Hands-On Hardware Hacking

Password Cracking

Web App Sec

Blue Team

Evidence Tampering

Puzzle

Lock Pick

Practical Prompt Injection (LLMs)

Purple Teaming

Active Directory Hacking

# RE

## **Blackout**

### **100**

Hard to see in the dark.

Blackout.pdf

## **Book10**

### **100**

Excel is fun!

HTHBook10.xls

## **Quarantine**

### **100**

Seems something is not right with one of these files.

Hint: I wonder if there is a difference

Quarantine.7z

## **GrrrrrrepCut**

### **170**

Parse all the things

Flag\_file.tar.xz

## **Diffrnt**

### **188**

thisOne is DIFFerent from thatOne

Diffrnt.ar

## **LitenUp**

### **188**

Its a database with stuff and things...

HTH\_database.db

## **Fractured in Time**

### **200**

Unzip and view readme

Fractured\_in\_Time.zip

# Ciphers

## **Basic Cipher**

# 

### **100**

# 

# cipher

# 

# You have intercepted a message that appears to be an unknown cipher. Your task is to decipher the message and uncover the hidden message within. We've provided you with a ciphertext file, cipher.txt.

# Hint: The challenge involves a substitution cipher.

# Hint: Kali Linux has various tools for cryptography analysis, including ones to break simple substitution ciphers. Tefp zexiibkdb rpbp x pfjmib prypqfqrqflk zfmebo

# Ffka vlro cixd tebk vlr plisb qeb ofaaib

# Glla irzh xka exmmv exzhfkd

# Fixd: HTH{Tebob\_fp\_kl\_prypqfqrqb\_4\_hkltibadb} **Riddle Me This**

# 

### **300**

# 

# cipher

# 

# Round and round we go with ones and zeros. What year is it? Long time since Vegenere was alive. Maybe we should look at the year through Vegenere's eyes. Wonder what posture he would have on gun control?

# Villages

## **Hardware Hacking Village #1**

SFRIezExLjAyLjIwMjMtODk1OTA1Nzh9

HTH{11.02.2023-89590578}

## **SecBox**

### **400**

Secbox is a phsyical container in the hardware hacking village that turns on a lightbub if you hack it. Photo included so you know what it looks like.

## **AD Village**

### **400**

Visit the AD village

## **Password Cracking Village**

### **400**

See the AD village for a hash, then visit the password cracking village.

**Hardware Hacking Village #1**

### **400**

To obtain this flag, you will need to visit the Hardware Hacking Village and exploit the embedded camera system. The flag can be found in a subfolder under the *'/mnt'* directory.

**Tamper Evidence Village #1**

### **400**

Visit the Tamper Evidence Village and bypass the tamper evident seal. Once complete, please show your work to the village lead to get the flag.

**Phone Notification**

### **400**

intro

Did you receive the phone application notification?

## **Lockpick Village 1**

### **400**

intro

Crack the box at the Lockpick village to get the flag. (Must also tell Andy that you like his hair)

# Village

# Forensics

## **Analysis Capture 2**

### **100**

web forensics beginner

You have intercepted a pcap file capture. Can you determine the ip address that the attacker connected to...

pcap1(1).pcap

## **Analysis Capture**

### **100**

web forensics beginner

You have intercepted a pcap file capture. Can you determine the ip address in the flag?

pcap1(2).pcap

## SVGeee

Fun with Scalable Vector Graphics!

SVGeee.zip

Open the svg file in a text editor, change the fill to #000000 then md5sum the file, use the hash to unlock the 7z file and sort by modified date. Take the hex characters from the metadata of the most recently edited SVG file and convert the hex to ascii characters, revealing the flag.

HTH{SVGsAreJustText}

## **Haystack**

### **300**

Its a haystack. Find the needles. Password to decrypt the GPG is "2023"

HTH2023-Haystack.gpg

# Exploitation

# Miscellaneous

## **HTH Logo 2**

### **100**

Its an image. Pretty.

Hint: There are two parts

HTH\_Logo-2(1).png

## **Kitt 2000**

### **100**

Misc

After "K.I.T.T. drove himself, Michael, and Shawn into the water, K.I.T.T. is brought back to life. The only problem is that he sounds a bit... different. Can you figure out what he is saying?

Hint : Wasnt James Doohan involved in this?

flag(2).wav

## **HTH Logo 1**

### **100**

Its an image. Pretty.

HTH\_Wallpaper-1(2).png

## **Between the Lines**

### **136**

Its an HTML page. Yup.

betweenthelines.ctf.digital

Hint:No comment

## **E4**

### **200**

You found this message; it seems reversible

Hint: This is not encryption

Hint: Try multiple encoding types

E4.txt

## **Double Agent**

### **200**

Oh great, B.U.F.F. infected us with ransomware! They sent a message saying they planted a flag containing the key to decrypt out data somewhere on our website. Michael's acting all weird and rolling around on the floor eating a cheeseburger so he won't be any help. Can you find the flag so we can get our data back?

doubleagent.ctf.digital

Hint: Some web applications respond differently depending on the browser you're using.

Hint: Maybe if you could *see* the *URL* you'll have better luck.

Hint:Michael's favorite Winter Olympic sport is that one where they use a broom to sweep the ice in front of those stones with handles. I'm not sure what it's called...

## **K.I.T.T. the Cat**

### **100**

Misc Beginner

I heard a rumor that cats are basically liquids. Does this apply to Cat Burglers? Lets see if we can see if Grace took the jewels or not.

nc kitt.ctf.digital 8889

## **Discord #ctf-support**

### **400**

Do you even Discord?<https://discord.gg/RpKgzSQaqG>

## **OSINT**

### **400**

Who is Rollinz007? This is a single win challenge!

# RE

GrrrepCut:

cat flag\_file.txt | grep "'" | grep '"' | tail -n 1337 | grep -v '\$' | grep -v 'X' | cut -d'1' -f 5 | cut -c 6- | cut -c -1 | tr -d '\n'

HTH{CLIROCKS!}

LitenUp:

echo 'U2FsdGVkX18y9i7iyofZolzOAHSfKakrSxkXTwj294iFcqMZvuS07DdPiIzA0n1r' | openssl enc -d -a -aes-256-cbc -p

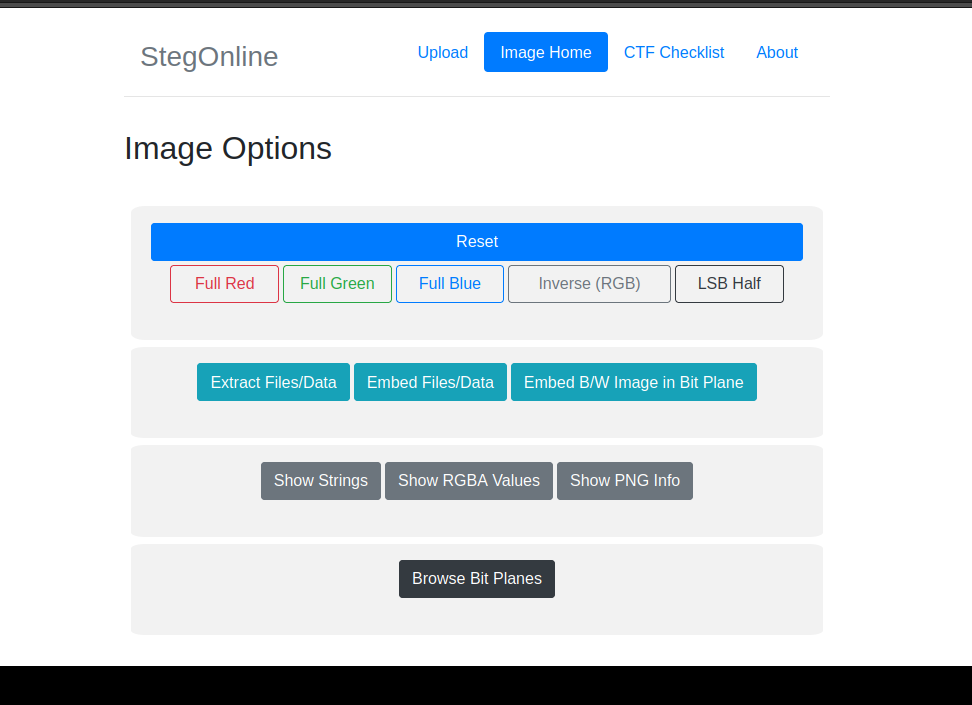
password: 1982PontiacTransAm

# Misc

## **HTH Logo 1**

Its an image. Pretty.

<https://stegonline.georgeom.net/image>

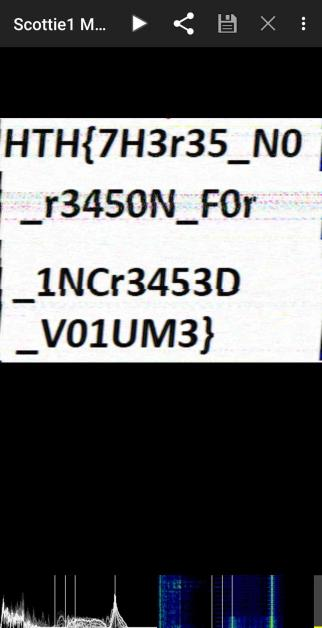




HTH{UPDOWNDOWNLRLRBABASTART}

HTH{UPUPDOWNDOWNLRLRBABASTART}

HTH{UPUPDOWNDOWNLRLRBABASTART}

KITT2000  


# Web

## Cookie Monster

I have this website that adds a random number of cookies to your cookie jar. If you fill up the jar, you get the flag. But you are impatient, see if you can get all the cookies you need really quick.

<https://cookiemonster1.ctf.digital/>

Hint :You really dont want to click that button millions of times... How else can you get cookies

* Click the button once to get some cookies, modify the cookie count using developer tools to a large number and click “get more cookies”, the flag is given when the threshold is exceeded.

HTH{OmNomnomnom1887987}

## **Super Secret Agent**

### **100**

web

This flag is not accessible unless your are a super secret Spiceduck agent.

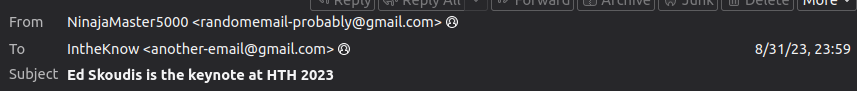
secret.ctf.digital

# OSINT

## **Eml\_me**

## **As Strongbad says "Email! Email! Email!"**

Hint: Ed is looking sharp!



| **Hey Friend,  Did you hear?! Ed Skoudis is the keynote at Hackers Teaching Hackers 2023. I just read the post from the conference founder, John Harper on LinkedIn. Check it out: https://www.linkedin.com/posts/harperjohn\_i-am-super-stoked-to-have-ed-skoudis-as-a-activity-7103223406459817984--lsA  Hope to see you at the conference!  Your Best Pal, NinjaMaster5000  P.S. I hear the CTF is going to be great. 😉😉** |
| --- |

## **Go to** [**https://www.linkedin.com/posts/harperjohn\_i-am-super-stoked-to-have-ed-skoudis-as-a-activity-7103223406459817984--lsA**](https://www.linkedin.com/posts/harperjohn_i-am-super-stoked-to-have-ed-skoudis-as-a-activity-7103223406459817984--lsA)**. Click the** [**https://lnkd.in/gMJZ\_nVe**](https://lnkd.in/gMJZ_nVe)**. Download EdSkoudis.jpg and run strings. base64 decode the last string. HTH flag for eml\_me is the name of the company that Ed worked for from 2000-2002. Example: HTH{Company Name} HTH{Predictive Systems}**

## 

## 

## **Treehouse\_Secrets:**

## **Passing secrets in treehouses since the 1980s! Find the answers to the clues and obtain the flag.**

## **unzip Treehouse\_Secrets.otp ./treehouse\_secrets.sh -d encoded\_20231026012257.txt Enter the key:** [**https://www.youtube.com/watch?v=S2-cnKDmB0w**](https://www.youtube.com/watch?v=S2-cnKDmB0w) **Enter the number of rounds: 9 cat decoded\_20231102131145.txt HTH{L337EncodingSkillz}**

## **Treehouse\_Secrets.otp**

# Introduction

## **Opening**

### **10**

intro

This flag was given out during the opening ceremony.

## **Introduction to Linux 1**

### **10**

intro

What year was the first release of a Linux operating system? Make sure to submit in HTH{year}

## **Introduction to Linux 2**

### **10**

intro

If we wanted to output the text "HackersTeachingHackers", what would our command be??

## **Introduction to Linux 3**

### **10**

intro

Explore the manual page of df. What directional arrow key would we use to navigate down the manual page?

linux3.ctf.digital

## **Introduction to Linux 4**

### **10**

intro

Explore the manual page of df. What flag would you use to make it human readable?

linux4.ctf.digital

## **Introduction to Linux 5**

### **10**

intro

How would you create the file named file?

linux5.ctf.digital

## **Introduction to Linux 6**

### **10**

intro

On the deployable machine, what is the file type of sample.txt?

linux6.ctf.digital

## **Introduction to Linux 7**

### **10**

intro

What are the contents of this file?

linux7.ctf.digital

## **Introduction to Linux 8**

### **10**

intro

Run the su command to become user2. Then navigate to user2's home directory and output the file located there.

linux8.ctf.digital

## **Introduction to Linux 9**

### **10**

intro

What is the directory path that would we expect logs to be stored in?

linux7.ctf.digital

## **Introduction to Linux 10**

### **10**

intro

What root directory is similar to how RAM on a computer works?

linux7.ctf.digital

## **Introduction to Linux 11**

### **10**

intro

Name the home directory of the root user

linux7.ctf.digital

Introduction to Linux 2: HTH{echo HackersTeachingHackers}

Introduction to Linux 3: HTH{down}

Introduction to Linux 4: HTH{-h}

Introduction to Linux 5: HTH{touch file}

Introduction to Linux 6: HTH{ASCII text}<http://linux6.ctf.digital/> gave me a black screen until I switched to another tab and switched back.

Introduction to Linux 7: HTH{contents}

Introduction to Linux 8 seems like it has a bug. It says to su user2 but there is no user2. Maybe there's a typo and it meant<http://linux8.ctf.digital/> but it gave a CloudFlare 502 Bad Gateway.

8, 9, 10, and 11 all say linux7, so I don't think that's it.

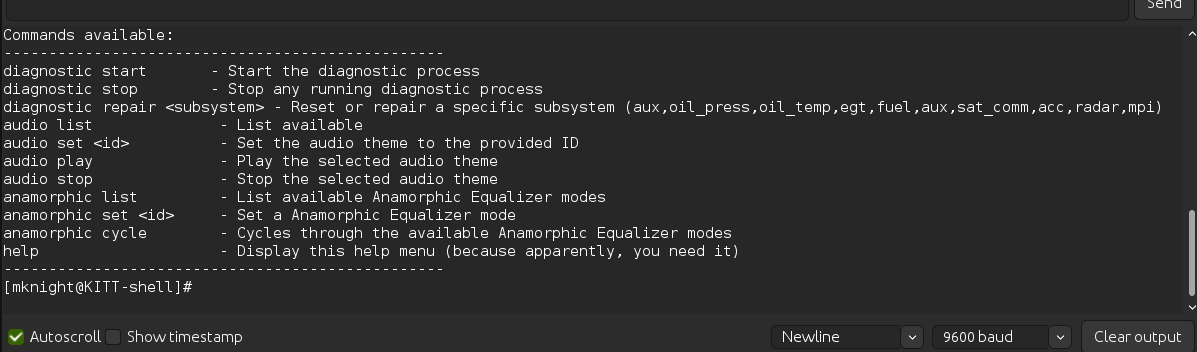
Introduction to Linux 8: HTH{user2} Looks like they're fixed now.

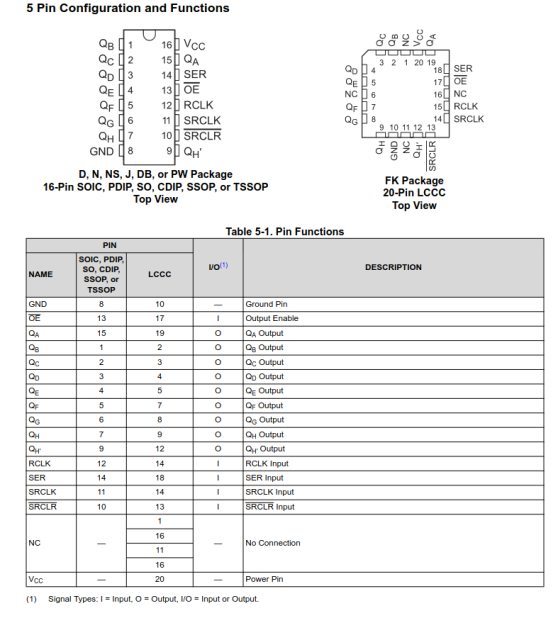
Introduction to Linux 9: HTH{/var/log}

Introduction to Linux 11: HTH{/root}

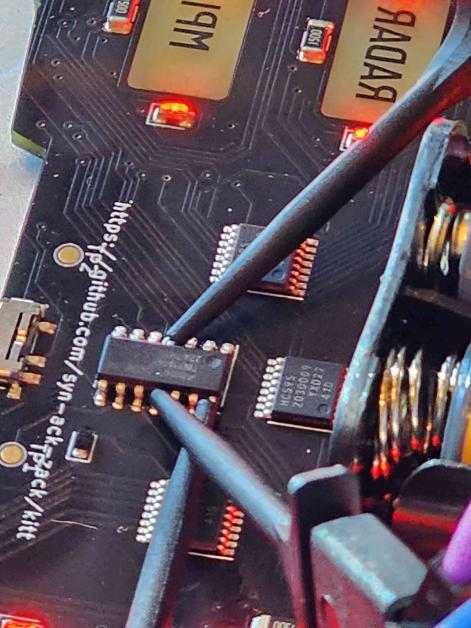
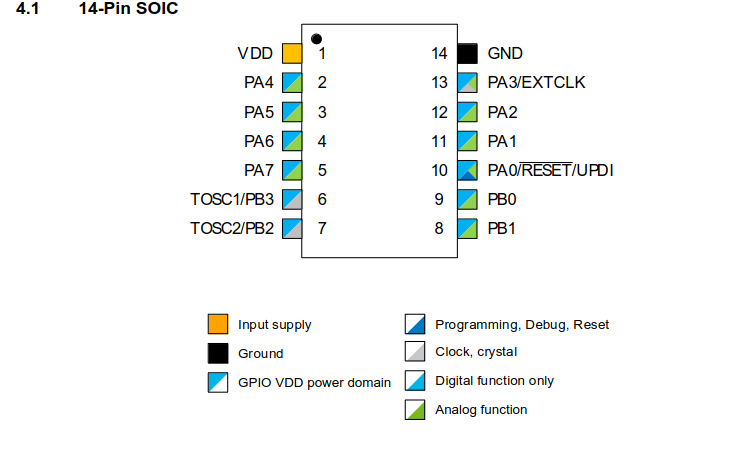
Introduction to Linux 10: HTH{/tmp}

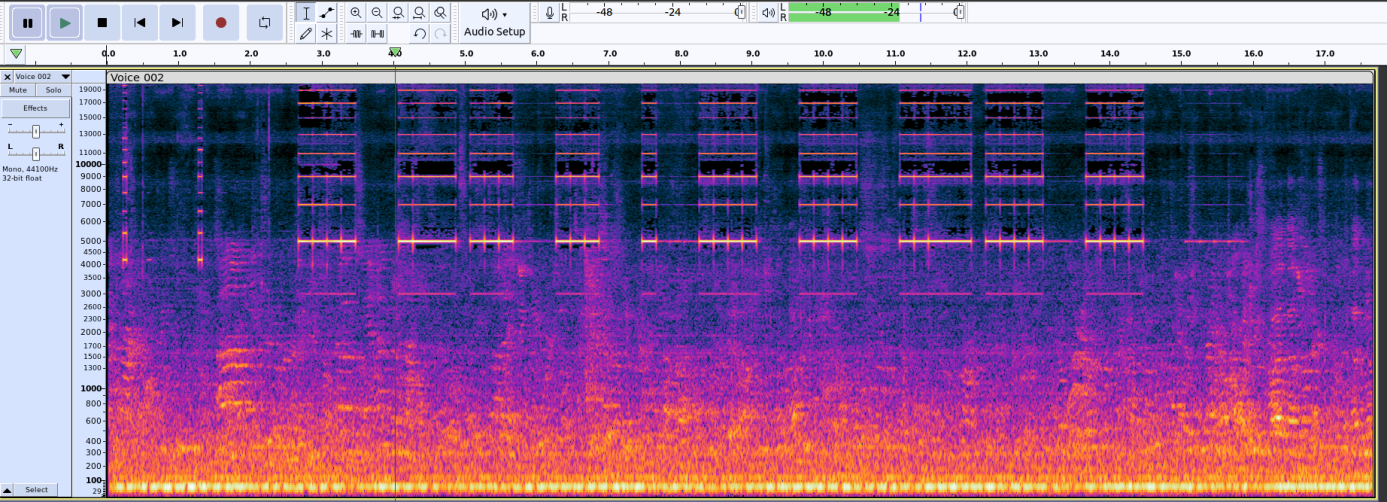
# Hardwaer





<https://www.ti.com/lit/ds/symlink/sn54hc595-sp.pdf?ts=1698991598915>





Hard to here morse code so put it in audacity to read

hasselhoff