Jack’s Discord Bot

Easy (I think idk)

New Desc (May use if want):

Jack created a new Discord Bot using a new source control platform, can you find the hidden flag that Jack hid?

Old Desc:

A Junior Developer just switched to a new source control platform. Can you find the secret token?

Answer: **HTB{v3rsi0n\_c0ntr0l\_am\_I\_right?}**

Instructions:

1. Go into the directory.
2. Run git log
3. Run:
   1. git show 47241a47f62ada864ec74bd6dedc4d33f4374699
4. It will display a token key being replaced by an encrypted key
   1. SFRCe3YzcnNpMG5fYzBudHIwbF9hbV9JX3JpZ2h0P30=
5. Decrypt the key with Base64

Hints:

1. Check for hidden folders
2. Learn how to use git 😊
   1. Check git log, git show, etc (Can be any of these)

Tutorials:

<https://www.thedigitalforensics.com/blog/hack-the-box-illumination-forensic-challenge>

Jack’s USB Log

Probably medium-hardish

New Desc (May use if want):

Jack received a USB Log from his friend who has been dumping all the USB events on his Linux host. One day, some bad guys stole data from his machine when they broke into his home. Can you help Jack figure out any leftover evidence from the bad guys?

Old Desc:

There is a sysadmin, who has been dumping all the USB events on his Linux host all the year... Recently, some bad guys managed to steal some data from his machine when they broke into the office. Can you help him to put a tail on the intruders? Note: once you find it, "crack" it.

Answer: **mychemicalromance**

Instructions:

1. First, the program opens the syslog file.
2. Iterate every line and check whether the “SerialNumber” exists.
3. If not exists, continue to the next iteration. If exists, get the hex number using string slice
4. Crosscheck the manufacturer number to auth.json, if exists, continue to next iterate, else write the serial number to a file.
5. Continue iteration for all lines.
6. User should get that
   1. 71DF5A33EFFDEA5B1882C9FBDC1240C6
   2. Is not in the auth.json
7. The code is MD5 encrypted
   1. Answer will be mychemicalromance

Hints:

1. Check SerialNumber?
2. Write an external script
3. MD5

Tutorials:

<https://joshuanatan.medium.com/hackthebox-forensics-usbripper-8b2669d7edb6>

Suspicious Image

Probably easy-medium

New Desc (May use if want):

Jack received a suspicious image from the Queen the other day, can you try and figure out what the image is

Old Desc:

Decrypt the code and find the Queen's secret!

Answer: **THEBABINGTONPLOT**

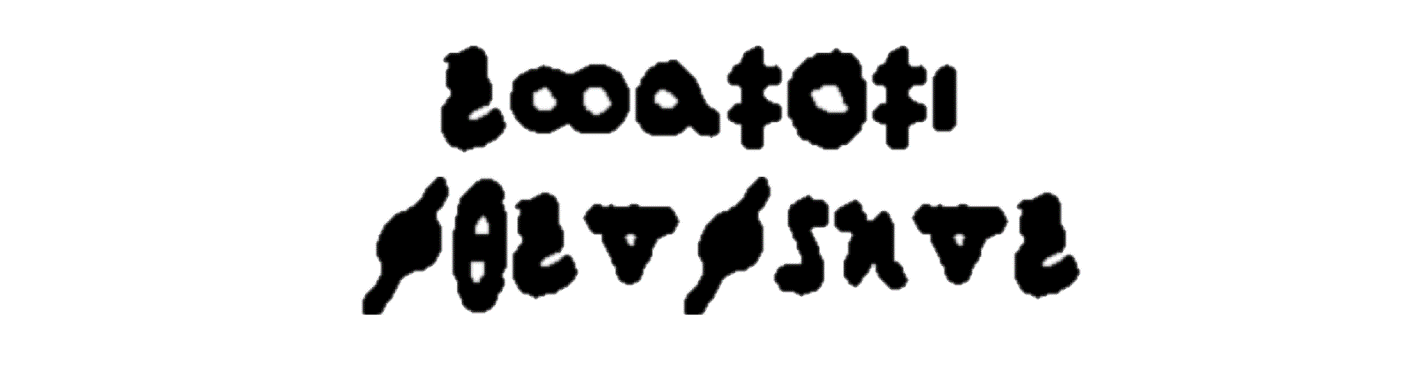
Instructions:

1. The image is a encrypted code, It uses the Mary Stuart Code cipher
2. Just use a website to decrypt it
3. <https://www.dcode.fr/mary-stuart-code>

Hints:

1. Also known as the queens cipher (But this pretty much gives it away)
2. Used by Mary Queen of Scot in 1586
3. IDK hints for this one is hard, it is really easy to give it away

The sus image:



Mystery Data File:

Medium-hardish

Desc:

Jack found a mysterious data file on his computer, he cannot figure out what the file is for or what it does. Please help Jack get to the bottom of this file

Answer: **8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL**

Instructions:

1. I was able to do this on the lab computer
2. Just follow the tutorial, it is from overthewire bandit level 12
3. You are given a hex dump, so you have to do a bunch of stuff to extract the content

Hints:

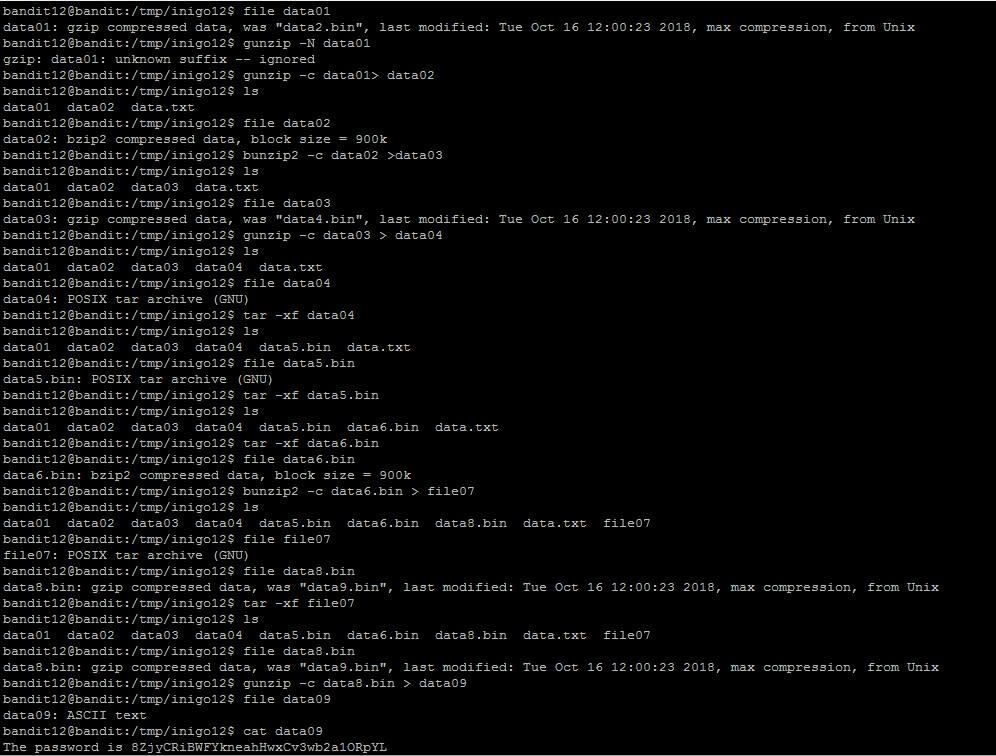
1. Look into hexdump
2. Look into the commands ‘xxd’, ‘file’,’ gunzip’,’ bunzip2’ and ‘tar’
3. grep, sort, uniq, strings, base64, tr, tar, gzip, bzip2, xxd, mkdir, cp, mv, file

Tutorials:

<https://nwrzd.medium.com/overthewire-bandit-wargames-all-level-walkthroughs-as-of-july-2019-f80f35900454>

<https://medium.com/secttp/overthewire-bandit-level-12-439f655f6fd5>

The commands to run is in the image below



Hacklab:

Probably easyish-medium?

New Desc (May use if want):

Jack was looking into the old Hacklab website, but he is a little stuck on trying to understand the code and could some use some help.

Old Desc:

We want to update our website but we are unable to because the developer who coded this left today. Can you take a look?

Answer: **W3Lc0m3\_70\_J4V45CR1p7\_d30bFu5C4710N**

Instructions:

1. Look at login.js
2. Paste the code there into a JS Deobfuscator
3. Look for ‘var res = String…’
4. Run the ‘var res = String…’ code in the Javascript console
5. Print out ‘res’, and it will give the flag

Hints:

1. Look into JS Obfuscator
2. Look for phishy code or useless code
3. Hints that direct them to look for ‘var res = String…’

Stuff

Easy

New Desc (May use if want):

The flag is stored in the file Stuff.txt and is the only line of text that occurs only once

Answer: **UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR**

Instructions:

1. Run cat Stuff.txt | sort | uniq -u

Hints:

Hints:

1. Look into the commands sort and uniq