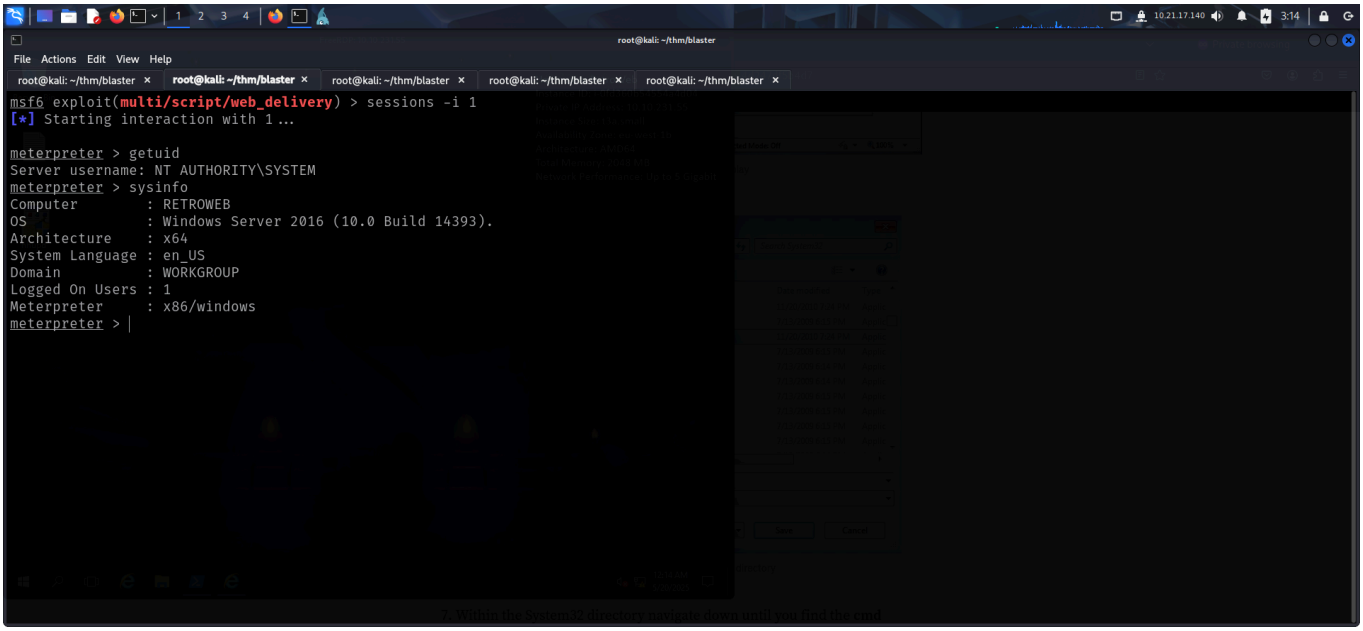


7. Within the System32 directory navigate down until you find the cmd



7. Within the System32 directory navigate down until you find the cmd





SUMMARY

Here's a short summary of how I solved **Blaster**:

- I discovered a blogging application on the IIS web server
- I found a username and password in the blogs
- I captured user.txt from Wade's Desktop
- I found an application called **hhupd** on the Desktop and looked for related exploits.
- I used the application to bypass UAC and spawn a shell as NT Authority System
- I migrated the shell to a meterpreter session using the `web_delivery` exploit in **metasploit** framework.
- I captured the root flag from Administrator's Desktop.

That's it from my side!
Until next time :)