Week 5 Journal – Offensive Security

RTFM

Time	**Who**	**Process**	**How (commands/notes/actions taken)**	**Outcome (what happened as a result)**
18/08/24 5:10	Samip	Gain access to the challenge and the linux environment	Login to Scoreboard url: https://offsec.site/ctf1/ to gain access to challenge Login to Web kali desktop portal: https://offsec.site/kali/ to gain access to virtual linux environment Using credential Provided	Gain access to the linux server

5:30	Samip	Read the challenge and access the challenge using telnet Installed telnet Login to RTFM challenge using telnet	Choose the challenge “RTFM” Sudo apt install telnet telnet 10.55.1.10	Login to the server 10.55.1.10 where the “RTFM” is located using guest.
5:40	Samip	Learned more about the challenge	Ls -la Googled the title of the challenge “RTFM” And the hint given	RTFM meant “Read the fuicking manual” Could not find anything about the hint

5:50	Samip	Searched for linux manual	Googled the command for linux manual guest@flag01: ~$ help guest@flag01: ~$ man guest@flag01: ~$ man man	Learned about man command Learned there is manual for different studd in linux which can be accessed through man command
6:00	Samip	Tried various man command with different options and keywords	guest@flag01: ~$ man ls guest@flag01: ~$ man man guest@flag01: ~$ man pages guest@flag01: ~$ man flag guest@flag01: ~$ man -k flag NAME flag - false flag	Got access to a man flag page which was filled with with filler text in latin. Relaized it was a custom man page and it was a step forward toward finding the flag Scrolled to th bottom of the page but could not fing anything

			SYNOPSIS flag DESCRIPTION flag Lore	
6:20	Samip	Tried various other man command and other command to find the flag	18 man man 19 man-pages (7) 20 man flag 21 man flag(2) 22 man flag (2) 23 man flag 2 24 man flag 25 ls -la	Could not get any closer to finding the flag. So decided to revisit the man flag page.

			26 cd .profile 27 ls\ 28 ls 29 cat .bash_logout 30 cat .bashrc 31 ls 32 ls -la 33 cat .profile 34 ls 35 ls -la 36 cat .lesshst 37 cd .cache/ 38 ls\ 39 ls 40 exit 41 cd .. 42 ls	

			43 readme 44 help 45 history 46 help name 47 help flag 48 help help 49 man -k flag 50 man flag 51 daylight 52 man daylight 53 exit 54 man man 55 man flag 56 man based 57 man base And other various commands	

6:30	Samip	Revisited man flag page and anlyzed the page more carefully	guest@flag01: ~$man flag Scrolled to the middle of man flag page and found the following: OPTIONS MZQWY43FEBTGYYLH SEE ALSO flag(1) offsec(7) rtfm(8) Entered the “MZQWY43FEBTGYYLH” as flag	Flag was incorrect But another hint Found Check the offsec and rtfm page also

6:40	Samip	Vist the man offsec and man rtfm page	guest@flag01: ~$man offsec Scorlled to the middle of the page and found this: OPTIONS MZQWY43FEBTGYYLH SEE ALSO flag(1) ctf(6) rtfm(8) This doesnot seem like it guest@flag01:~$ man rtfm OPTIONS MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2=== SEE ALSO flag(1) ctf(6) offsec(7) The “MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2===” seems like the	Entered “MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2===” as the flag It was incorrect. The string seems to be encoded.

			flag	
6:50	Samip	Decode the string to get the flag	echo "MZWGCZ33GVTGEZRVMUZTQNTGG44DMNJRMQYTAZRRHFSTINJWGEZTSYJWGQZX2===" | base32 --decode flag{5fbf5e386f78651d10f19e456139a643} Found the flag “5fbf5e386f78651d10f19e456139a643”	Entered the flag “5fbf5e386f78651d10f19e456139a643” Correct flag Challenge Completed

Spartan

Time	**Who**	**Process**	**How (commands/notes/actions taken)**	**Outcome (what happened as a result)**
August 21st, 6:58:41 PM	Ayush	Trying to find the CTF for sunlight part called spartan	Opened Link https://offsec.site/ctf1/challenges#Gone%20fishin'-7 through iLearn for CTF 1 Opened link https://offsec.site/kali/ through iLearn for Web kali desktop portal Logged in with given credentials Opened Terminal Emulator on Kali web Saw the challenges on Sunlight zone and chose “Spartan” It shows “telnet to 10.x.1.40 where x is your team number” Went to web kali and typed telnet 10.55.1.40 as 55 is our team number Shows telnet not found	Got flag : flag{f5052eab8924bff54b1a1b82dcd28cb4}

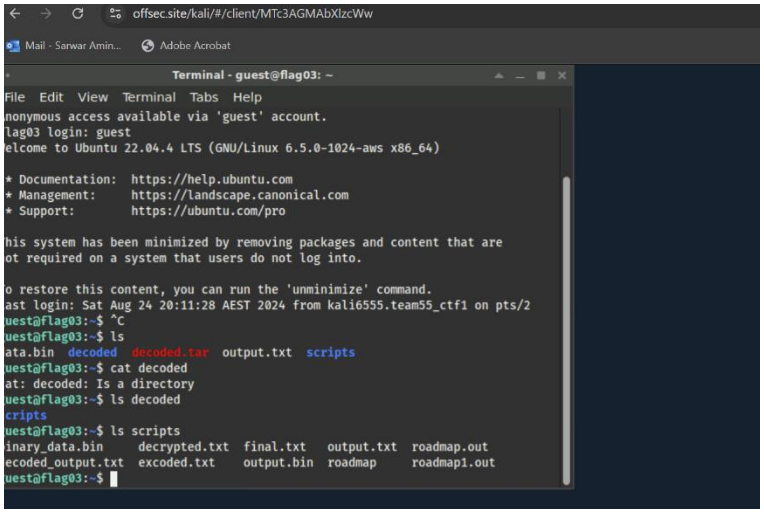
			So I have to install telnet first with the command “sudo apt install telnet” and installed telnet In terminal typed “telnet 10.55.1.20” then I got asked for flag2 login and I login as a guest. Typed csh then bash got “1% Reset tty pgrp from 1077 to 1074” Again typed csh got got “2%” then typed bash Then lastly typed csh again and got “3%” and now I typed flag and got “ZmxhZ3tmNTA1MmVhYjg5MjRiZmY1NGIxYTFiODJkY2QyOGNiNH0K” Then I used base 64 to decode this text. I typed “echo ZmxhZ3tmNTA1MmVhYjg5MjRiZmY1NGIxYTFiODJkY2QyOGNiNH0K | base64 –d”	

August 22-24	Ayush	Trying to find other CTFs which are not done	Tried everything to find the ctf but could not get it.	No result found

CTF1- Yousra Mehrin, Student ID: 48638218

Mirror Maze

Time	**Who**	**Process**	**How (commands/notes/actions taken)**	**Outcome (what happened as a result)**

19:30	*YM	For the CTF 1 challenges, I tried the problem called “Mirror Maze”. My first step was to login to the telnet server with respect to my team number as a replacement of x.	In the terminal I entered the following commands to connect to the telnet server. telnet 10.55.1.30 Then I logged in to the guest account using the password: guest.	I could successfully login to the guest account in the telnet server.
19:34	*YM	I entered command for listing all the files and directories and explored options to see where I can find the specific flag for this task.	I used the ls command to view all the files and directories. I found a few directories and files. I then used these commands to explore the possible files that could contain the flag for the given task. The commands I used are shown in the screenshot below: 	I found a directory named “decoded”. When I entered that directory, I was forwarded to a “scripts” directory. And once I entered the directory, I found multiple text files which could contain the flag I was looking for.

```
offsec.site/kali/#/client/MTc3AGMAbXlzcWw
Terminal - guest@flag03: ~
nonymous access available via 'guest' account.
lag03 login: guest
elcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1024-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

his system has been minimized by removing packages and content that are
ot required on a system that users do not log into.

o restore this content, you can run the 'unminimize' command.
ast login: Sat Aug 24 20:11:28 AEST 2024 from kali6555.team55_ctf1 on pts/2
uest@flag03:~$ ^C
uest@flag03:~$ ls
ata.bin  decoded  decoded.tar  output.txt  scripts
uest@flag03:~$ cat decoded
at: decoded: Is a directory
uest@flag03:~$ ls decoded
cripts
uest@flag03:~$ ls scripts
inary_data.bin     decrypted.txt  final.txt   output.txt  roadmap.out
ecoded_output.txt  excoded.txt    output.bin  roadmap     roadmap1.out
uest@flag03:~$
```

19:45	*YM	I found a file named decoded.tar which needed to be decoded. I tried to find out necessary commands to get access to this tar file.	I entered the following command in the terminal to decode the tar file: tar -xvf decoded.tar	It displayed a directory named: scripts/roadmap
19:58	*YM	I explored the "scripts" directory using various commands to find the relevant files containing the flag.	Previously I used ls script command as shown in the snippet above to explore the necessary files and the directory. I used that again and found roadmap.out file. I used the following command to learn detail about the file type: file scripts.roadmap.out	The mentioned command gave the following output: scripts/roadmap.out: ASCII text I tried to decompress the bzip2 file by using the command: bunzip2 scripts/roadmap However, the output showed that the scripts/roadmap.out already exists in the terminal.

20:20	*YM	Since I figured out that the roadmap.out file in the script directory contains the flag we are looking for, I used various commands to find the output content.	At first, I used the cat scripts/roadmap.out command but found a huge file containing various ASCII codes. After that, I used the following command to find the particular content in the big file. grep "CTF{" scripts/roadmap.out	Even after trying to find a specific command in the huge file content, there was no display found. Hence, after rigorous attempts, I was unable to find the required flag for the task

CTF1 (**Gone fishin'**) – Chisthia Khan (48728470)

Time	**Who**	**Process**	**How (commands/notes/actions taken)**	**Outcome (what happened as a result)**

August 22, 10:25	Chisthia	Trying to login as guest in the Linux terminal for **Gone fishin’**	Wrote telnet command and pressed enter. A login module appeared where after entering guest it logged in as guest@flag04 telnet 10.55.1.40 here 55 is the group number assigned to us.	Logged in as a guest user.
August 22, 12:05	Chisthia	Trying to locate clue about the flag	wrote ls -la to see all the file under /home/guest. A script file named copyfile.sh was located which after opening with cat copyfile.sh command showed a code snippet.	Analyzed code showed the way to locate the flag file.

August 22, 14:44	Chisthia	Trying to locate the flag file	Copied the code from copyfile.sh and create a new.sh file using below commands: Touch new.sh And populated the copied code in here using below command for text inputting prompt: nano new.sh Cntrl + O Enter Cntrl + X After that, created a file named request under /tmp and ran the modified commands. ./new.sh sh new.sh	The location of the flag was written in the request file: /home/eve/flag.txt
August 22, 17:50	Chisthia	Trying to read the flag.txt file to find out the flag	First, checked the permission using the below command, ls -l /home/eve/flag.txt it showed no permission for guest user: -rw-------	Used all means, AI, online document but could not extract the flag.

			Then, tried to run the script file meeting all the condition but failed to extract the flag from flag.txt since no read permission were given to the guest user.	