ACM

WRITE UP FOR S3 CYBER WEEK 1
NAME: B RAJMOHITH REDDY
BRANCH: CYBER SECURITY
SIG: CYBER

1. FOUNDATIONAL TASKS -1
MACHINE: HACKTHEBOX – CAP
OBJECTIVE: COMPROMISE THE VULNERABLE CAP SERVER AND RETRIEVE THE USER FLAG.

Recon statergy:

I began the challenge by running a network mapping using:

Cmd: “nmap 10.10.10.245 -sC -sV -oA initial-recon -Pn”.

This revealed the no of ports that are open, they are ftp,ssh and http which should in open state (ports 21,22,80).

Using these 3, first I used ftp and tried an anonymous login which was unsuccessful.

- so later on, moved to port 80 i.e http i.e http://10.10.10.245.
- That consists of a page with some data and some user name like Nathan ....

- The something will be found and that ins the the next answer.
- Verify for the other possible values like 0,1,2,3,4,5 etc…
- And download the files and that gives the wireshark captures so make a analysis so that we can find the user name and password.
- Login using ftp “ftp 10.10.10.245” no flag will be found.
- Now use ssh to access Nathan’s shell.” Ssh nathan@10.10.10.245.”
- After login use “ls-la” to find the list of all files.
- And “ cat user.txt”.there you can find the flag

2. Foundational Tasks -1

MACHINE: tryhackme -brute it

OBJECTIVE: crack SSH login credentials through brute force and capture the flag

3. FORENSIC TASKS:

1.CTFlearn (challenge 96):forensic 101

Tools needed:strings

i)download the file from the link given in the question .

ii) now use strings <filename> > strings output.txt

iii) then use cat <filename.txt> to get the flag.

iv) final flag is “flag{wow!_data_is_cool}”

2.CTFlearn(challenge 138) corrupted file

Tools required: ghex and base 64 decoder

i) download the file from link in the question.
ii) Now using ghex get the files base 64 representation.
iii) Insert the header of GIF8 infront of 9a in the ascii representation.
iv) Now open the image we will get the flag in th base 64 code from the gif that needs to reduce the spped of playing.
v) Decode that using base 64 decoder.
vi) Final flag: flag{g1f_or_j1f).

3.CTFlearn(challenge 104) Git is Good

Tools used: git log -p and ls

i)unzip the zip file using “unzip <file name>

ii) explore all the list of files found through ls -la

find the flag in the git files.

iii)final flag: flag{protect_your_git}

4.CTFlearn: Milk's Best Friend

Tools used: Strings ,binwalk

i) Use binwalk to extract all the files and explore all the files .
ii) Use strings command "strings <filename>" to find the flag.
iii) final flag: flag{eat_more_oreos}

5.CTFlearn : 07601

Tools needed:Strings and binwalk

i)use the command strings we will find nothing and now extract the files using binwalk command"binwalk -e <file name>

ii) explore all the files using strings so that we will find the output flag.

iv)final flag : ABCTF{Du$t1nS_D0jo}1

6.CTFlearn: glory of the garden

Tool needed: strings

i)use the command “strings <file name>”

ii) you will see the output.

iii) the flag is “flag{more_than_m33ts_the_3y3657BaB2C}”

7.picoCTF: m00n walk

Tools required: qsstv pactl,pavucontrol

i)first listen to the audio file so that you may find the flag.

ii) now on researching all the tools I got to know about qsstv and pactl.

iii)use these commands

- qsttv
- pactl load-module module-null-sink sink_name=virtual-cable
- pavucontrol
- paplay -d virtual-cable main.wav

iv) now we will get an image so that it will be in the inverted form so now read the flag.

v) the final flag is: picoCTF {beep_boop_im_in_space}

8.picoCTF: Surfing the Waves

Tools required: hexa decimal decoder,python 3 (scipy.io)

i) open python 3

ii) enter the given below code:

```
from scipy.io import wavfile
file_object=open('coba.txt','a')
samplerate,data=wavfile.read('main.wav') for i in
data: r=(i-1000)//500 file_object.write(hex(r)[2:])
file_object.close()
```

we will get an array of data

iii)we will get the data and convert that to ascii form we will get the required flag.

iv)final flag: picoCTF{mU21C_1s_1337_b040e2da}

9.picoCTF: Matryoshka doll

Tools required: binwalk

i) use binwalk -e <file name> and re locate to the location accordingly and we will use this for four times.

ii) so that at the fourth file we will find a .txt file to get the flag.

iii) Final flag: picoCTF{336cf6d51c9d9774fd37196c1d7320ff}

10.picoCTF: tunn3l v1s10n

Tools required: ghex,exiftool

i)find the nature of the file as it is given as .unknown using exiftool.

ii) now according convert the type of the file as the extension changes.

iii)change the dimensions from 32 01 to 32 03. And open the image through file manager.

iv)final flag: picoCTF {qu1t3_a_v13w_2020}.

11.picoCTF: can you see

Tools required: exiftool and base64 decoder

i) Find the file that was downloaded from the question.

ii) Use exiftool to find the complete indepth data about the file.

iii) And we will find a code of base 64 now decode it.

iv) Final flag: picoCTF{ME74D47A_HIDD3N_a6df8db8}