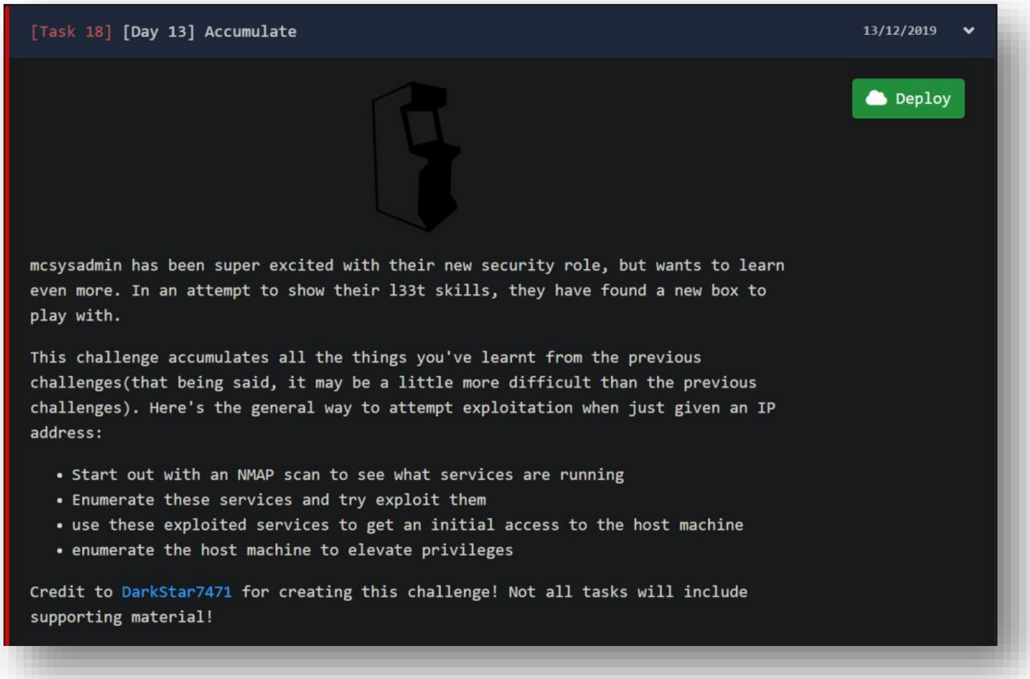
- No supporting material for this challenge!!



[Task 18] [Day 13] Accumulate

13/12/2019

mcsysadmin has been super excited with their new security role, but wants to learn even more. In an attempt to show their l33t skills, they have found a new box to play with.

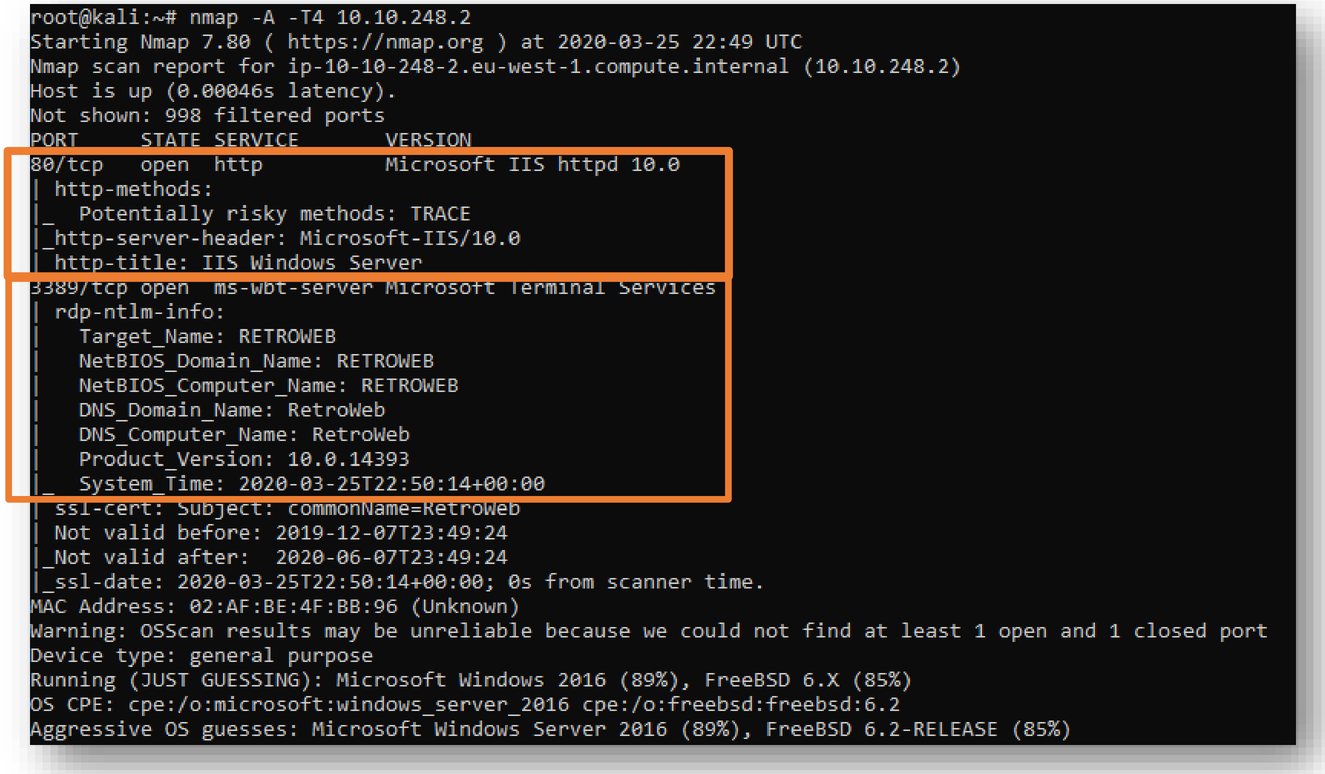
This challenge accumulates all the things you've learnt from the previous challenges(that being said, it may be a little more difficult than the previous challenges). Here's the general way to attempt exploitation when just given an IP address:

- Start out with an NMAP scan to see what services are running
- Enumerate these services and try exploit them
- use these exploited services to get an initial access to the host machine
- enumerate the host machine to elevate privileges

Credit to DarkStar7471 for creating this challenge! Not all tasks will include supporting material!

Objectives

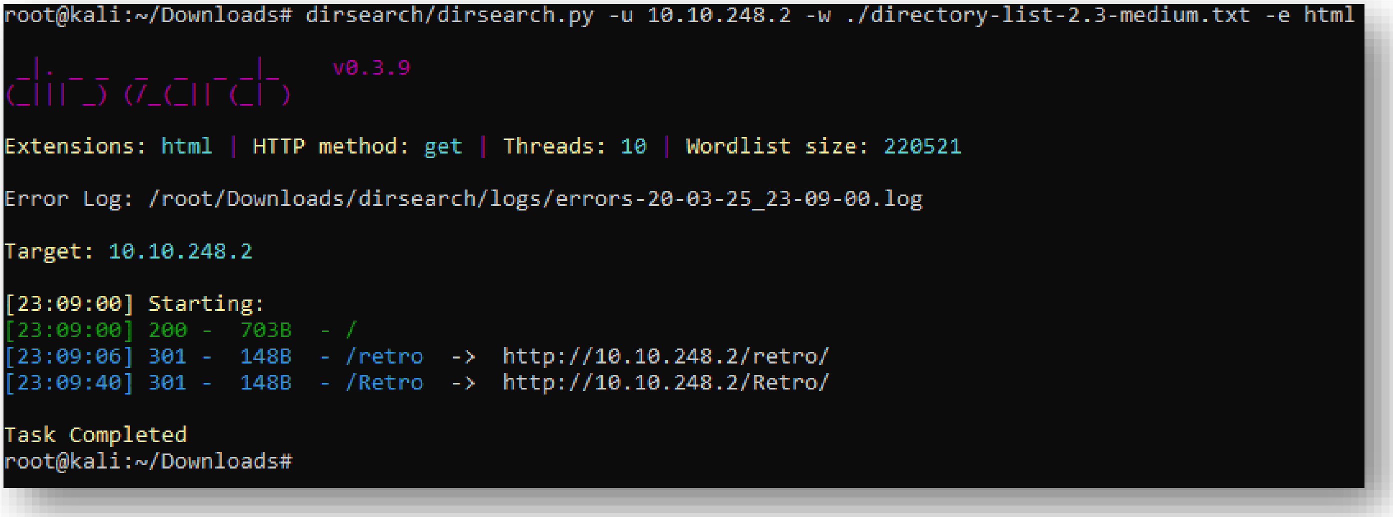
1. A web server is running on the target. What is the hidden directory which the website lives on?
2. Gain initial access and read the contents of user.txt
3. [Optional] Elevate privileges and read the content of root.txt



```
root@kali:~# nmap -A -T4 10.10.248.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 22:49 UTC
Nmap scan report for ip-10-10-248-2.eu-west-1.compute.internal (10.10.248.2)
Host is up (0.00046s latency).
Not shown: 998 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: 2020-03-25T22:50:14+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: 2020-03-25T22:50:14+00:00; 0s from scanner time.
MAC Address: 02:AF:BE:4F:BB:96 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows Server 2016 (89%), FreeBSD 6.2-RELEASE (85%)
```

- An nmap scan shows two open ports, one is a web server on port 80 and the other is a Microsoft terminal on port 3389

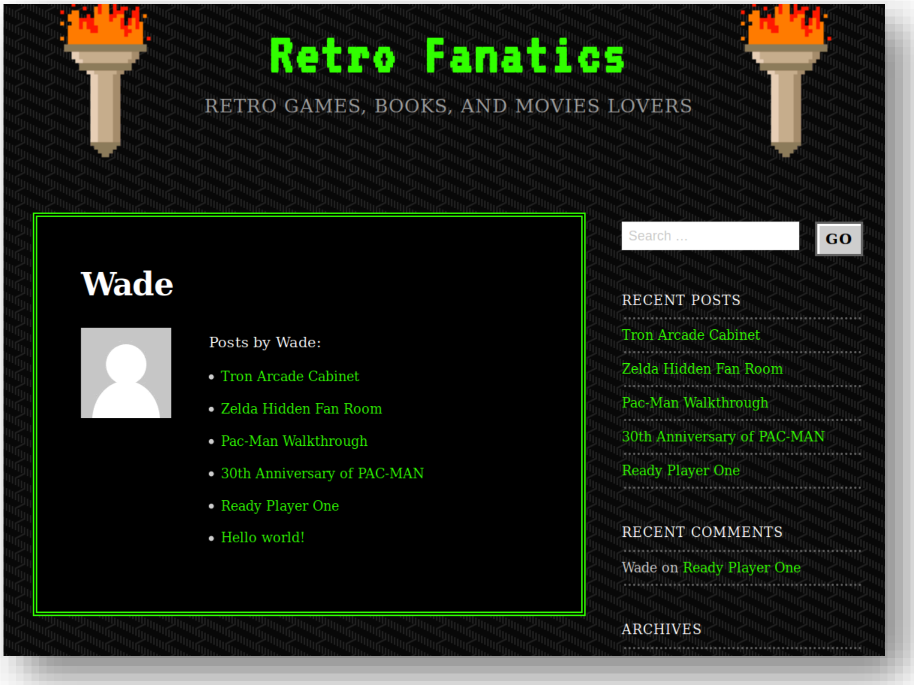
1. A web server is running on the target. What is the hidden directory which the website lives on?
   - Let's try out a directory search brute force attack
   - Referencing Day 2's challenge: https://docs.google.com/document/d/1622ejYtCmLOS0zd16CyfhA1xgQk8l55gYWMY8fnpHfQ/edit
   - The directory list is found at the directory buster github: https://github.com/daviddias/node-dirbuster/tree/master/lists



```
root@kali:~/Downloads# dirsearch/dirsearch.py -u 10.10.248.2 -w ./directory-list-2.3-medium.txt -e html

 _|. _ _  _  _  _ _|_    v0.3.9
(_||| _) (/_(_|| (_| )

Extensions: html | HTTP method: get | Threads: 10 | Wordlist size: 220521

Error Log: /root/Downloads/dirsearch/logs/errors-20-03-25_23-09-00.log

Target: 10.10.248.2

[23:09:00] Starting:
[23:09:00] 200 -   703B  - /
[23:09:06] 301 -   148B  - /retro  ->  http://10.10.248.2/retro/
[23:09:40] 301 -   148B  - /Retro  ->  http://10.10.248.2/Retro/

Task Completed
root@kali:~/Downloads#
```

   - The hidden directory is **/retro**

2. Gain initial access and read the contents of user.txt



Retro Fanatics

RETRO GAMES, BOOKS, AND MOVIES LOVERS

Wade

Posts by Wade:

- Tron Arcade Cabinet
- Zelda Hidden Fan Room
- Pac-Man Walkthrough
- 30th Anniversary of PAC-MAN
- Ready Player One
- Hello world!

RECENT POSTS

Tron Arcade Cabinet

Zelda Hidden Fan Room

Pac-Man Walkthrough

30th Anniversary of PAC-MAN

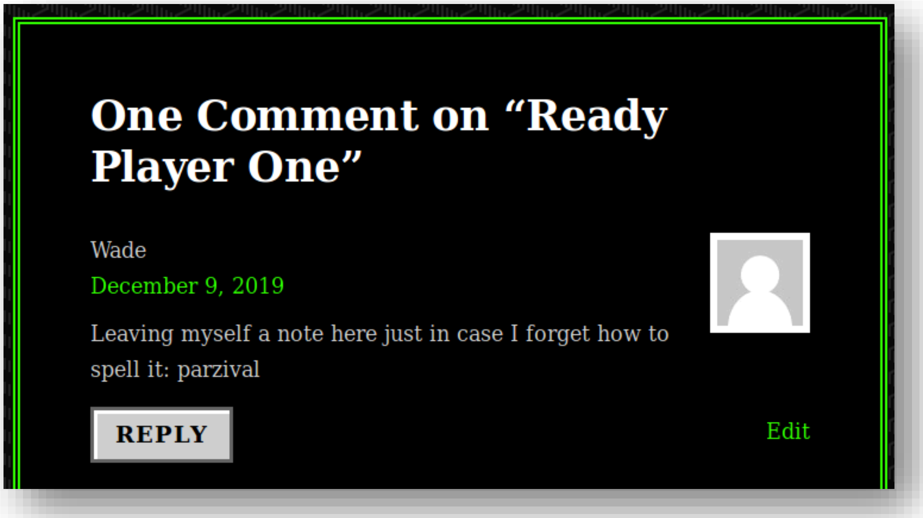
Ready Player One

RECENT COMMENTS

Wade on Ready Player One

ARCHIVES

- Visit and enumerate the /retro website; we can see that all the posts are made by a user named wade and the only comment on the site is a reminder of how to spell ‘parzival’. This is a reference to ready player one, a book by ernest cline about a dystopian future where everyone works and plays in a virtual reality world that is based off of 70s and 80s pop culture.

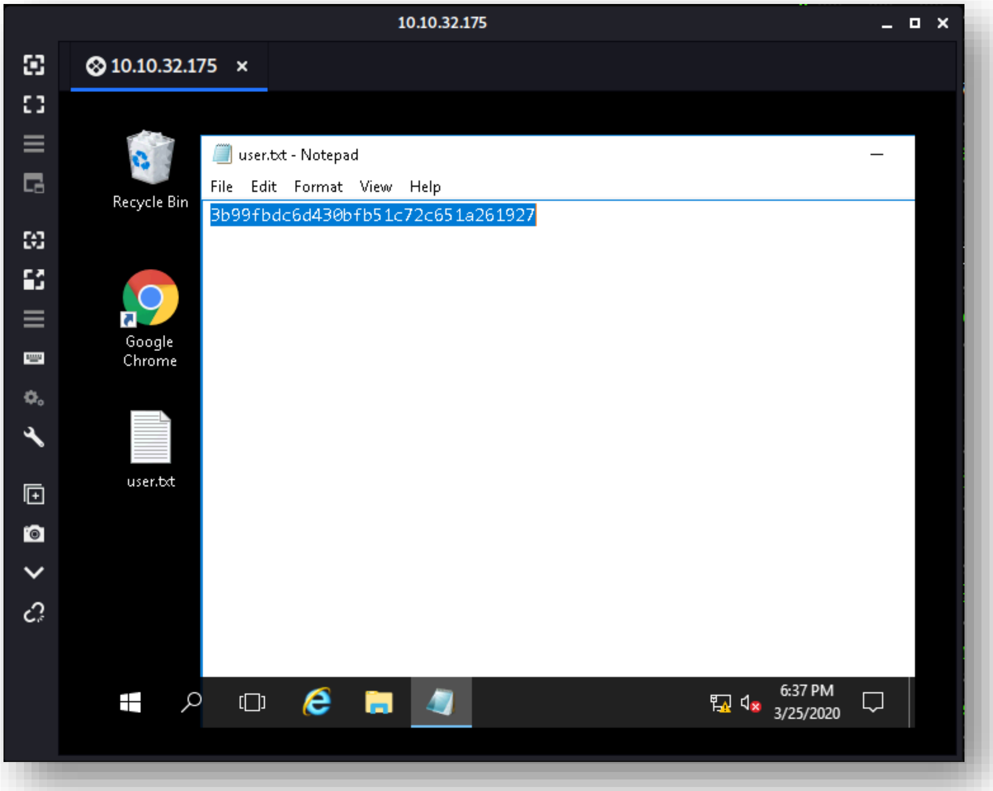


One Comment on “Ready Player One”

Wade
December 9, 2019

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

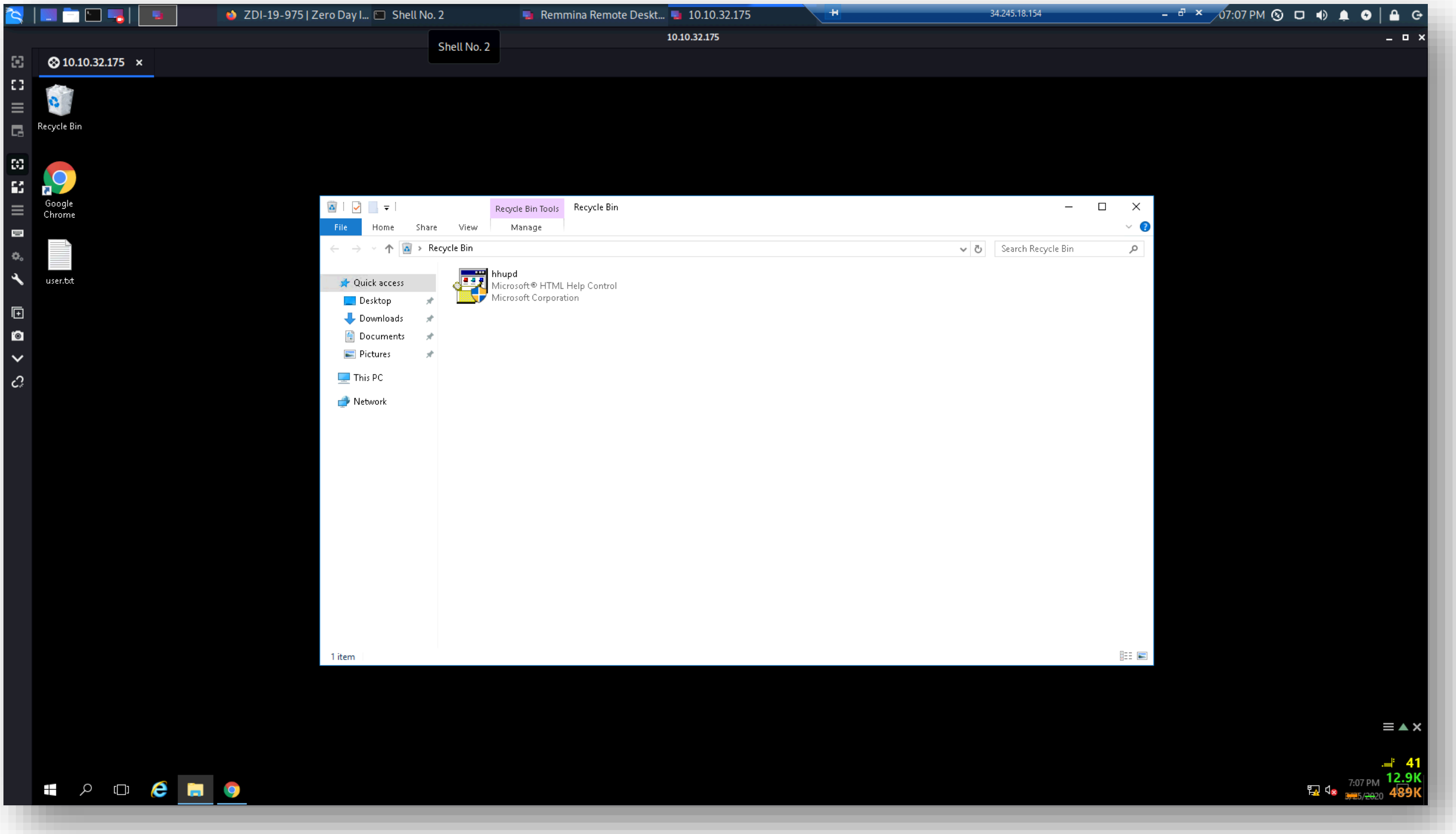
- Wade’s site uses wordpress and the password ‘parzival’ allows access to the site admin page, but there is nothing of note or interest there
- I tried using Metasploit and search for CVE’s that match the services found by nmap on the machine, but none were relevant (I tried many of them)
  - Tried many IIS exploits, but they are for older versions
  - Tried a couple RDP exploits but I wasn’t sure what prerequisites were needed or how to set it up…
- Next logical step is to connect to the machine via RDP. I’m currently connected to the THM kali machine via RDP on my windows client. Then inside the kali machine, I needed to install Remmina, a RDP client for Linux.
- Using the credentials wade:parzival, we have access to the windows server 2016 machine



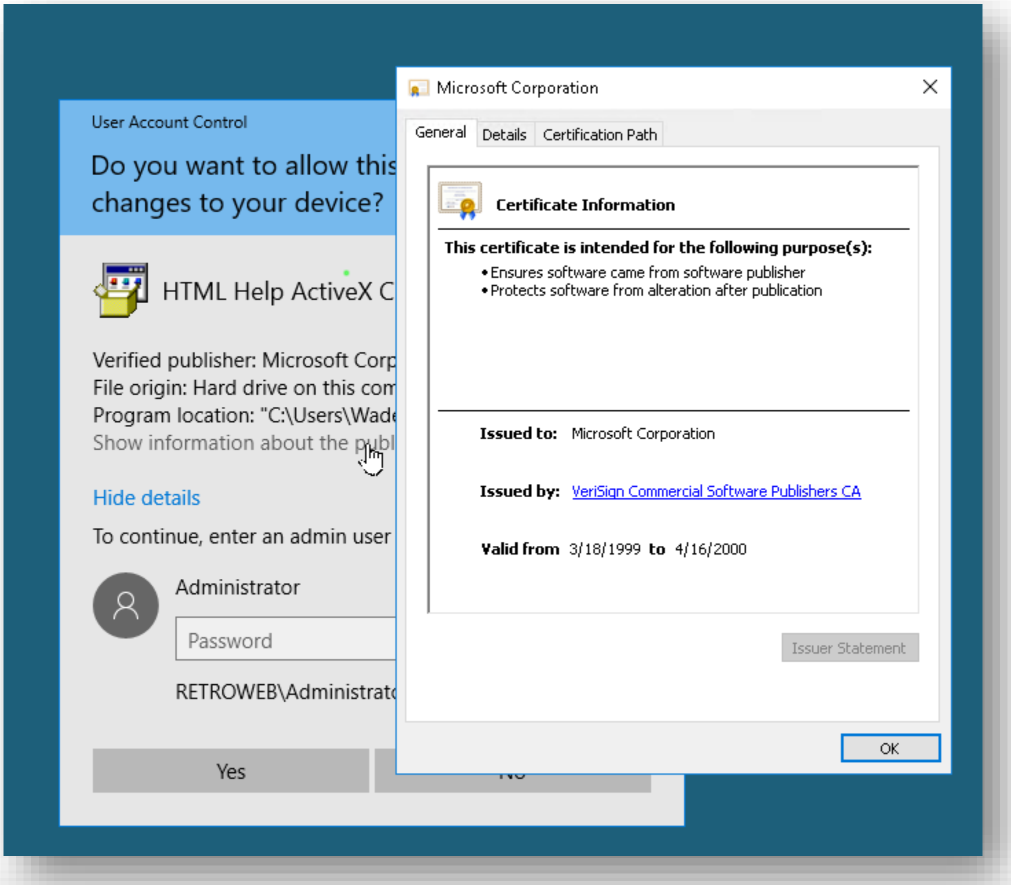
```
3b99fbdc6d430bfb51c72c651a261927
```

- On the desktop is user.txt and inside is the flag: 3b99fbdc6d430bfb51c72c651a261927

3. **[Optional] Elevate privileges and read the content of root.txt**
   - The hint says to check what the user was last doing on the computer; we see chrome on the desktop, lets see the users browser history
   - Looks like Wade was looking into a CVE-2019-1388 vulnerability; this allows escalation of privileges. A quick youtube search shows us how to exploit it:
   - https://www.youtube.com/watch?v=3BQKpPNlTSo



   - In the recycle bin is a binary; the same Microsoft-signed executable that was shown in the youtube video.
   - Once restored from the recycle bin, run as Admin, and the Windows UAC pops up asking for admin password
   - Root access in brower allows us to open a file-browser window and can access any file on the system



User Account Control

Do you want to allow this changes to your device?

HTML Help ActiveX C

Verified publisher: Microsoft Corp
File origin: Hard drive on this com
Program location: "C:\Users\Wade
Show information about the publ

Hide details

To continue, enter an admin user

Administrator

Password

RETROWEB\Administrat

Microsoft Corporation

Certificate Information

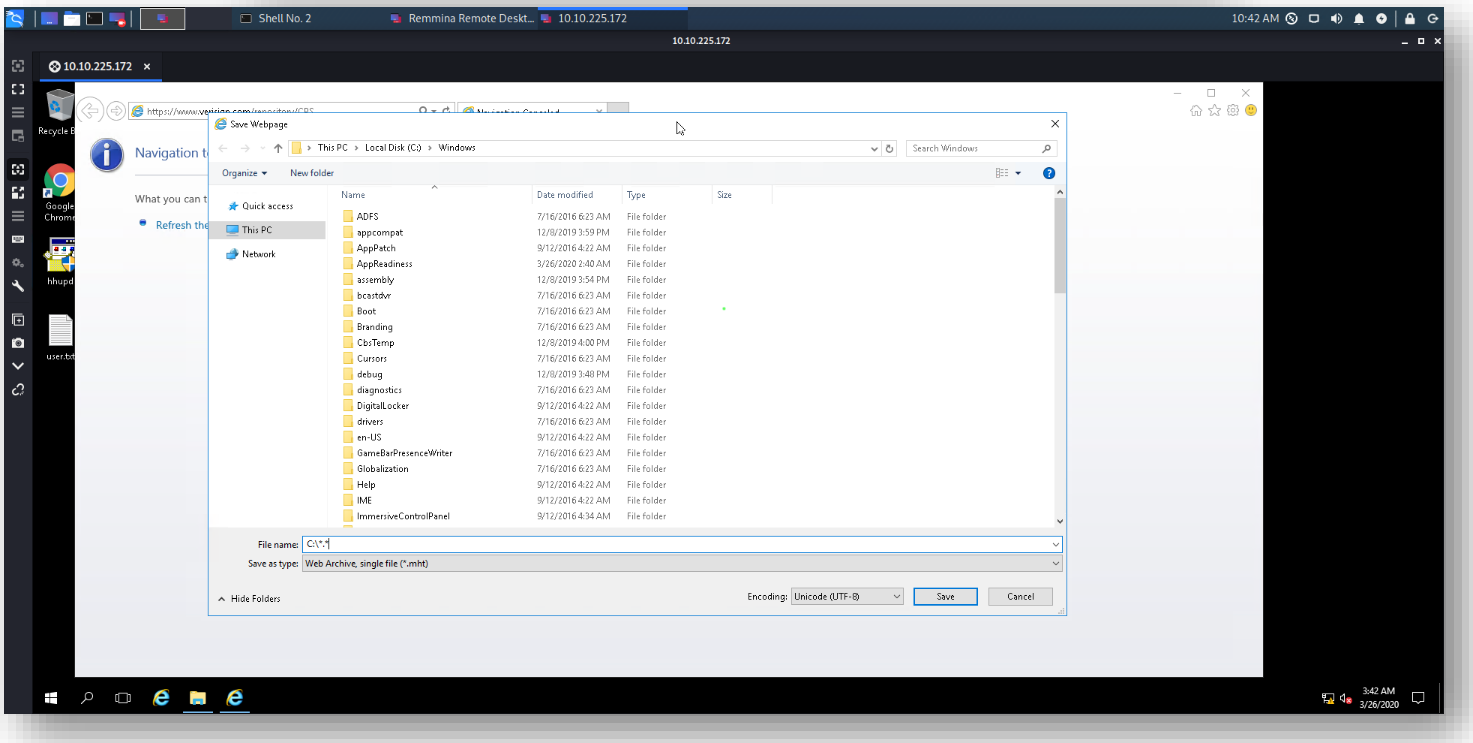
This certificate is intended for the following purpose(s):

- 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



Save Webpage

This PC › Local Disk (C:) › Windows

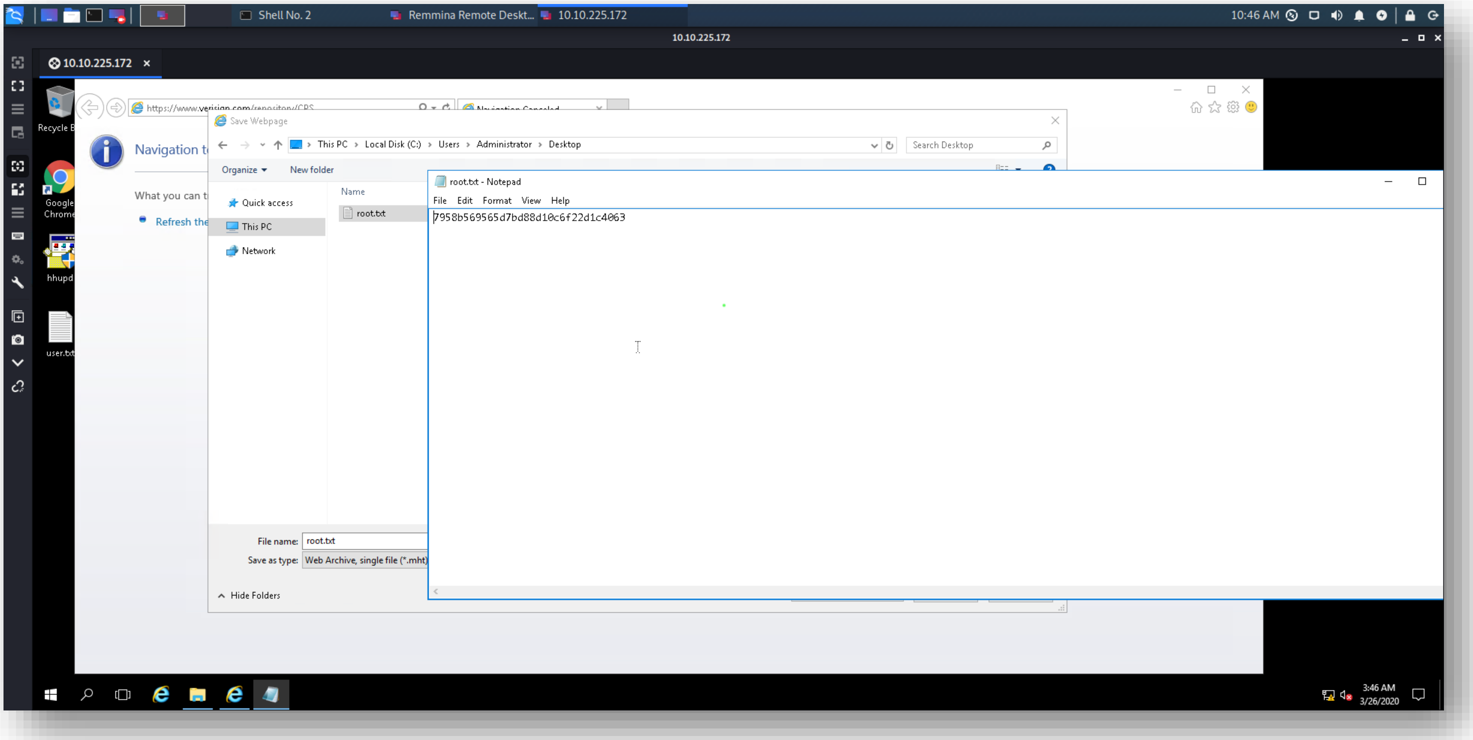
Name	Date modified	Type	Size
ADFS	7/16/2016 6:23 AM	File folder	
appcompat	12/8/2019 3:59 PM	File folder	
AppPatch	9/12/2016 4:22 AM	File folder	
AppReadiness	3/26/2020 2:40 AM	File folder	
assembly	12/8/2019 3:54 PM	File folder	
bcastdvr	7/16/2016 6:23 AM	File folder	
Boot	7/16/2016 6:23 AM	File folder	
Branding	7/16/2016 6:23 AM	File folder	
CbsTemp	12/8/2019 4:00 PM	File folder	
Cursors	7/16/2016 6:23 AM	File folder	
debug	12/8/2019 3:48 PM	File folder	
diagnostics	7/16/2016 6:23 AM	File folder	
DigitalLocker	9/12/2016 4:22 AM	File folder	
drivers	7/16/2016 6:23 AM	File folder	
en-US	9/12/2016 4:22 AM	File folder	
GameBarPresenceWriter	7/16/2016 6:23 AM	File folder	
Globalization	7/16/2016 6:23 AM	File folder	
Help	9/12/2016 4:22 AM	File folder	
IME	9/12/2016 4:22 AM	File folder	
ImmersiveControlPanel	9/12/2016 4:34 AM	File folder	

File name: C:\*.*

Save as type: Web Archive, single file (*.mht)

Encoding: Unicode (UTF-8)

- Save web page opens this file browser, can use ‘ *.* ‘ in a directory to see all files in the directory. From there, navigate to admin user folder and view the root.txt file
- The flag is 7958b569565d7bd88d10c6f22d1c4063

</br>

File name: root.txt

Save as type: Web Archive, single file (*.mht)

```
7958b569565d7bd88d10c6f22d1c4063
```