CAPTURE THE FLAG – TEAM 16

STANLEY ONYEDIKA EPUNA
ID: 45731365

11TH April 2020

ABSTRACT

Capture the Flag (CTF) competitions allow students to learn cybersecurity skills in a fun and engaging way. It is an effective platform to increase students' interest in cybersecurity and prepare them for defending against real cyber attackers. A typical CTF competition requires at least some basic technical security knowledge and months of diligent preparation.

The primary goal is to teach students with little or no technical knowledge about the different cybersecurity challenges that a cybersecurity professional must address and the problem-solving skills needed for a cybersecurity career, all without direct use of technology.

INTRODUCTION

Capture the flag (CTF) task and competitions nowadays are well know events in various semi -professional cyber security fields. Everyone can demonstrate his or her skills in practical cyber security exercise. This CTF task deals with various practical aspect of information security. This CTF requires knowledge and experience with exploitation, using the terminal to perform exploitation task. These simulated real-life problems set an example for people to learn how to develop their selves in becoming penetration testers.

TEAM MEMBERS

1. **Stanley Onyedika Epuna**
2. **Divya Kaur**
3. **Sadiq Abuwala Mohammed**
4. **Ayush Wadhwa**
5. **Abishek Sobti**

CONNECTION

We were given the following to connect using the Secure Shell (SSH) remote login to get the CTF tasks

1. Username: Alice
2. Server Address: 10.46.255.208
3. Password: greensand34
4. Port Number: 22

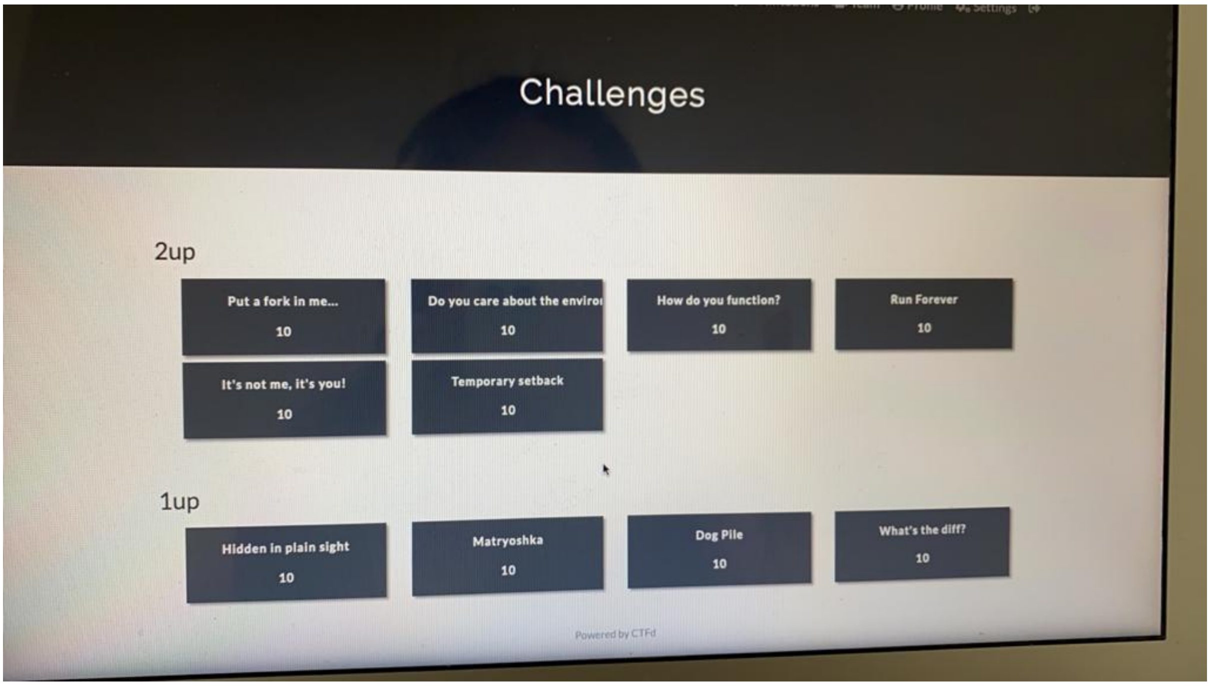
In this scenario we used Kali interface to remotely connect to the server

Using SSH

ssh: ssh user@remotehostip -p xxx
Alice – Username
10.46.255.208 – Remote Host Ip
-p 22 – Port number

for me to create a ssh command
type the following command in the terminal:

```
ssh alice@10.46.255.208 -p 22
```



FLAG 1 (Hidden in plain sight)

The goal of this level is for you to log into the CTF using SSH and find the flag 1. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the hidden plain text which is located at the dir directory. This task was gotten by Stanley Epuna.

Procedure:

Go into the terminal and type:

ssh alice@10.46.255.208 -p 22

password: **greensand34**

then it gets you into the server network using the ssh connection.

Type **ls -a** and it brings out the hidden files:

. .. .bash_logout .bashrc **.cache** .profile **dir1**

cd dir1 brings you to the dir1 folder

input ls -a in the terminal:

. .. .flag1.txt flag1.txt

So, the flags are in one of them.

Cat flag1.txt gives us the hidden in plain sight

FLAG 3 (Dog Pile)

The goal of this level is for you to log into the CTF using SSH and find the flag 3. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the hidden plain text.

Go into the terminal and type:

ssh alice@10.46.255.208 -p 22

password: **greensand34**

FLAG 4 (WHAT'S THE DIFFERENCE)

The goal of this level is for you to log into the CTF using SSH and find the flag 4. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the difference between two files namely, report.bak and report.txt. We the team researched and got the flag.

Go into the terminal and type:

```
ssh alice@10.46.255.208 -p 22
```

password: **greensand34**

then it gets you into the server network using the ssh connection.

Type **cd ..** and it gets you to your home folder

In the home folder type **ls -a** (which shows you all hidden files and folders)

So many files were brought out and I accessed all files and checked for the flag by.

Let's say the first file was **Alice** and to access it we use this command,

cat Alice and it gets us into the folder **Alice.**

To view the files in their input **ls -a** and the files are gotten

```
ls -a
.bash_logout .bashrc .profile
```

So, I did this for all the files to check for the report.bak and report.txt and I got the answer in the **Vanna** file.

```
ls -a
.bash_logout .bashrc .profile report.bak report.txt
```

So, we got the files report.bak and report.txt

To get the difference input:

```
diff report.bak report.txt
```

and the flag is gotten: **3f4b6d1effee1f1312a835e42a2d8aa9**

To ascertain academic integrity

Before we got to this answer, we already got the answer by someone in team 6 but it was a different imputation. We needed to do it ourselves not just getting the answers, so we dig more, and we found the answers ourselves.

FLAG 6 (Do you care about the environment)

The goal of this level is for you to log into the CTF using SSH and find the flag 6. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the flag 6. This flag was gotten by us the team members.

Go into the terminal and type:

```
ssh alice@10.46.255.208 -p 22
```

password: **greensand34**

then it gets you into the server network using the ssh connection.

To get the flag (Do you care about the environment)

We type in the terminal:

```
printenv
flag6 = c4852b99b00e35424685c1e9b41bce35
```

FLAG 8 (RUN FOREVER)

This goal is to get the flag 8 which is hidden in the current running process. This flag Go into the terminal:

ssh alice@10.46.255.208 -p 22

password: **greensand34**

it gets you into the host network

Type ls -a and all files are displayed including hidden files

The file we are looking for is in the etc dir

cd etc gets into the etc directory

so, we are now in the etc dir, now to access the current running process where the flag is located, input:

ps -aux (displays the current running process and their PID)

the flag 8 is visible with its password.

FLAG 9 (IT'S NOT ME, IT'S YOU)

The goal of this level is for you to log into the CTF using SSH and find the flag 9. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the flag 9. This flag was gotten by combined teamwork between we team members

Go into the terminal and type:

ssh alice@10.46.255.208 -p 22

password: **greensand34**

then it gets you into the server network using the ssh connection.

Type **cd ..** and it gets you to your home folder

In the home folder type **ls -a** (which shows you all hidden files and folders)

So many files were brought out and I accessed all files and checked for the flag by.

Let's say the first file was **Alice** and to access it we use this command,

cd Alice and it gets us into the folder **Alice.**

To view the files, input **ls -a** and the files are gotten

ls -a

.bash_logout .bashrc .profile

So, we tried all of the files and we got the one in **Michael's**

cd michael

ls -a

.bash_logout .bashrc .feline .profile flag9.txt

ls -al (show a long listing of all files in the current directory)

to get the flag, input:

./.feline flag9.txt

69f3c5c8b3fc08263dd200d2a4ce07ac

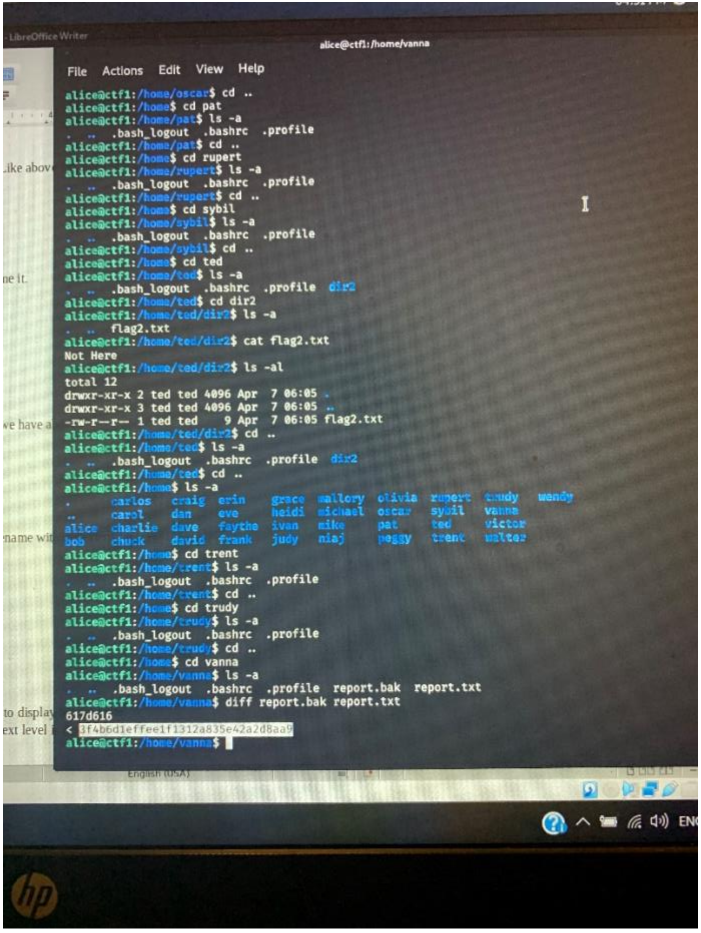
FLAG 10 (Temporary Setback)

The goal of this level is for you to log into the CTF using SSH and find the flag 10. The host to which you need to connect is 10.46.255.208, on port 22. The username is Alice and the password are greensand34. Once logged in, we need to find the flag 10.

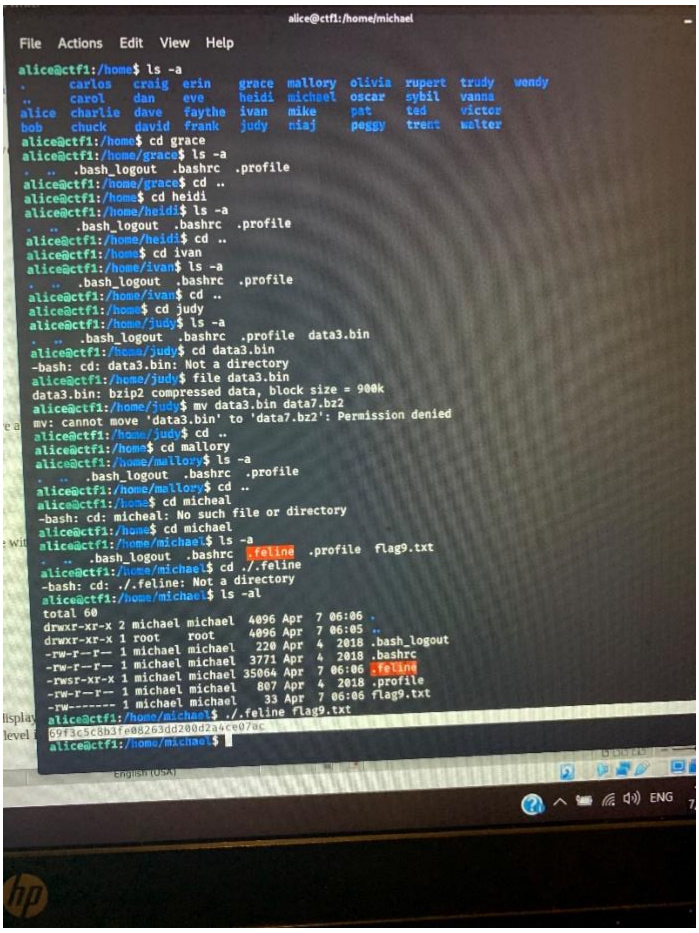
Go into the terminal and type:

ssh alice@10.46.255.208 -p 22
password: **greensand34**
then it gets you into the server network using the ssh connection.
Type **ls -a** and it gets you to hidden folders
In this scenario we need to get to the etc folder
So, we type
cd etc
and we arrive in the etc folder
where the flag is located is in the sudoers.d files
cat flag10 prints the output
the output revealed permission denied.
So, we tried to find the properties of the file flag 10 and the output was:
Flag 10 regular file, no read permission
we got stuck in there because we could not break the flag because of the privilege mode that the flag resides in. We tried copying the files to another folder, but it was not successful, also we even researched about sudoers.d online but all the steps we took didn't profit much.

To ascertain academic integrity
we got flag5, flag 8 and flag 9 from other team members but it was a different imputation. We needed to do it ourselves not just getting the answers, so we researched more as a group and got some of the flags on our own. Here is the screenshot of the one we got:



```
alice@ctf1:/home/oscar$ cd ..
alice@ctf1:/home$ cd pat
alice@ctf1:/home/pat$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/pat$ cd ..
alice@ctf1:/home$ cd rupert
alice@ctf1:/home/rupert$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/rupert$ cd ..
alice@ctf1:/home$ cd sybil
alice@ctf1:/home/sybil$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/sybil$ cd ..
alice@ctf1:/home$ cd ted
alice@ctf1:/home/ted$ ls -a
.  ..  .bash_logout  .bashrc  .profile  dir2
alice@ctf1:/home/ted$ cd dir2
alice@ctf1:/home/ted/dir2$ ls -a
.  ..  flag2.txt
alice@ctf1:/home/ted/dir2$ cat flag2.txt
Not Here
alice@ctf1:/home/ted/dir2$ ls -al
total 12
drwxr-xr-x 2 ted ted 4096 Apr  7 06:05 .
drwxr-xr-x 3 ted ted 4096 Apr  7 06:05 ..
-rw-r--r-- 1 ted ted    9 Apr  7 06:05 flag2.txt
alice@ctf1:/home/ted/dir2$ cd ..
alice@ctf1:/home/ted$ ls -a
.  ..  .bash_logout  .bashrc  .profile  dir2
alice@ctf1:/home/ted$ cd ..
alice@ctf1:/home$ ls -a
.      carlos   craig  erin    grace  mallory  olivia  rupert  trudy   wendy
..     carol    dan    eve     heidi  michael  oscar   sybil   vanna
alice  charlie  dave   faythe  ivan   mike     pat     ted     victor
bob    chuck    david  frank   judy   niaj     peggy   trent   walter
alice@ctf1:/home$ cd trent
alice@ctf1:/home/trent$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/trent$ cd ..
alice@ctf1:/home$ cd trudy
alice@ctf1:/home/trudy$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/trudy$ cd ..
alice@ctf1:/home$ cd vanna
alice@ctf1:/home/vanna$ ls -a
.  ..  .bash_logout  .bashrc  .profile  report.bak  report.txt
alice@ctf1:/home/vanna$ diff report.bak report.txt
617d616
< 3f4b6d1effee1f1312a835e42a2d8aa9
alice@ctf1:/home/vanna$
```



```
alice@ctf1:/home$ ls -a
.       carlos   craig  erin    grace  mallory  olivia  rupert  trudy   wendy
..      carol    dan    eve     heidi  michael  oscar   sybil   vanna
alice   charlie  dave   faythe  ivan   mike     pat     ted     victor
bob     chuck    david  frank   judy   niaj     peggy   trent   walter
alice@ctf1:/home$ cd grace
alice@ctf1:/home/grace$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/grace$ cd ..
alice@ctf1:/home$ cd heidi
alice@ctf1:/home/heidi$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/heidi$ cd ..
alice@ctf1:/home$ cd ivan
alice@ctf1:/home/ivan$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/ivan$ cd ..
alice@ctf1:/home$ cd judy
alice@ctf1:/home/judy$ ls -a
.  ..  .bash_logout  .bashrc  .profile  data3.bin
alice@ctf1:/home/judy$ cd data3.bin
-bash: cd: data3.bin: Not a directory
alice@ctf1:/home/judy$ file data3.bin
data3.bin: bzip2 compressed data, block size = 900k
alice@ctf1:/home/judy$ mv data3.bin data7.bz2
mv: cannot move 'data3.bin' to 'data7.bz2': Permission denied
alice@ctf1:/home/judy$ cd ..
alice@ctf1:/home$ cd mallory
alice@ctf1:/home/mallory$ ls -a
.  ..  .bash_logout  .bashrc  .profile
alice@ctf1:/home/mallory$ cd ..
alice@ctf1:/home$ cd micheal
-bash: cd: micheal: No such file or directory
alice@ctf1:/home$ cd michael
alice@ctf1:/home/michael$ ls -a
.  ..  .bash_logout  .bashrc  .feline  .profile  flag9.txt
alice@ctf1:/home/michael$ cd ./.feline
-bash: cd: ./.feline: Not a directory
alice@ctf1:/home/michael$ ls -al
total 60
drwxr-xr-x 2 michael michael  4096 Apr  7 06:06 .
drwxr-xr-x 1 root    root     4096 Apr  7 06:05 ..
-rw-r--r-- 1 michael michael   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 michael michael  3771 Apr  4  2018 .bashrc
-rwsr-xr-x 1 michael michael 35064 Apr  7 06:06 .feline
-rw-r--r-- 1 michael michael   807 Apr  4  2018 .profile
-rw------- 1 michael michael    33 Apr  7 06:06 flag9.txt
alice@ctf1:/home/michael$ ./.feline flag9.txt
69f3c5c8b3fe08263dd200d2a4ce07ac
alice@ctf1:/home/michael$
```

Summary

The CTF has been established as a potential tool in educating students about the cybersecurity field. This CTF activities dip students into realistic scenarios walking them through different cybersecurity career fields. During this challenge we were exposed to challenges and skills required for a cybersecurity expert. For example, this CTF challenge familiarizes students with Kali Linux operating system used for penetrating testing which we may use as we develop ourselves as cybersecurity professionals.

Our team where not able to get some of the flags and we failed to take some screenshots of the ones we did, but we are happy with the step we have taken to get some flags, with this we will be able to improve in other CTF task we are going to participate in the near future.