CyberSec Recruitment Tasks – Week 1 Release

- G.YESHWANTHI REDDY(CYS)

2. Forensics Track

1) CTFlearn – Forensics101

- **Tools used –** Strings
- **Process –** firsly downloaded the file
  Run the command **strings 95f6edfb66ef42d774a5a34581f19052.jpg |grep "flag"**
  Here string is used to find any readable text that image and grep is used to Find a text with "flag"
- **Flag –** After the cmd is excuted I obtained the flag **flag{wow!_data_is_cool}**

2)CTFlearn – Corrupted File

- **Tools used – Hxd,strings**
- **Process –** firstly downloaded the file and open it was empty
  Then opened the file in Hxd(hex editor- used to edit any hex values are Corrupted).
  As it is GIF the hex values should be **47 49 46 38 39 61(GIF89a)** but it wasn't.
  Now changed the first bits to **47 49 46 38 39 61** and saved the file
  Run the cmd **strings unopenable.jpg |grep "flag"**
- **Flag –** After the cmd is excuted the flag obtained was **flag{g1f_or_j1f}**

3)CTFlearn -Git is Good

- **Tools used – git,linux**
- **Process –** downloaded the git from url
  Cloned the repository and checked log history by **git log**, then used **git show** to find any changes .
- **Flag –** flag obtained was **flag{protect_your_git}**

4)CTFlearn – Milks best friend

- **Tools used –** strings
- **Process –** downloaded the file from given url
  Run the cmd **strings oreo.jpg |grep "flag"** to find any hidden text
- **Flag –** after the cmd was excuted the flag obtained was **flag{eat_more_oreos}**

5)CTFlearn – 07601

- **Tools used –** binwalk,strings
- **Process –** firstly downloaded the file then run the **binwalk AGT.png** to find any hidden Files , Now extacted the file with cmd binwalk -e file_name
  Now used stings cmd **strings I\ warned\ you.jpeg** (as I warned you is secret File extracted)
- **Flag** - after the cmd was excuted the flag obtained was **ABCTF{Du$t1nS_d0jo}**

6)PicoCTF- Glory Of The Garden

- **Tools used –** Text editor(notepad)
- **Process –** downloaded the garden.jpg file then opened with notepad to find readable Text
- **Flag –** at the end of notepad I found the flag as **"picoCTF{more_than_m33ts_the_3y33dd2eEF5}"**

7)PicoCTF -m00nwalk

- **Tools used –** sstv,strings
- **Process –** firstly installed sstv then downloaded the audio mesaage.
  Run the command **sstv -d message.wav** to find any hidden images in audio
  Now run the command **strings result.png** to find hidden text in this file(as Result.png is hidden file found in sstv)
- **Flag -** after the string cmd excuted the flag obtained was **picoCTF{beep_boop_im_in_space}**

8)PicoCTF -Surfing the waves

I tried a lot but could'nt find the flag

9)PicoCTF - Matryoshka doll

- **Tools used –** binwalk
- **Process –** run **binwalk dolls.jpg** to search any hidden files within the image
  We obtain a zip archive so we need to unzip it by **unzip dolls.jpg** which Extracts a file base_images/2_c.jpg .again unzip by **unzip base_images/2_c.jpg** .we find another file from that extaction process we obtain a file Flag.txt.now run cat flag.txt
- **Flag - picoCTF{336cf6d51c9d9774fd37196c1d7320ff}**

10)PicoCTF - tunn3l v1s10n

I tried a lot but couldn't find the flag(used wireshark)

11)PicoCTF – Can you see

- **Tools used –** exitf tool,cyberchef
- **Process –** downloaded the unknown.zip file
  Run the cmd exitf **unknown.zip .**i found a suspicious strind so decoded by Cyberchef
- **Flag –** After decoding the text using cyberchef I obtained the flag **picoCTF{ME74D47A_HIDD3N_d8c381fd}**

1) Foundational tasks

Machine – Hackthebox – Cap

Recon stratergy: Firstly nmap scan to scan ports etc after inspection I found 3 ports open 21-FTP , 22-SSH , 80-HTTP,pcap file downloaded of nonencypted network traffic

Exploitation Method : BY changing the values of http://cap.htb/data/1 i found 3 files .To inspect those files I used wireshark.and got username and password

Steps to Retrieve the Flag: Ater login credentials use reverseshell(trick to connect back to your system from victim machine) ,later go to the user folder **cd/home/pcap** and to print the flag **cat user.txt**

Challenge: TryHackMe – Brute It

Techniques used for brute-forcing:

- Dictionary Attack: Tried many passwords from a list until the correct one was found.

Tools and wordlists used:

- Hydra: A fast brute-force tool used for cracking login credentials.
- rockyou.txt: A popular wordlist that contains millions of common passwords.
- Known username: admin

  hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://<>

  password found : my2boys

  admin : my2boys

Flag(s) captured and steps taken to reach them:

User Flag:

1. Logged in to the target using: ssh
2. Moved to the admin user's home folder: **cd /home/admin , cat user.txt**
3. Got the user flag from user.txt.

Root Flag :

1. Checked : **sudo -l**

   Output : (ALL : ALL) NOPASSWD: /bin/tar
2. Used a known tar exploit to get a root shell:

sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/bash

3. Became root, then accessed the root folder**: cd /root ,cat root.txt**
   Captured the root flag!