Findings for Capture the Flag (CTF) Exercise 1

Mohammed Sadiq Abuwala: 45921407

Team Number: 16

17 April 2020

Abstract

The capture the Flag (CTF) exercise is a security hacking game organized for COMP 6320 (Offensive Security). For the purpose of this particular exercise, we entered a Ubuntu (Linux) Server and we describe our experience and results here in detail.

Introduction

Hardware and Software used during the exercise:

Hardware:

Processor: Intel ® Core ™ i7-8550U CPU @ 1.80GHz

Installed memory (RAM): 8.00 GB

Primary Storage: 512GB SSD M.2 2280 PCIe NVMe

Note: Hardware specifications above may not be relevant as we are using a Virtual Machine (VM) as noted below.

Software:

Oracle virtual Machine running Kali Linux with following configuration:

System Base Memory (RAM): 2048MB

Processors: 2

Initially, at the start of the exercise, we were provided with the following credentials:

1. IP Address – **10.46.255.208**
2. Password – **greensand34**
3. Port number – **22**

We probe this IP address further to find further network properties like open ports by using the network scanning utility **nmap**. This confirms the above data that port 22 is open. There are no further open ports such as HTTP. Hence, we can now try connecting to the given system address by using the above credentials. Flags have been recorded below in the order that they were discovered by the individual.

Flag 1: Hidden in Plain Sight

With these above pieces information, we can power on our Virtual Machine (VM) running the Kali Linux shell and use the SSH command to connect to this server address :

- ssh alice@10.46.255.208 -p 22

At this point, the terminal will respond back asking for a password which we provide as – **greensand34**

On entering the password, we are now connected to the server. Firstly, we check what files and directories are available to us by using the **ls** command

- ls -a

The above command prints the available directories including hidden files as follows:

- . .. .bash_logout .bashrc .cache .profile dir1

Let us investigate what is inside the directory **dir1**

- cd dir1
- ls -a

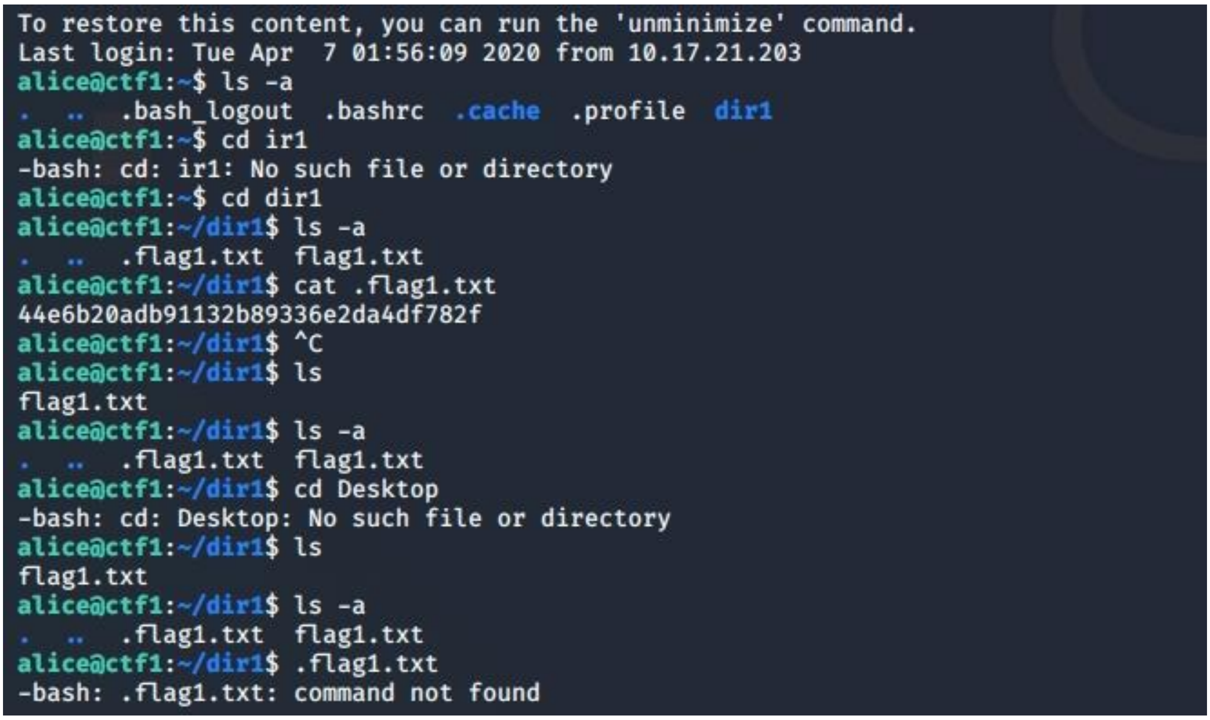
Upon investigating available directories in the folder **dir1**, we came across a text file called **flag1.txt** and another hidden file text file also called **flag1.txt**

- flag1.txt flag1.txt

Upon using the **cat** command to view the contents of both the above text files, we found that the code for flag 1 was stored in the hidden text file **flag1.txt**

- cat .flag1.txt
- 44e6b20ad91132b89336e2da4df782f

The corresponding screenshot image for the above workings is provided below:



```
To restore this content, you can run the 'unminimize' command.
Last login: Tue Apr  7 01:56:09 2020 from 10.17.21.203
alice@ctf1:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  .profile  dir1
alice@ctf1:~$ cd ir1
-bash: cd: ir1: No such file or directory
alice@ctf1:~$ cd dir1
alice@ctf1:~/dir1$ ls -a
.  ..  .flag1.txt  flag1.txt
alice@ctf1:~/dir1$ cat .flag1.txt
44e6b20adb91132b89336e2da4df782f
alice@ctf1:~/dir1$ ^C
alice@ctf1:~/dir1$ ls
flag1.txt
alice@ctf1:~/dir1$ ls -a
.  ..  .flag1.txt  flag1.txt
alice@ctf1:~/dir1$ cd Desktop
-bash: cd: Desktop: No such file or directory
alice@ctf1:~/dir1$ ls
flag1.txt
alice@ctf1:~/dir1$ ls -a
.  ..  .flag1.txt  flag1.txt
alice@ctf1:~/dir1$ .flag1.txt
-bash: .flag1.txt: command not found
```

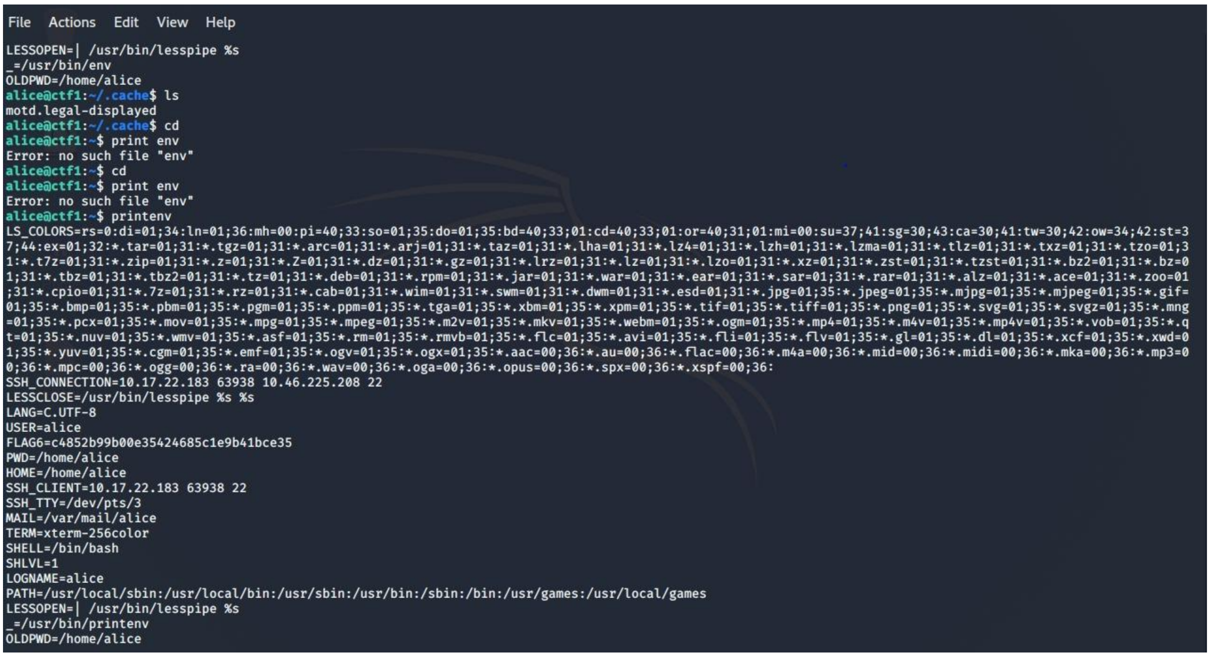
Flag 6: Do you care about the environment?

The name of the flag gives us the first clue. Let us try to find more information on the environment variables of this server. Once again, we use the Kali Linux shell command to type the following:

- printenv

The above command prints all the values of the environment variables set in the system. In the following output, we find another environment variable called **FLAG6** with the value **c4852b9900e35424685c1e9b41bce35**

The screenshot image for the above workings is provided below:



```
LESSOPEN=| /usr/bin/lesspipe %s
_=/usr/bin/env
OLDPWD=/home/alice
alice@ctf1:~/.cache$ ls
motd.legal-displayed
alice@ctf1:~/.cache$ cd
alice@ctf1:~$ print env
Error: no such file "env"
alice@ctf1:~$ cd
alice@ctf1:~$ print env
Error: no such file "env"
alice@ctf1:~$ printenv
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=3
7;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;3
1:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=0
1;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01
;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.esd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mjpg=01;35:*.mjpeg=01;35:*.gif=
01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng
=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.q
t=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=0
1;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=0
0;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
SSH_CONNECTION=10.17.22.183 63938 10.46.225.208 22
LESSCLOSE=/usr/bin/lesspipe %s %s
LANG=C.UTF-8
USER=alice
FLAG6=c4852b99b00e35424685c1e9b41bce35
PWD=/home/alice
HOME=/home/alice
SSH_CLIENT=10.17.22.183 63938 22
SSH_TTY=/dev/pts/3
MAIL=/var/mail/alice
TERM=xterm-256color
SHELL=/bin/bash
SHLVL=1
LOGNAME=alice
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
LESSOPEN=| /usr/bin/lesspipe %s
_=/usr/bin/printenv
OLDPWD=/home/alice
```

Flag 9: It’s not me It’s you

The above flag name gives us a hint that this particular flag could have something to do with user files. As the home directory serves as a repository for a user’s personal files, let us once again use the Kali Linux shell to input the following command:

```
cd  /home
```

The above command outputs a list of directories which consists of every user profile. Next, we navigate to the user profiles before coming across the user profile directory called **Michael**:

```
cd  Michael
ls  -a
```

The command line now goes to the user profile directory called **Michael** and then we use the **ls** command to see available directories in this folder. This outputs:

```
.  ..  .bash_logout   .bashrc   .feline   .profile   flag9.txt
```

In the above output, the files **.feline** and **flag9.txt** look interesting. Let us investigate further by long listing all the file properties of the files in this directory:

```
ls  -al
```

The above piece of code long lists all the file properties on the command line. On viewing the file properties, it comes to our attention that both the files **.feline** and **flag9.txt** were last modified at the same time. Finally, we input the following command:

```
./.feline flag9.txt
```

This reveals flag 9 and the following code is printed on the command line interface:

```
69f3c5c8b3f408263dd200d2a4ce07ac
```

Flag 10: Temporary Setback

During further investigation into available directories, we type the following command to see all available configuration files:

- cd /etc

The above command brings us into the directory called **etc.** Again, we use the **ls** command to see available directories in the **etc** folder:

- ls -a

The resultant output is that all available directories are printed out on the shell. Now, upon investigating the folders in the directory, we come upon a directory called **subdoers.d:**

- cd subdoers.d

Again, using the ls command to see available directories in the subdoers.d folder:

- ls -a

The following output is produced and this reveals flag 10:

- . .. README flag10

Like previous flags, we tried to open the file **flag10** by using the **cat** command:

- cat flag10

The above command prints the following output:

- cat: flag10: Permission denied

To investigate further, we have tried to find the properties of the file **flag10** to see what permissions are available:

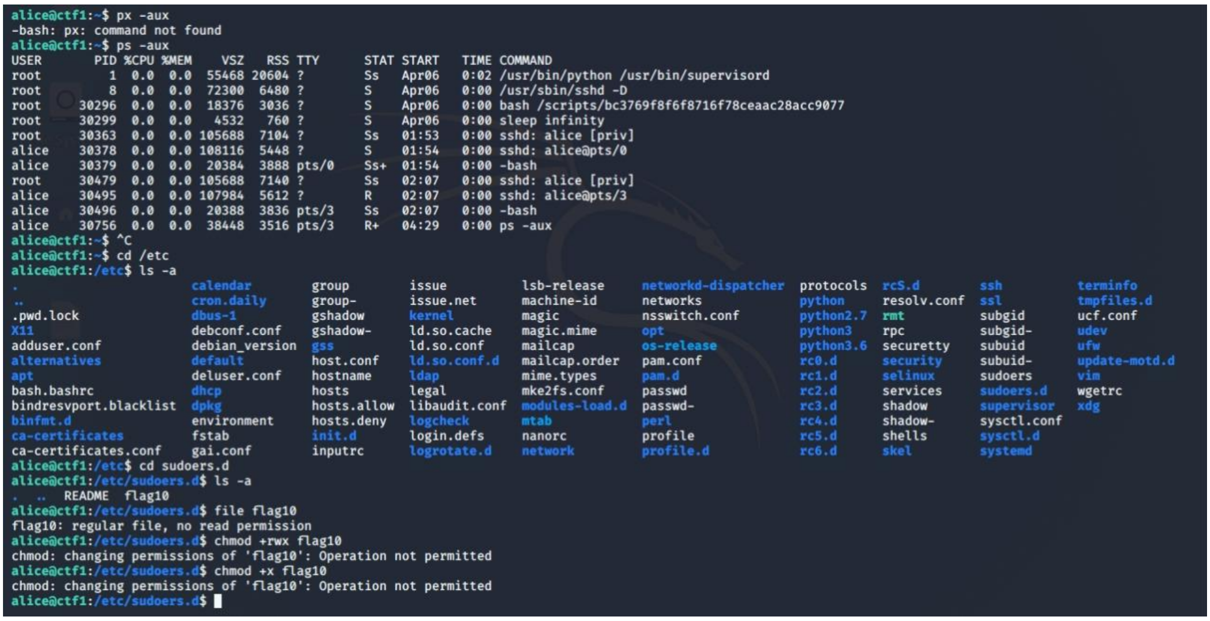
- file flag10

The above command prints the following output:

- flag10: regular file, no read permission

The above output reveals that we do not have read permission for the file flag10. To access this file, access privilege escalation might have been required but we were unable to generate any further outcome.

The screenshot image for the above workings of this flag is shown below:



```
alice@ctf1:~$ px -aux
-bash: px: command not found
alice@ctf1:~$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  55468 20604 ?        Ss   Apr06   0:02 /usr/bin/python /usr/bin/supervisord
root         8  0.0  0.0  72300  6480 ?        S    Apr06   0:00 /usr/sbin/sshd -D
root     30296  0.0  0.0  18376  3036 ?        S    Apr06   0:00 bash /scripts/bc3769f8f6f8716f78ceaac28acc9077
root     30299  0.0  0.0   4532   760 ?        S    Apr06   0:00 sleep infinity
root     30363  0.0  0.0 105688  7104 ?        Ss   01:53   0:00 sshd: alice [priv]
alice    30378  0.0  0.0 108116  5448 ?        S    01:54   0:00 sshd: alice@pts/0
alice    30379  0.0  0.0  20384  3888 pts/0    Ss+  01:54   0:00 -bash
root     30479  0.0  0.0 105688  7140 ?        Ss   02:07   0:00 sshd: alice [priv]
alice    30495  0.0  0.0 107984  5612 ?        R    02:07   0:00 sshd: alice@pts/3
alice    30496  0.0  0.0  20388  3836 pts/3    Ss   02:07   0:00 -bash
alice    30756  0.0  0.0  38448  3516 pts/3    R+   04:29   0:00 ps -aux
alice@ctf1:~$ ^C
alice@ctf1:~$ cd /etc
alice@ctf1:/etc$ ls -a
.                       calendar        group        issue          lsb-release     networkd-dispatcher  protocols  rcS.d        ssh          terminfo
..                      cron.daily      group-       issue.net      machine-id      networks             python     resolv.conf  ssl          tmpfiles.d
.pwd.lock               dbus-1          gshadow      kernel         magic           nsswitch.conf        python2.7  rmt          subgid       ucf.conf
X11                     debconf.conf    gshadow-     ld.so.cache    magic.mime      opt                  python3    rpc          subgid-      udev
adduser.conf            debian_version  gss          ld.so.conf     mailcap         os-release           python3.6  securetty    subuid       ufw
alternatives            default         host.conf    ld.so.conf.d   mailcap.order   pam.conf             rc0.d      security     subuid-      update-motd.d
apt                     deluser.conf    hostname     ldap           mime.types      pam.d                rc1.d      selinux      sudoers      vim
bash.bashrc             dhcp            hosts        legal          mke2fs.conf     passwd               rc2.d      services     sudoers.d    wgetrc
bindresvport.blacklist  dpkg            hosts.allow  libaudit.conf  modules-load.d  passwd-              rc3.d      shadow       supervisor   xdg
binfmt.d                environment     hosts.deny   logcheck       mtab            perl                 rc4.d      shadow-      sysctl.conf
ca-certificates         fstab           init.d       login.defs     nanorc          profile              rc5.d      shells       sysctl.d
ca-certificates.conf    gai.conf        inputrc      logrotate.d    network         profile.d            rc6.d      skel         systemd
alice@ctf1:/etc$ cd sudoers.d
alice@ctf1:/etc/sudoers.d$ ls -a
.  ..  README  flag10
alice@ctf1:/etc/sudoers.d$ file flag10
flag10: regular file, no read permission
alice@ctf1:/etc/sudoers.d$ chmod +rwx flag10
chmod: changing permissions of 'flag10': Operation not permitted
alice@ctf1:/etc/sudoers.d$ chmod +x flag10
chmod: changing permissions of 'flag10': Operation not permitted
alice@ctf1:/etc/sudoers.d$ █
```

Flag 4: What’s the difference

While investigating user profiles for flag 9, we also came across some interesting files in the directory **olivia**. We use the following command to navigate to this directory:

- cd olivia
- ls -a

the above command prints the files (including hidden files) in this directory:

- report.bak report.txt

The name of the flag provides us with a hint that flag 4 must be the difference between these two files. First, let us try to see if both **report.bak** and **report.txt** have the same file type by inputting the following command:

- file report.bak

This prints the following output:

- report.bak: ASCII text, with very long lines

Now, let us check the file type of report.txt:

- file report.txt

This prints the following output:

- report.bak: ASCII text, with very long lines

We can now confirm that both the files have the same file type. Hence, we can use the **diff** command to find the difference between the two files:

- diff report.bak report.txt

The above command prints the and output which is the result for flag 4.

Conclusion

While this exercise furthermore induced our interest in learning, it was challenging for our team as this was the first time that we had taken part in such a competition. Due to the adversarial nature of the field of cybersecurity, the real difficulty lies in outsmarting motivated individuals. The Capture the Flag (CTF) exercise was an interactive and interesting tool in enabling us to further our knowledge in testing systems. Additionally, the exercise helped us understand the concepts at a more practical level.

Disclaimer

Unfortunately, a few of my teammates have shared or received flags from other teams. Individually, I have not shared or received flags from any of the other team and have maintained all logs in the submitted journal. Additionally, screenshot images of individual workings have also been attached in this report if further examination is required.