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.

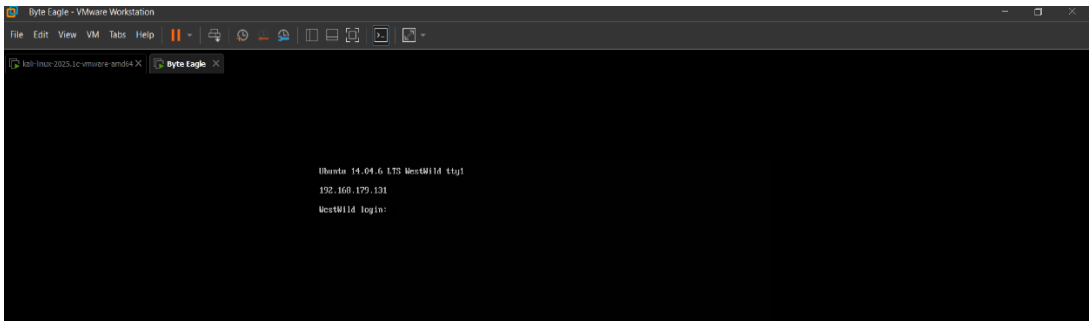
Byte Eagle CTF:

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.

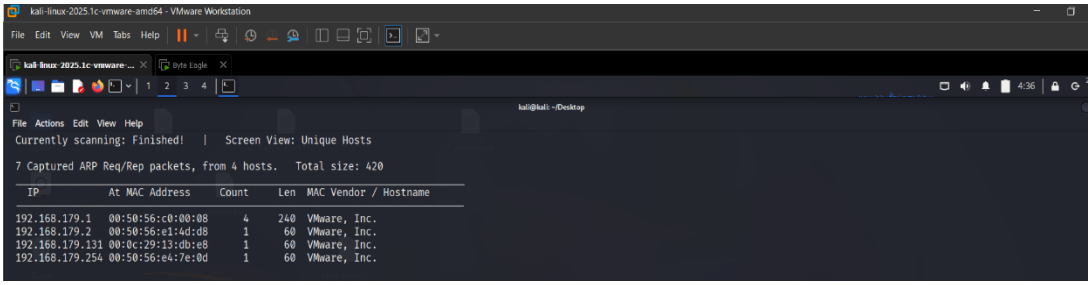
Tools and Methods used:

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

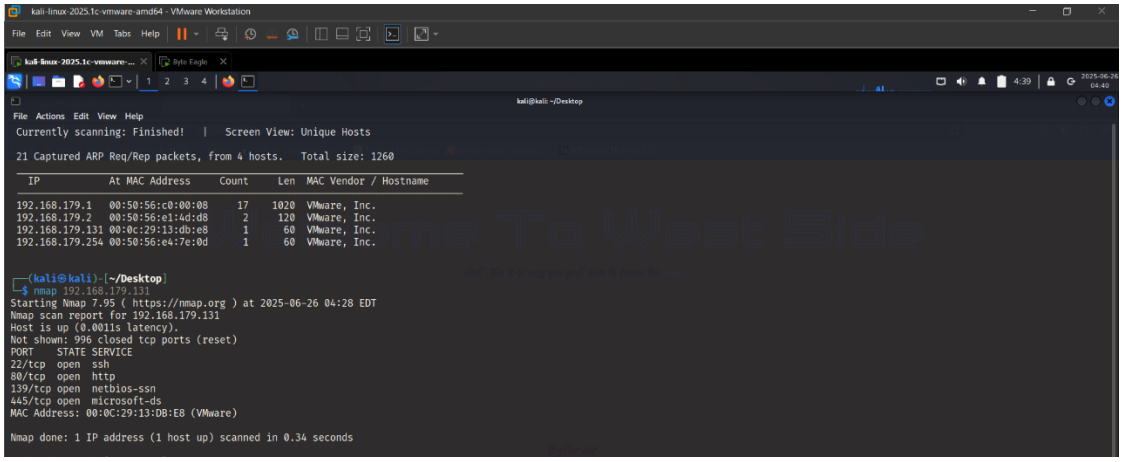
- Byte Eagle: Run the Byte Eagle machine and Kali Linux on your virtual machine (I used VMware work station).



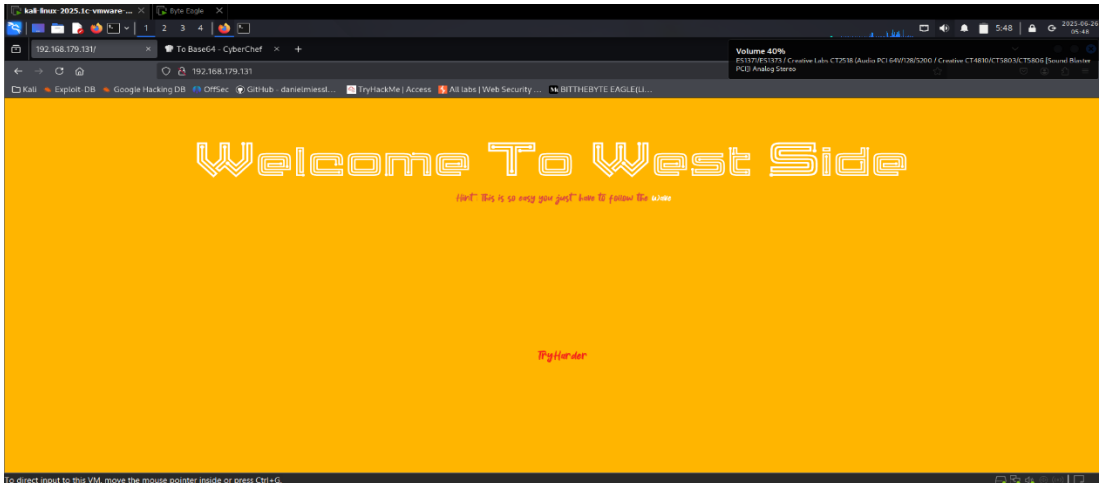
- Open terminal on kali linux and use the “netdiscover” command to scan the IP addresses and to identify your byte eagle IP address.



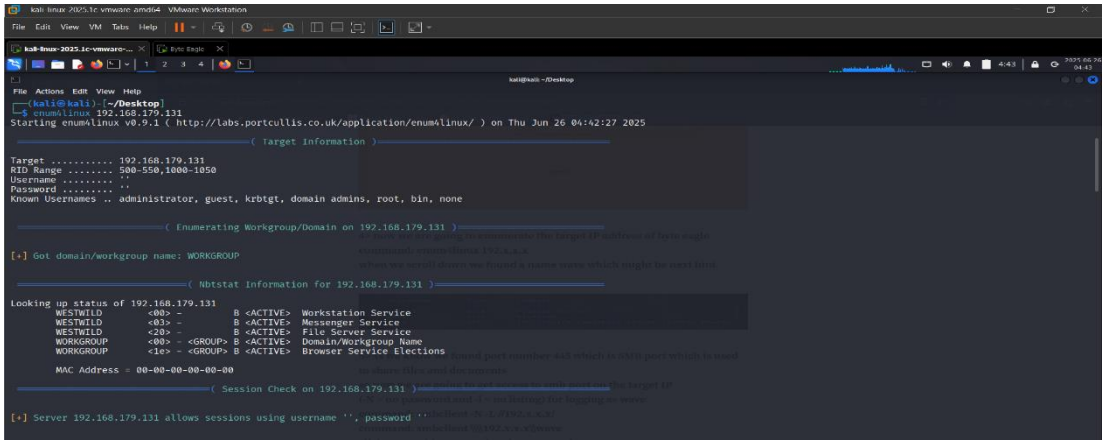
- Namp: Use the nmap command to check for the open ports. I discovered that there were four ports open (22, 80, 139, 445). This meant that the server was running a webserver which we could access using a browser.



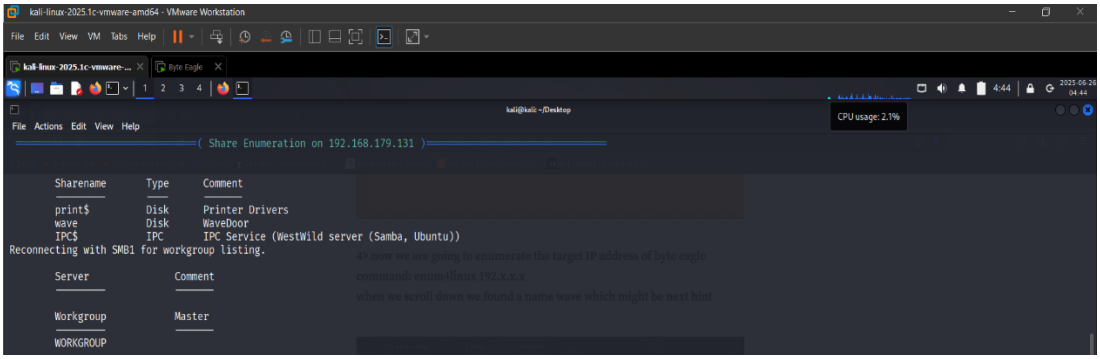
- Check the IP address on web browser so we can get to know any hint for CTF. We don't see any vulnerabilities but there is a hint saying "Hint: this is so easy you just have to follow the wave", keep a note of this hint.



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

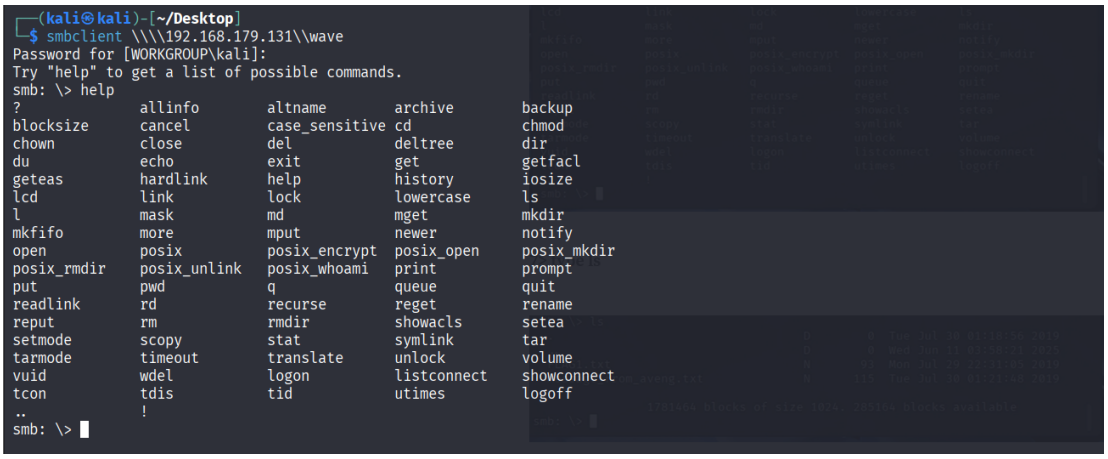


- When we scroll further, we find a wave name which might be our next hint (just like from the web browser hint).



- 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.

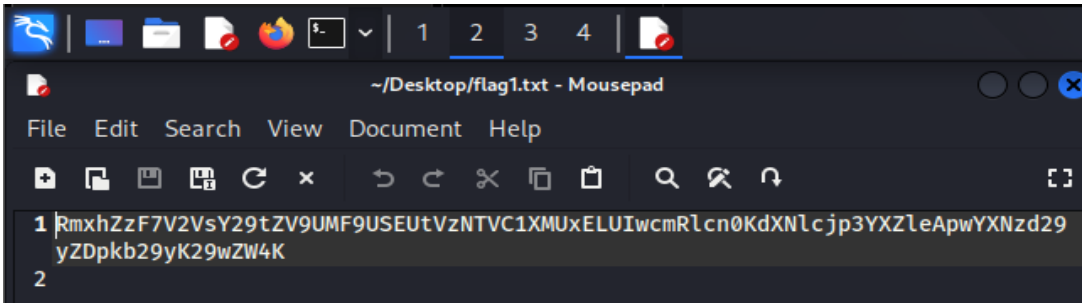


- Use the "help" command to get the list of all possible commands and use the "ls" command to list all the files

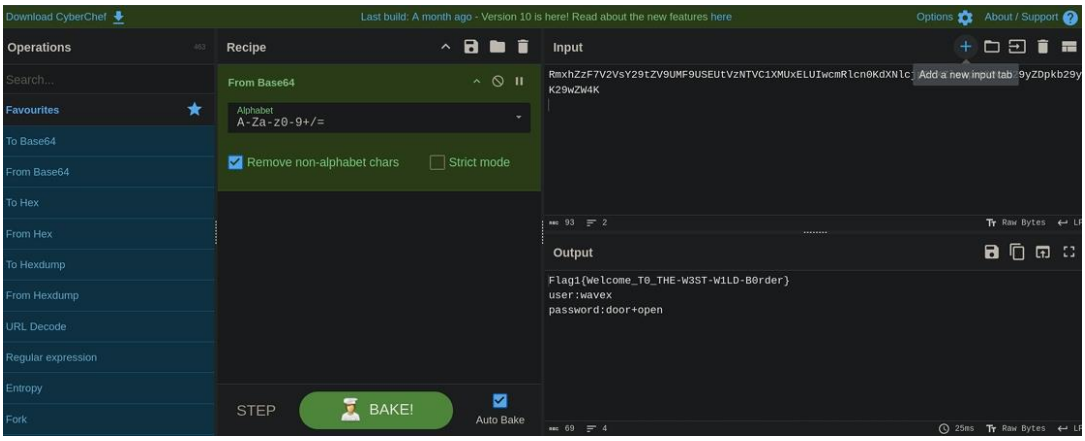
```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient \\\\192.168.179.131\\wave
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
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
  ..                                  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.

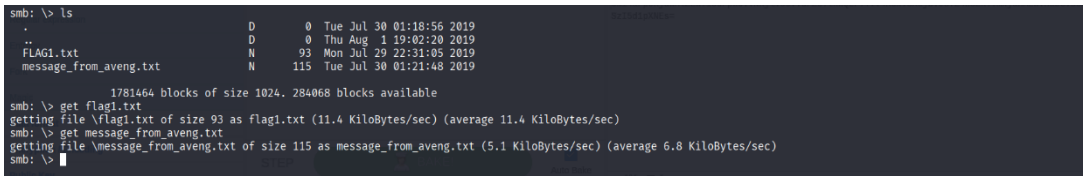


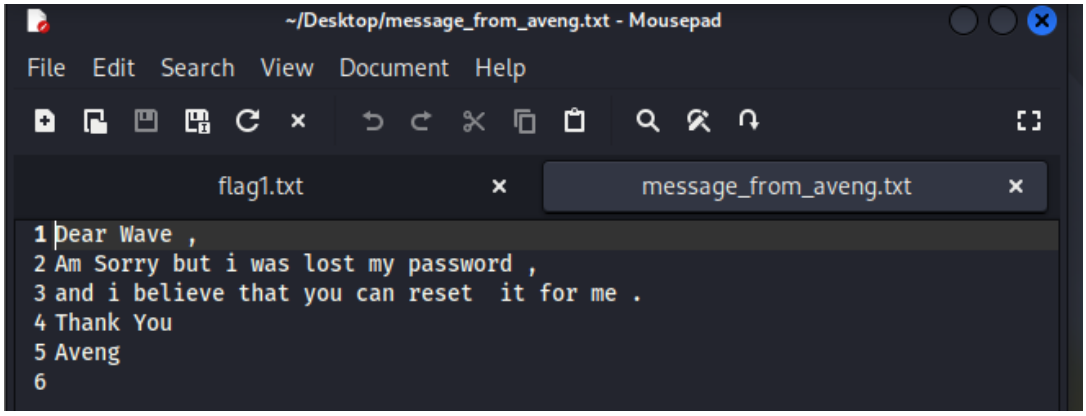
- Decode the data/information using "CyberChef" decoder and select "To Base64" option to convert binary data into text format.



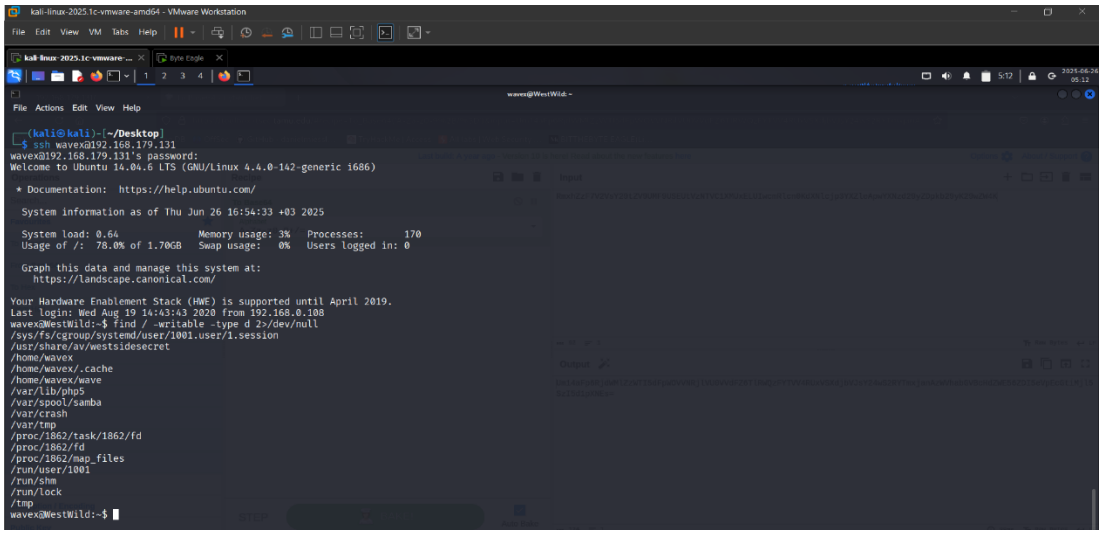
- Once the data is decoded, we get the username and password for one of the users.

- Now use the “get message_from_aveng.txt” command

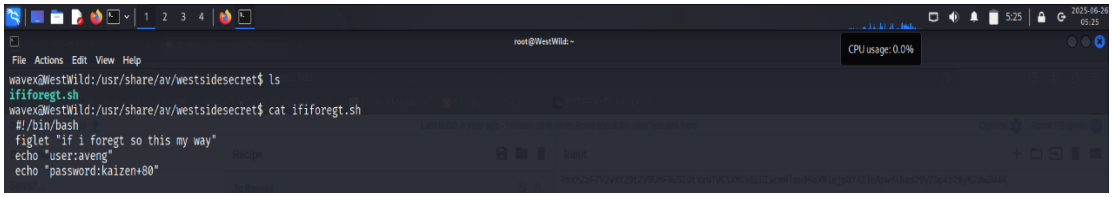




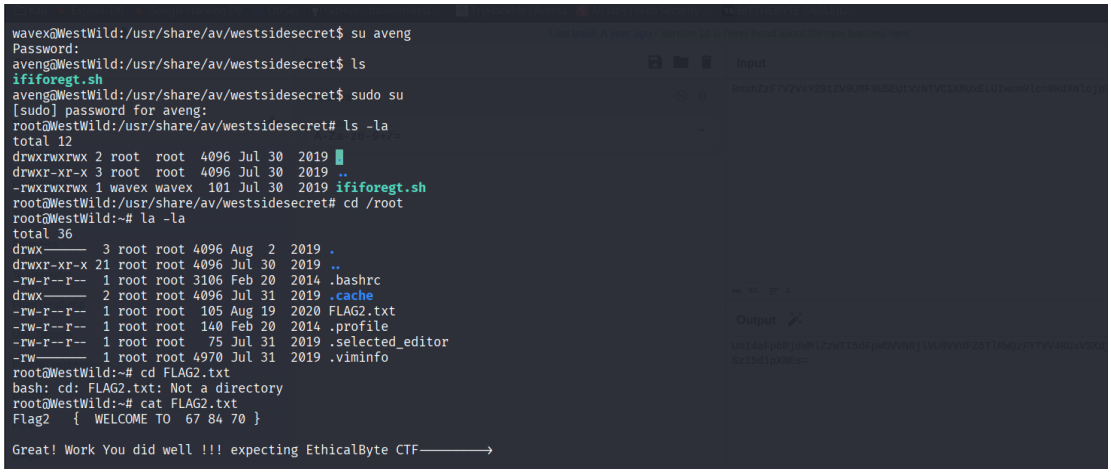
- As we can notice aveng has lost the password and wave has yet to reset it, so we now know the username and password of wave, hence we can login as a root user.
- Use the command “ssh wavex@192.168.179.131” and password “door+open” to login in place of wave as a root user.
- Write the command “find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



- We can see the westsidesecreat 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.



- 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”



- 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