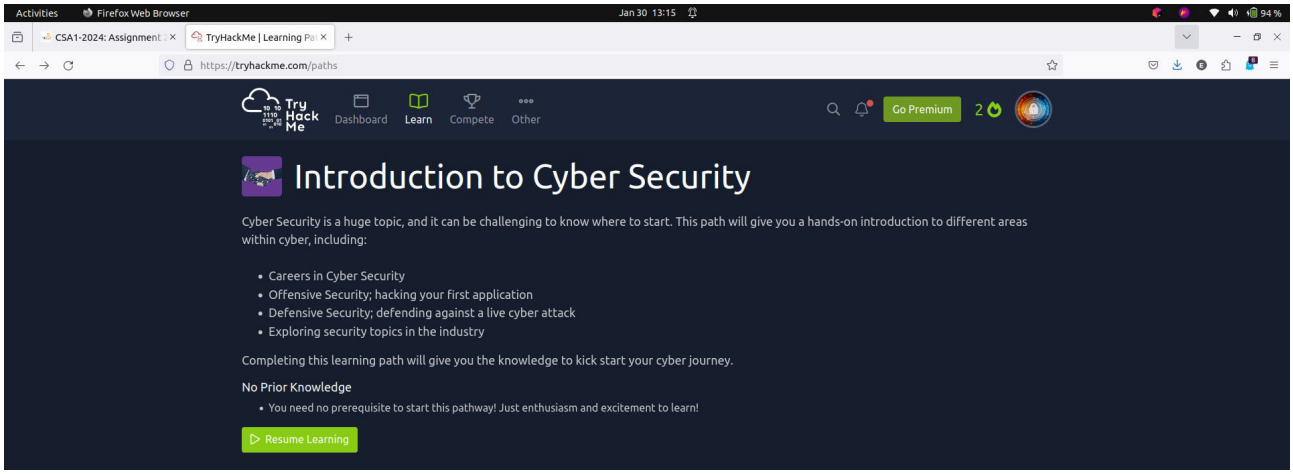
Eric Mwenda

Introduction to Cyber Security

https://tryhackme.com/p/Ericm



Task 1: What is Offensive Security

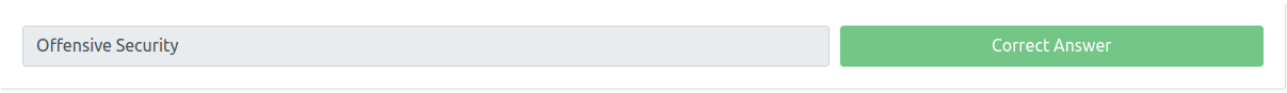
In this task the room begins by giving an explanation on what offensive security is and they define it as a process of breaking into a computer system, exploiting bugs and finding loopholes in applications to gain unauthorized access to them.

For one to beat an hacker you have to think and understand like an hacker, this is why even an ethical hacker should learn and know about Offensive Security.

Answer the questions below

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

ANS: Offensive Security



Hacking your first machine.

In this room an explanation on how to start a machine so as to hack is given:-

Here is the procedure:-

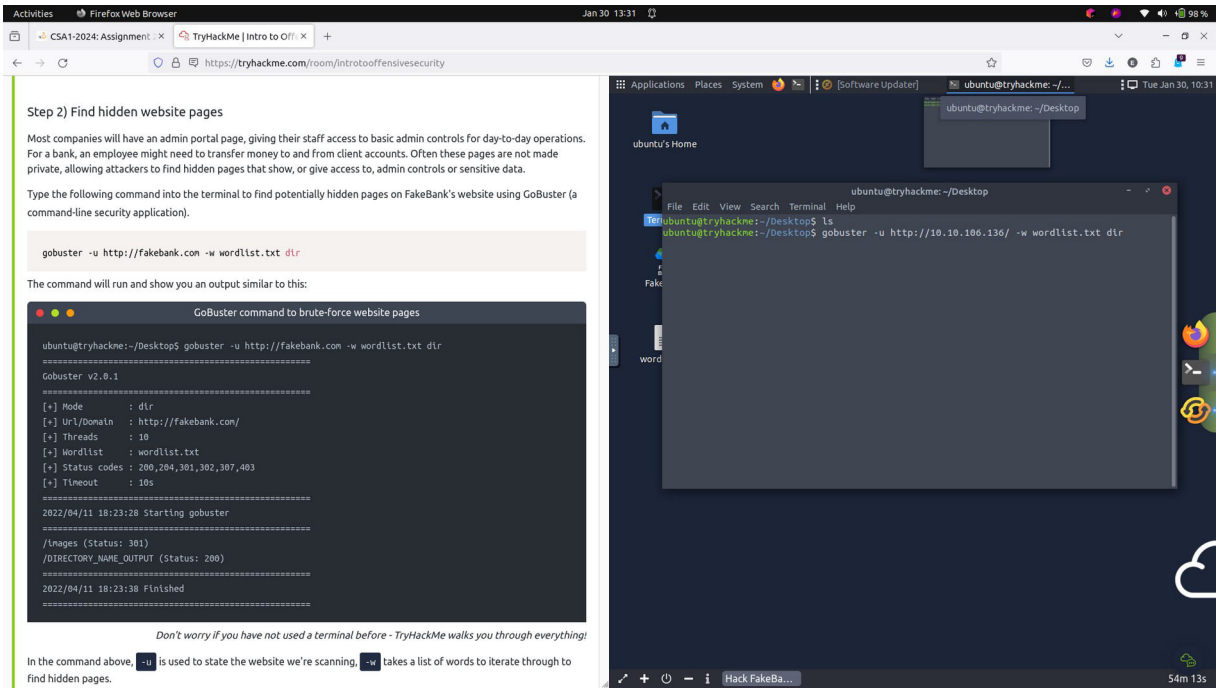
1. Click Start Machine button

2. Open the terminal in the AttackBox that you have started.

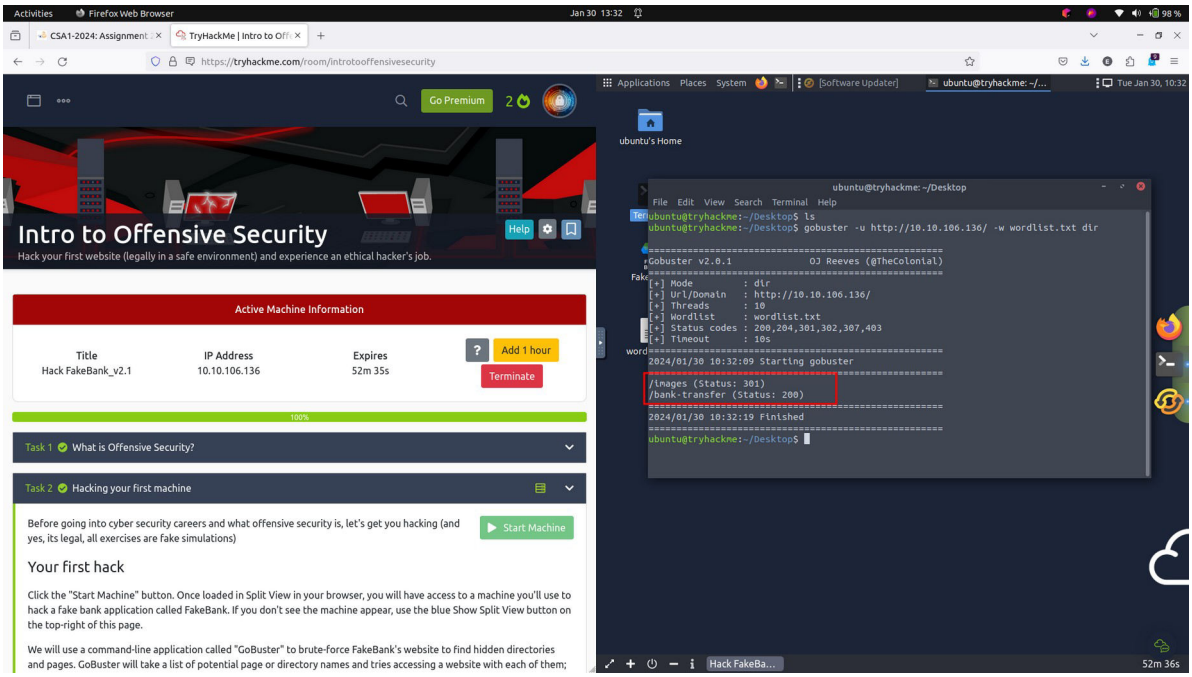
3. Run gobuster tool on the terminal to unveil hidden pages in from the target

Command that should be run is:- gobuster -u http://10.10.106.136 -w wordlist.txt dir

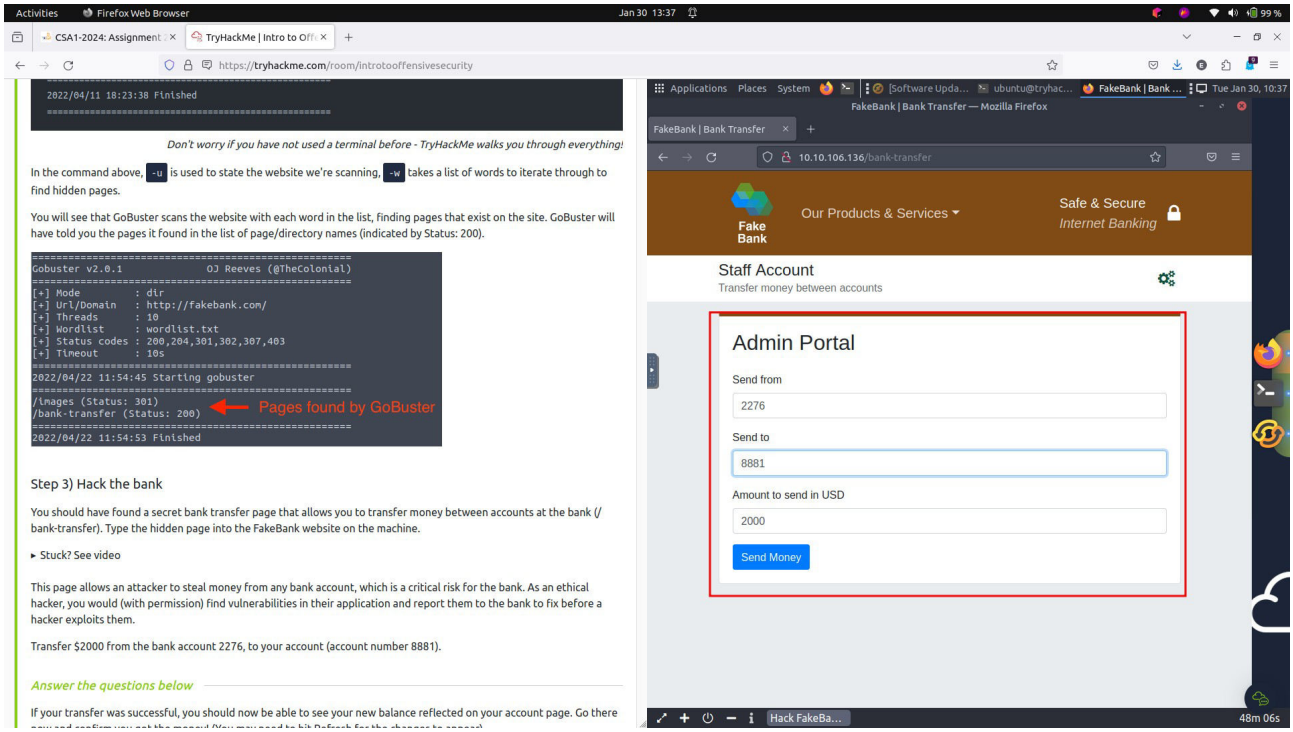
In the command above, -u is used to state the website we're scanning, -w takes a list of words to iterate through to find hidden pages.

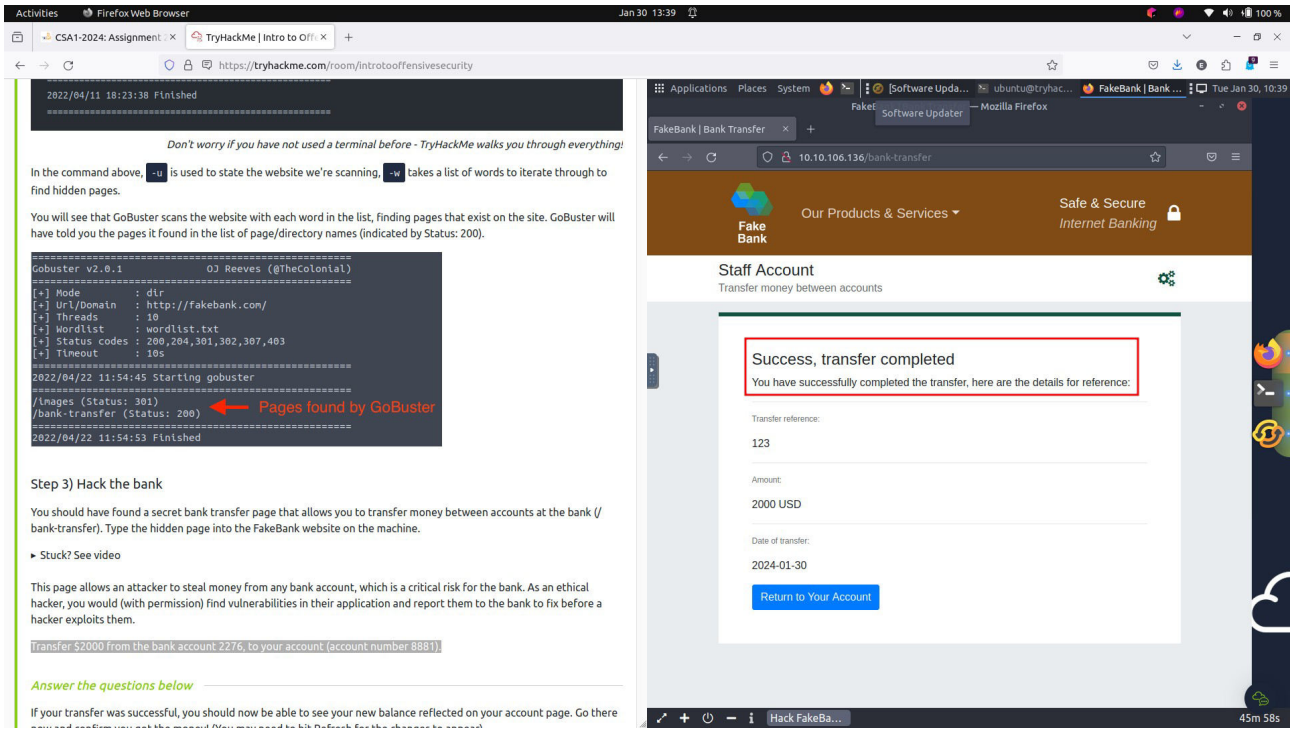


Here is the output giving out hidden pages as:- /images and /bank-transfer.



The next task given is to visit the hidden page /bank-transfer and Transfer $2000 from the bank account 2276, to your account (account number 8881).

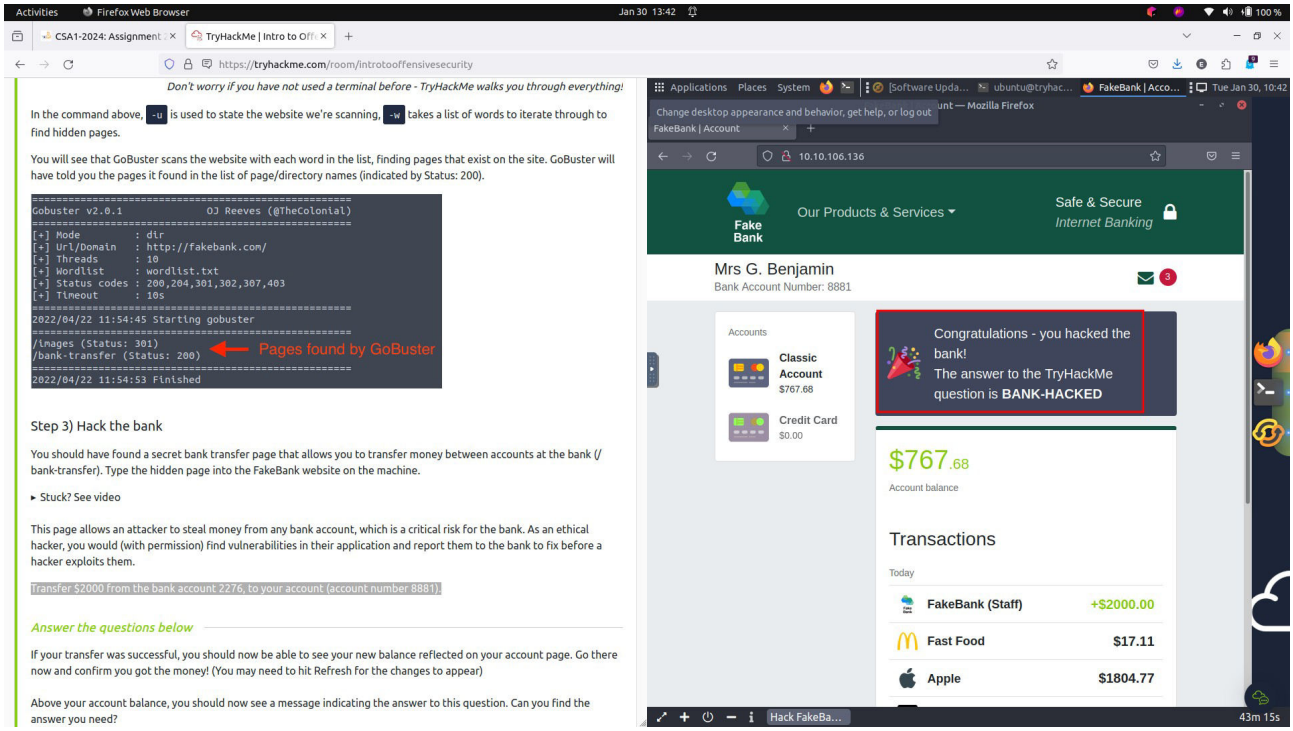


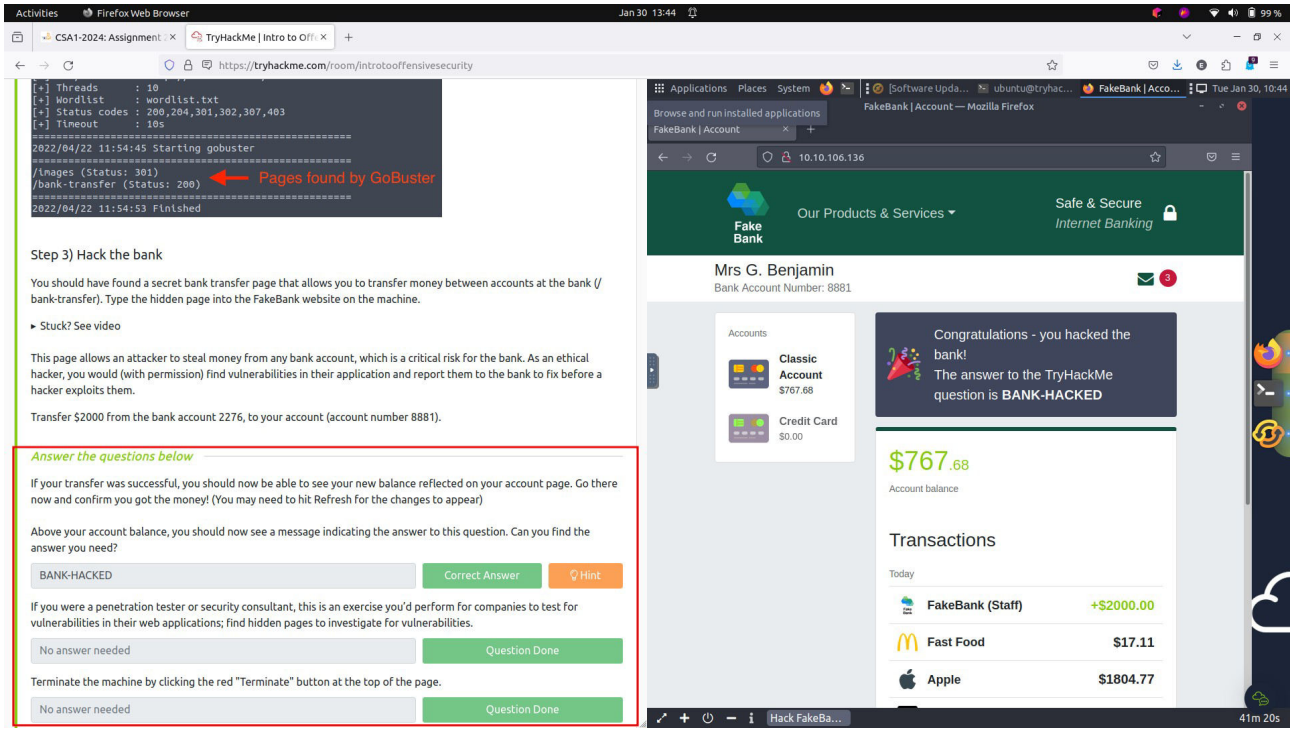


Answer the questions below

If your transfer was successful, you should now be able to see your new balance reflected on your account page. Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need? **ANS: BANK-HACKED**

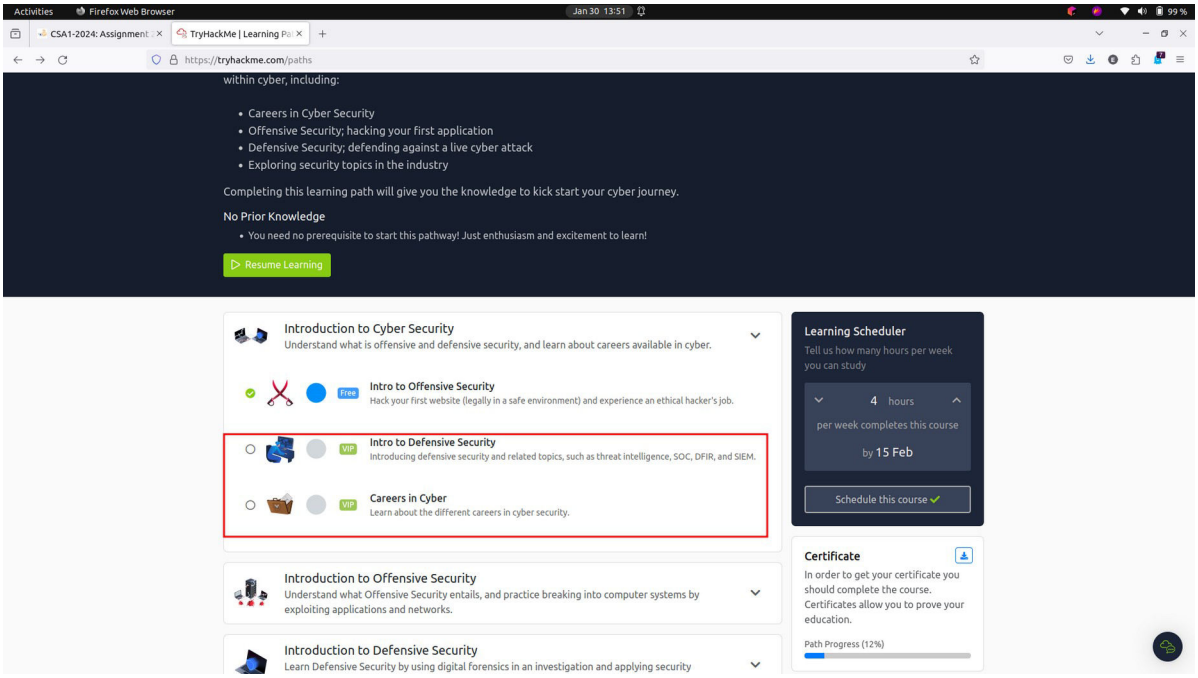




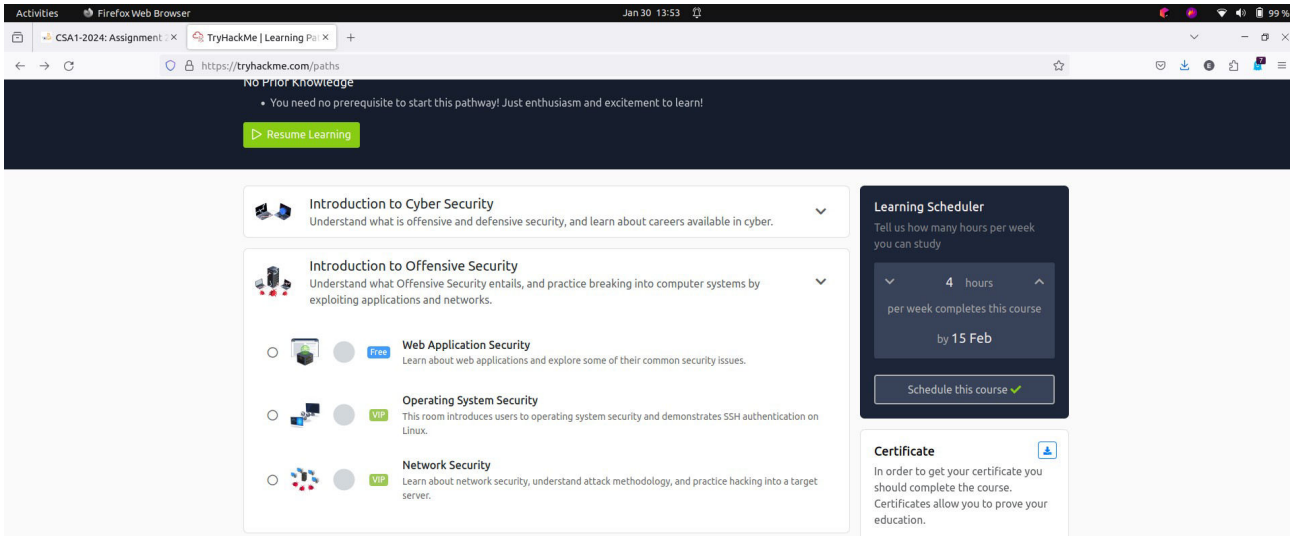
How can I start learning?

To learn an area of cyber security you're interested in, and regularly practice using hands-on exercises. Build a habit of learning a little bit each day on TryHackMe, and you'll acquire the knowledge to get your first job in the industry.

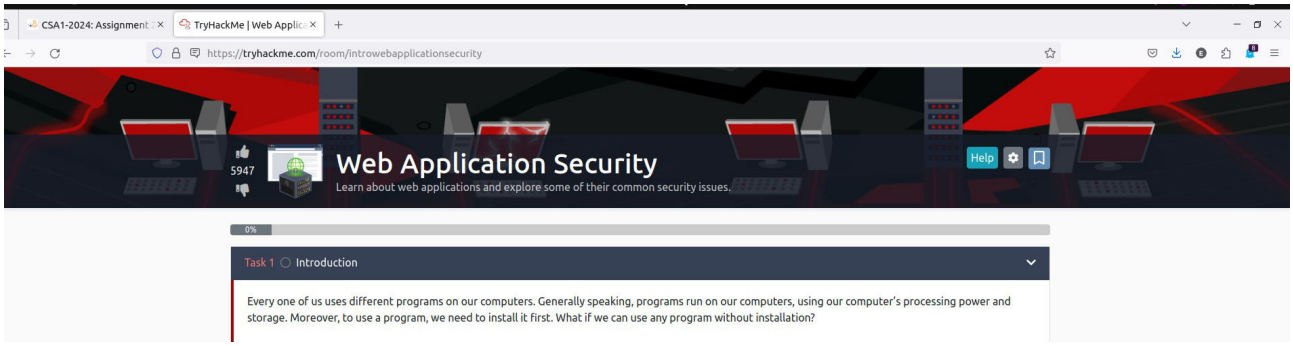
The remaining areas in this section require a subscription therefore I was unable to have a look in them so ill jump to the next sections and practice those tasks that are free.



Introduction to Offensive Security.



Task 1: Web Application Security.



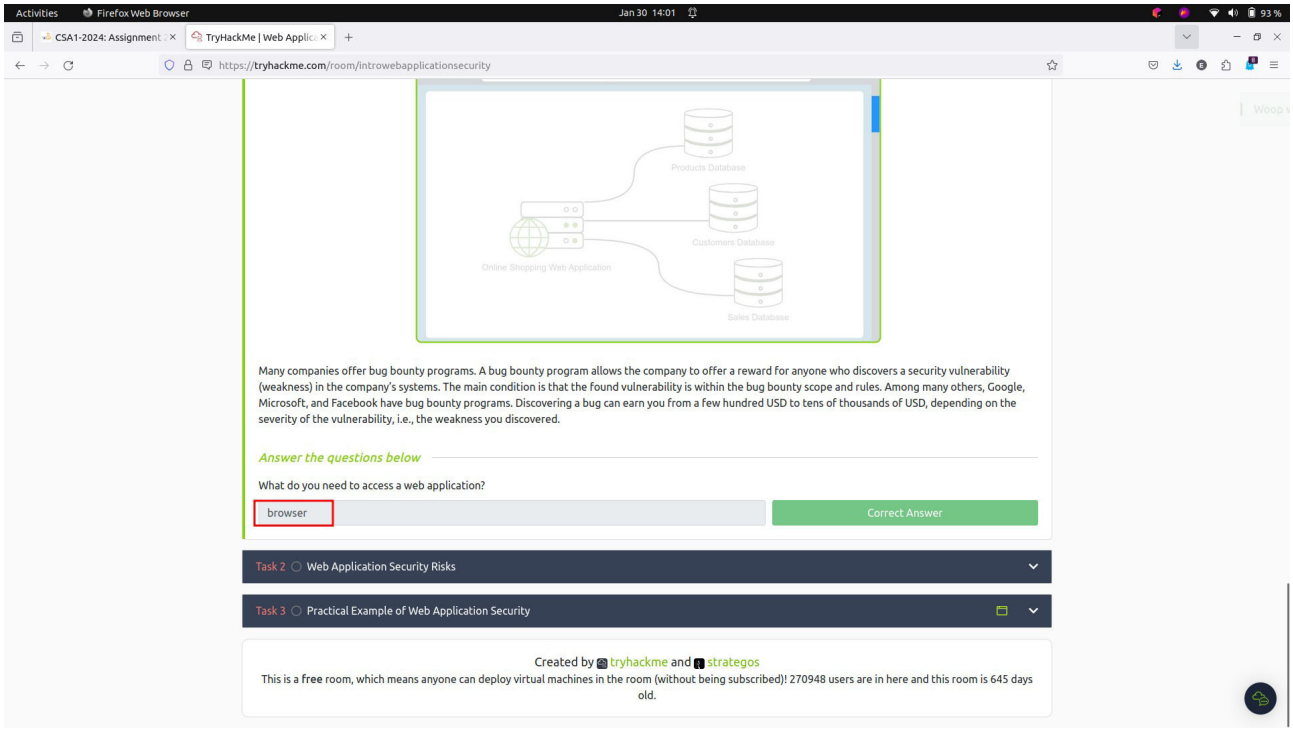
In general programs need first to be installed and run on computers, using computer's processing power and storage.

Its also possible to run programs without utilizing your personal storage devices by using web applications as long as we have a modern standard web browser, such as Firefox, Safari, or Chrome this is made possible.

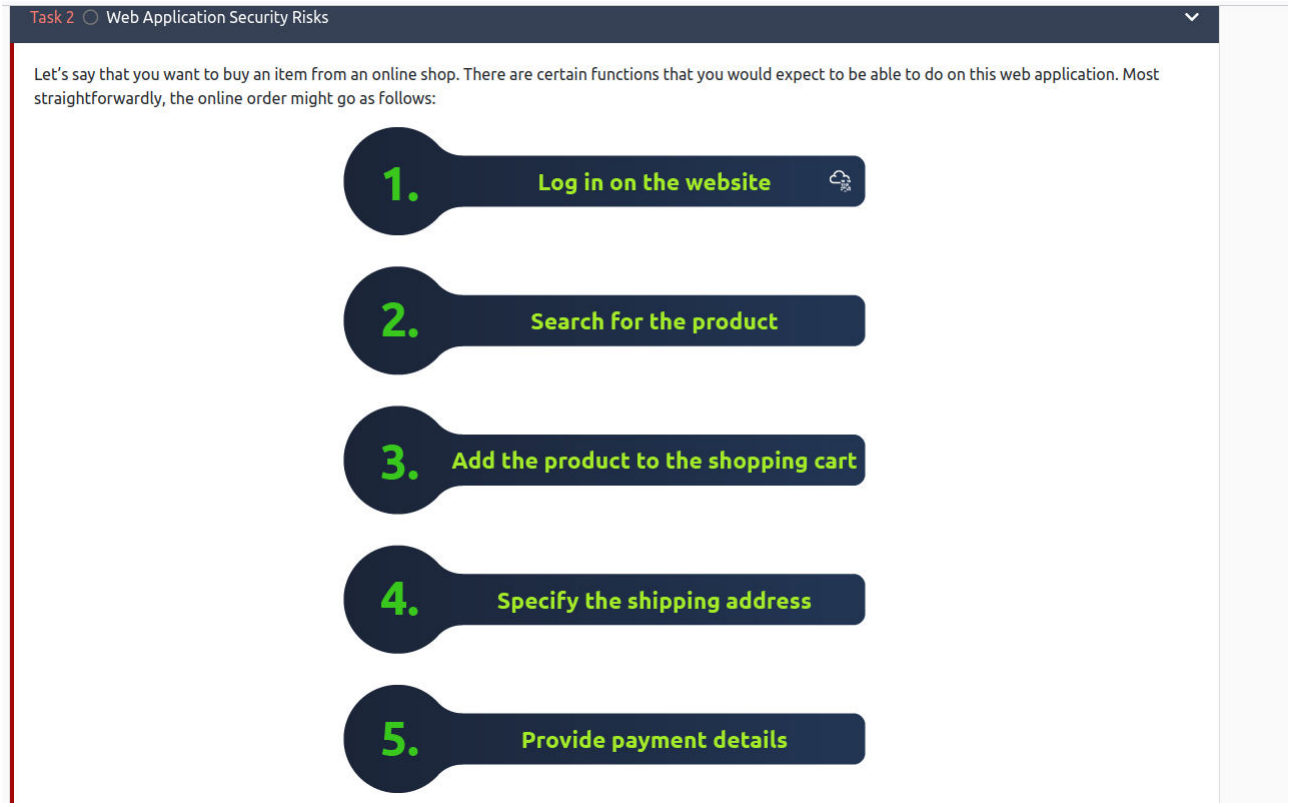
The idea of a web application is that it is a program running on a remote server. A server refers to a computer system running continuously to "serve" the clients. In this case, the server will run a specific type of program that can be accessed by web browsers.

Answer the questions below

What do you need to access a web application? **ANS: Browesr**



Task 2: Web Application Security Risks



I learnt that we have a few main categories of common attacks against web applications.

Here is an example to steps and their related attacks.

1. Log in at the website: The attacker can try to discover the password by trying many words. The attacker would use a long list of passwords with an automated tool to test them against the login page.

2. Search for the product: The attacker can attempt to breach the system by adding specific characters and codes to the search term. The attacker's objective is for the target system to return data it should not or execute a program it should not.

3. Provide payment details: The attacker would check if the payment details are sent in clear-text or using weak encryption. Encryption refers to making the data unreadable without knowing the secret key or password.

Identification and Authentication Failure are failures during authentication whereby the system lack the ability to prove that the user is whom they claim to be.

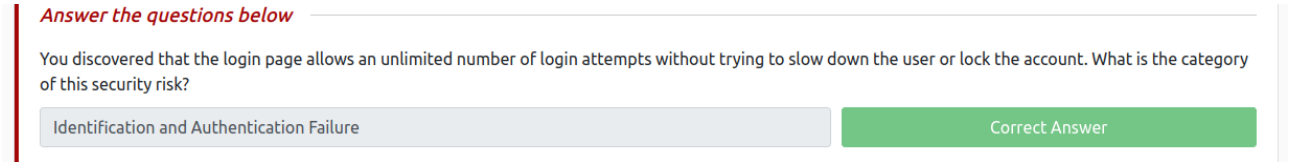
Broken Access Control is the failure in which a system cannot control only the right user to access files (documents, images, etc.) related to their role or work.

Cryptography is the the processes of encryption and decryption of data. Encryption scrambles cleartext into ciphertext, which should be gibberish to anyone who does not have the secret key to decrypt it

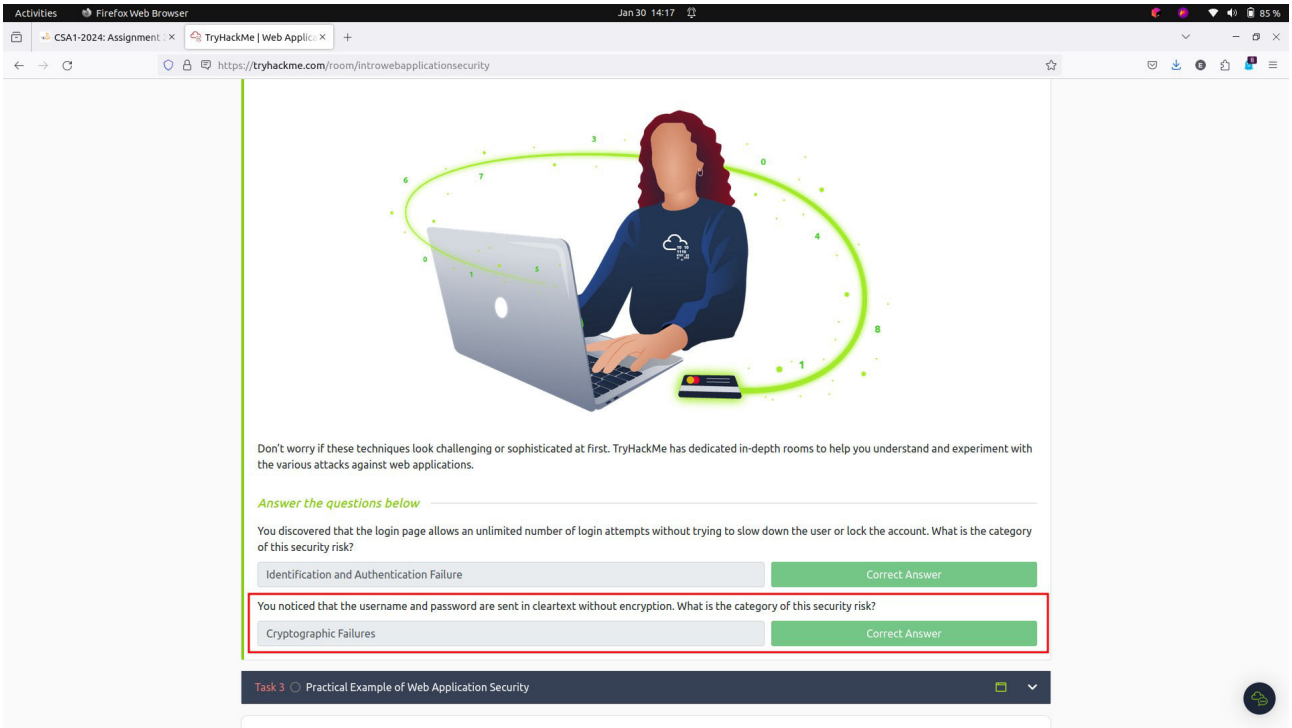
Answer the questions below

You discovered that the login page allows an unlimited number of login attempts without trying to slow down the user or lock the account. What is the category of this security risk?

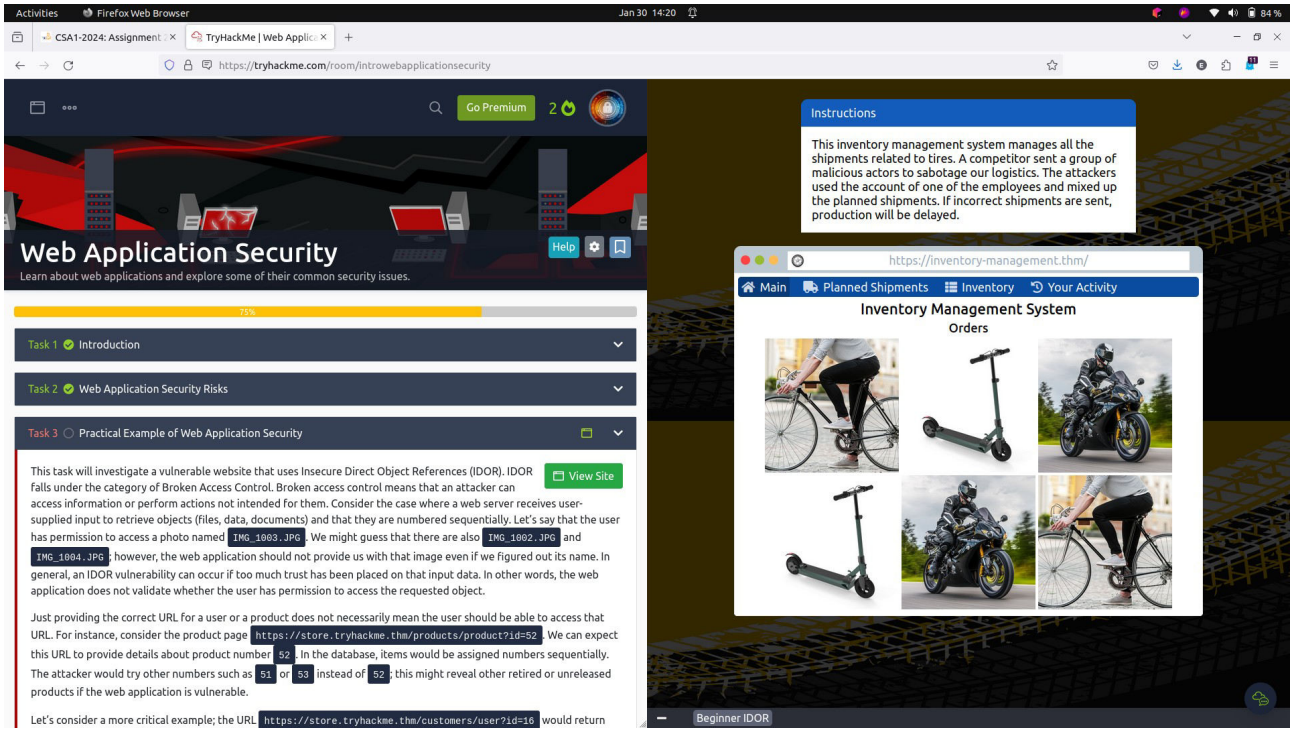
ANS: Identification and Authentication Failure



You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk? **ANS: Cryptographic Failures**



Task 3: Practical Example of Web Application Security.



In this task we investigated a vulnerable website that used Insecure Direct Object References (IDOR).

IDOR falls under the category of Broken Access Control.

Answer the questions below

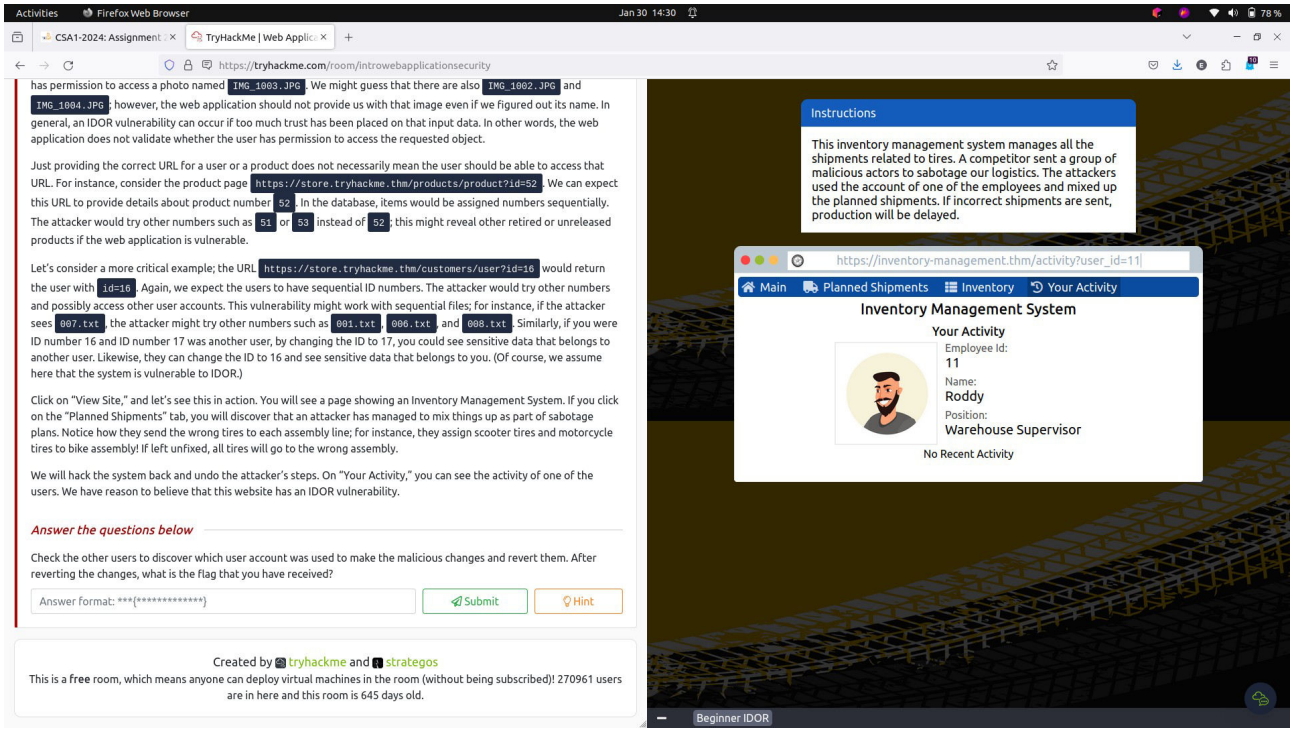
Check the other users to discover which user account was used to make the malicious changes and revert them. After reverting the changes, what is the flag that you have received?

Here are the instructions that I should follow:

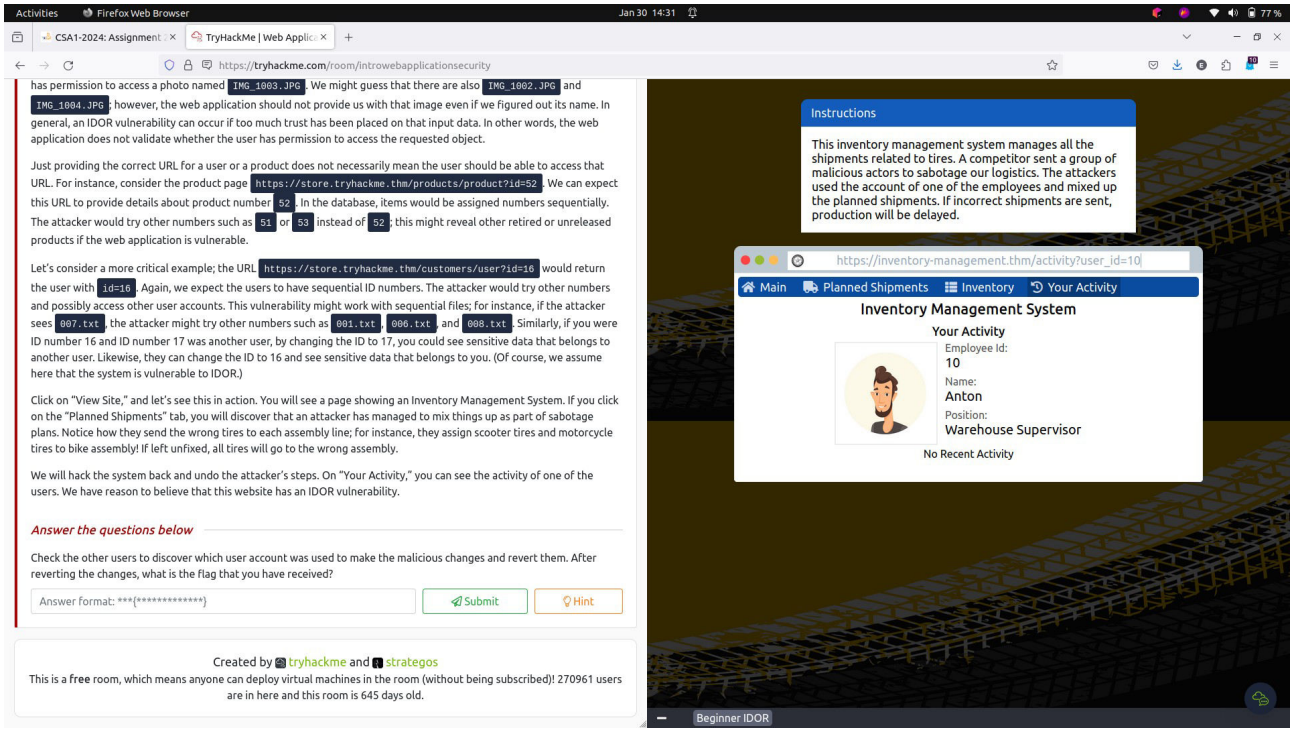
Click on “View Site,” and let’s see this in action. You will see a page showing an Inventory Management System. If you click on the “Planned Shipments” tab, you will discover that an attacker has managed to mix things up as part of sabotage plans. Notice how they send the wrong tires to each assembly line; for instance, they assign scooter tires and motorcycle tires to bike assembly! If left unfixed, all tires will go to the wrong assembly.

We will hack the system back and undo the attacker’s steps. On “Your Activity,” you can see the activity of one of the users. We have reason to believe that this website has an IDOR vulnerability.

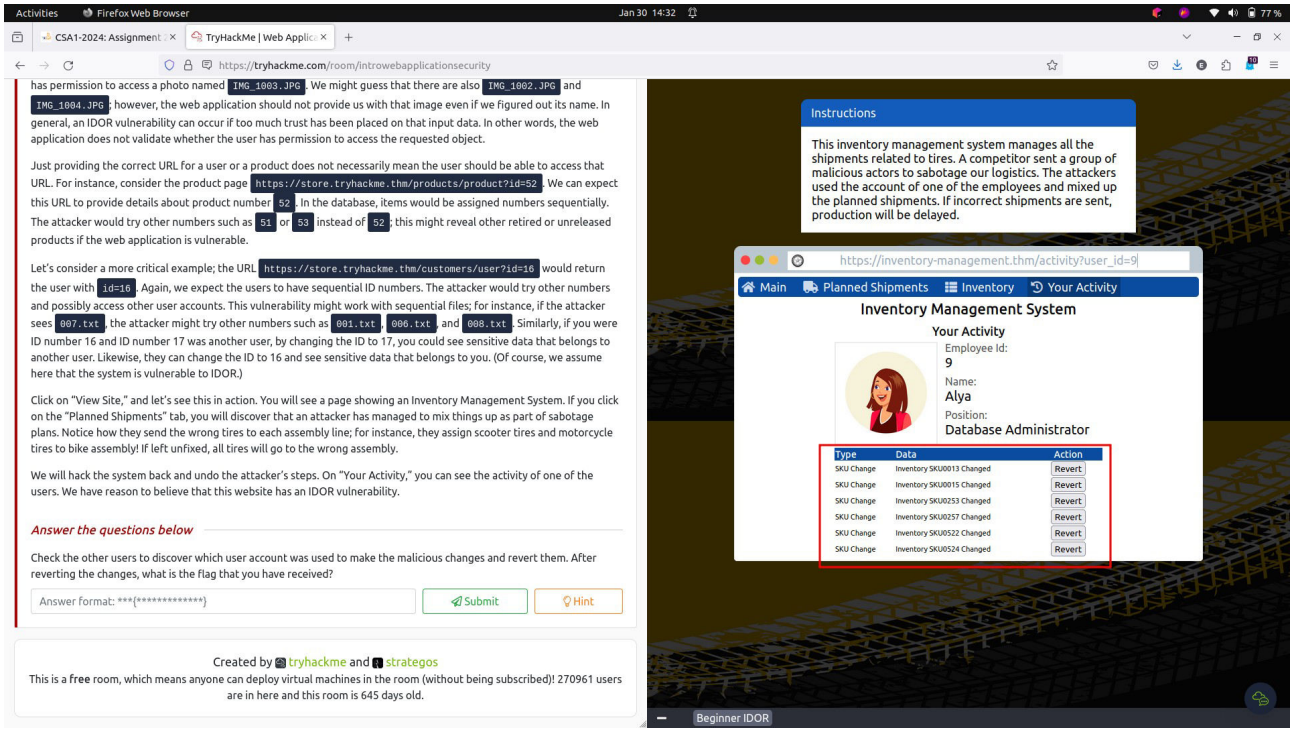
https://inventory-management.thm/activity?user_id=11



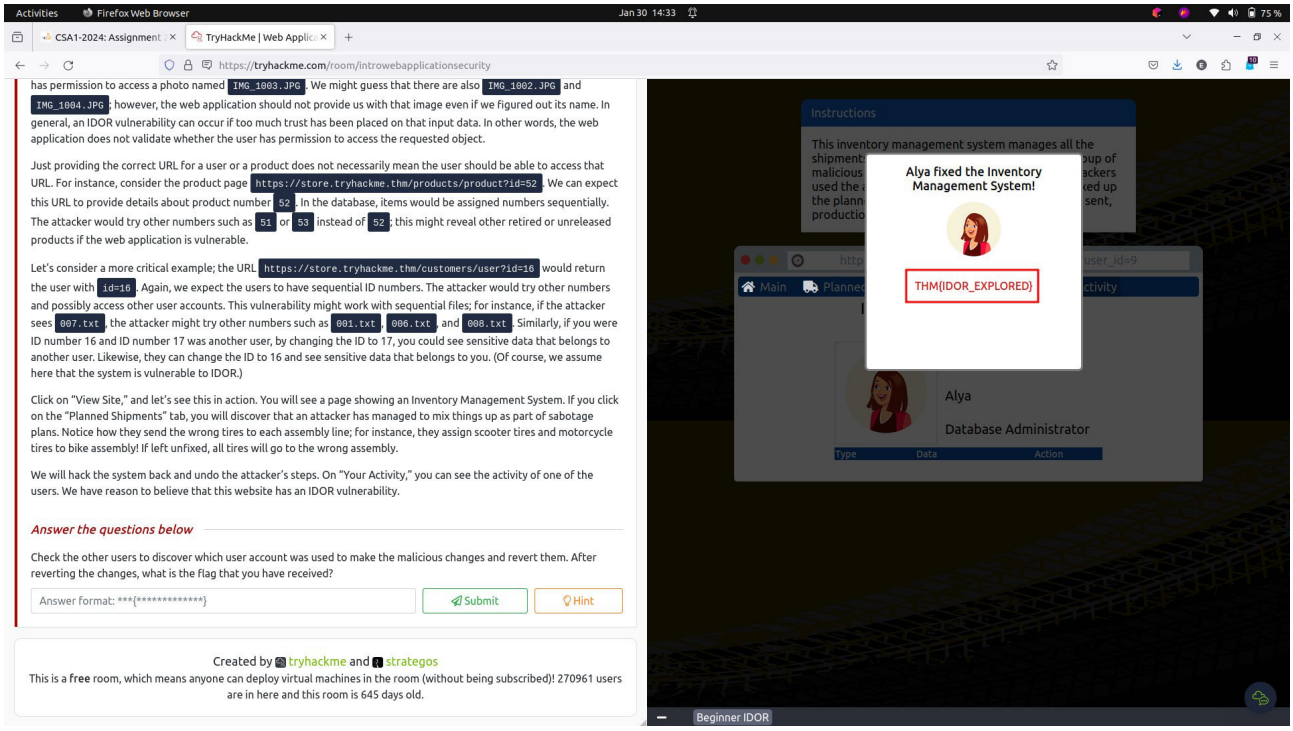
https://inventory-management.thm/activity?user_id=10



https://inventory-management.thm/activity?user_id=9



Lets revert all changes made.

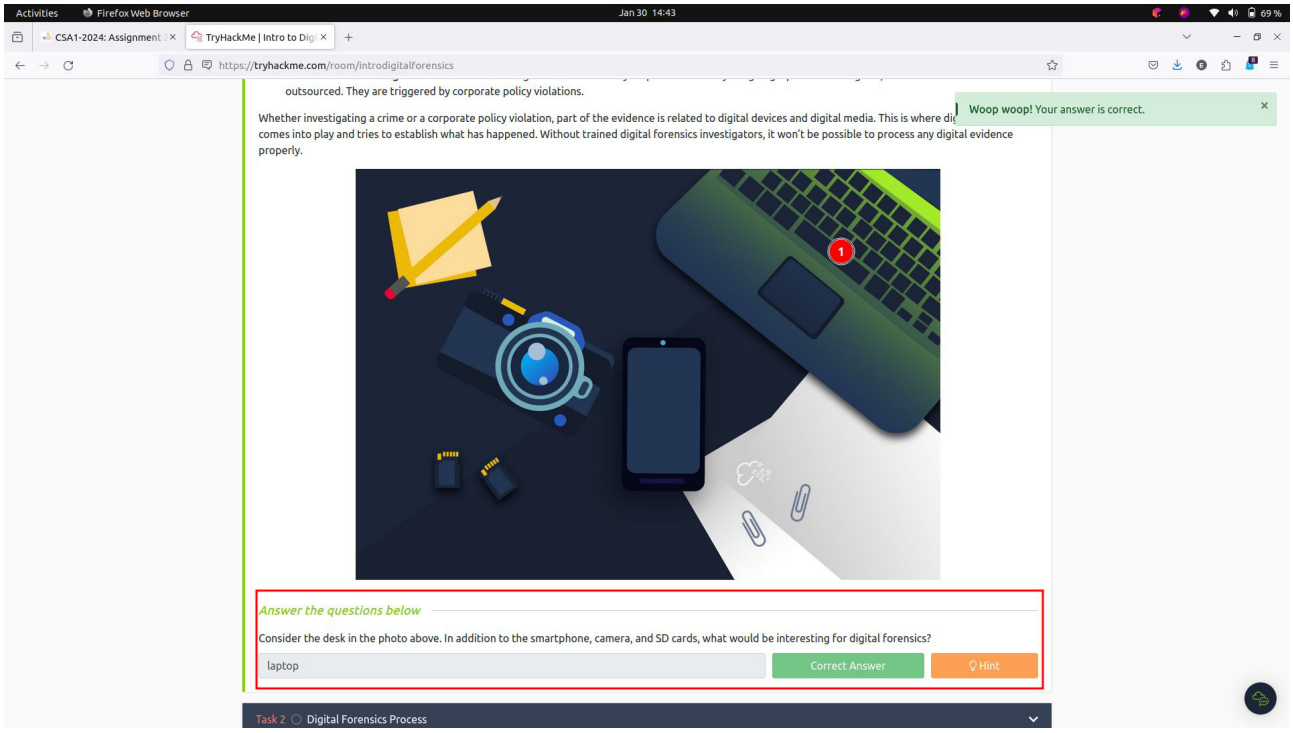


Task 1: Introduction to Digital Forensics.

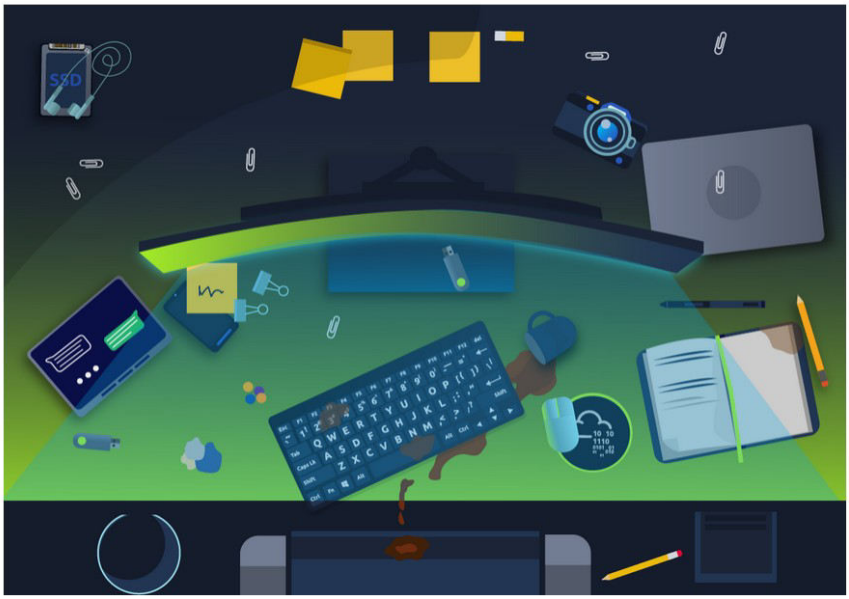
Forensics is the application of science to investigate crimes and establish facts. With the use and spread of digital systems, such as computers and smartphones, a new branch of forensics was born to investigate related crimes: computer forensics, which later evolved into, digital forensics.

Answer the questions below

Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics? **ANS: laptop**



Task 2: Digital Forensics Process.



In this section Ken Zatyko, states that digital forensics includes:-

- Proper search authority: Investigators cannot commence without the proper legal authority.

- Chain of custody: This is necessary to keep track of who was holding the evidence at any time.

- Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.

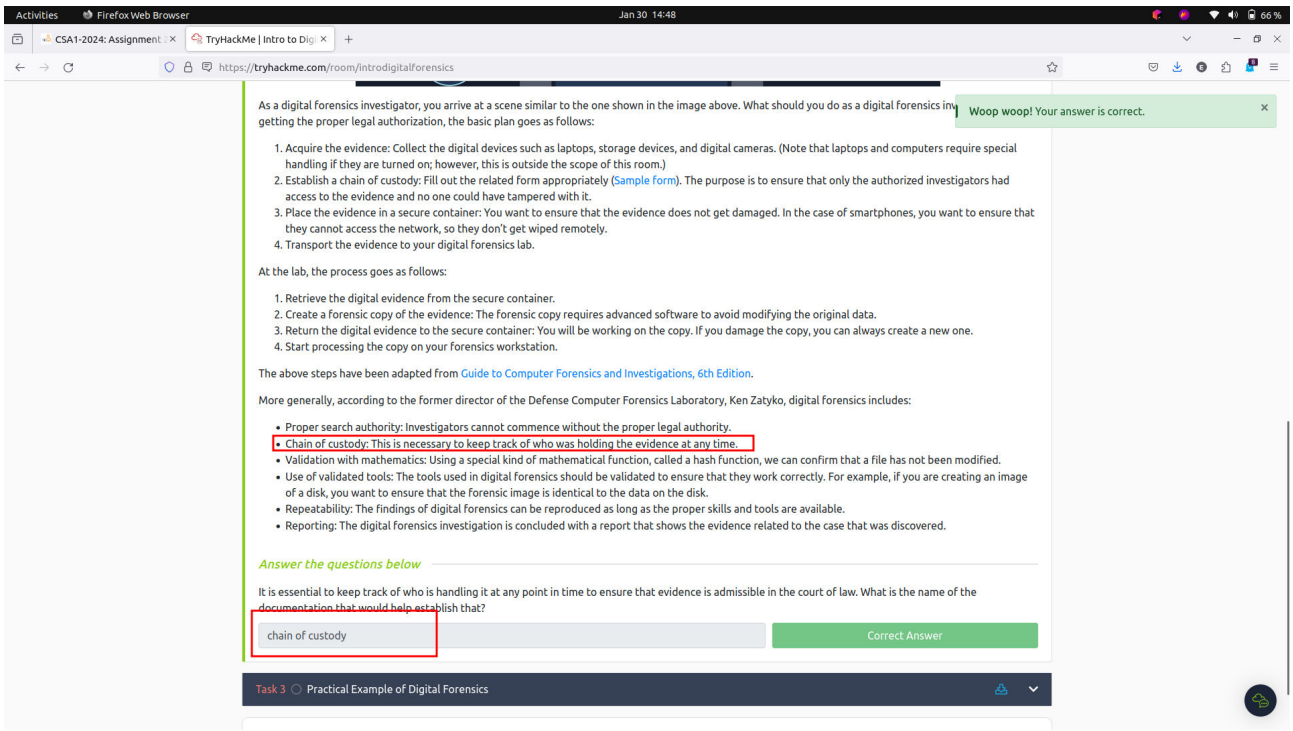
- Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.

- Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.

- Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.

Answer the questions below

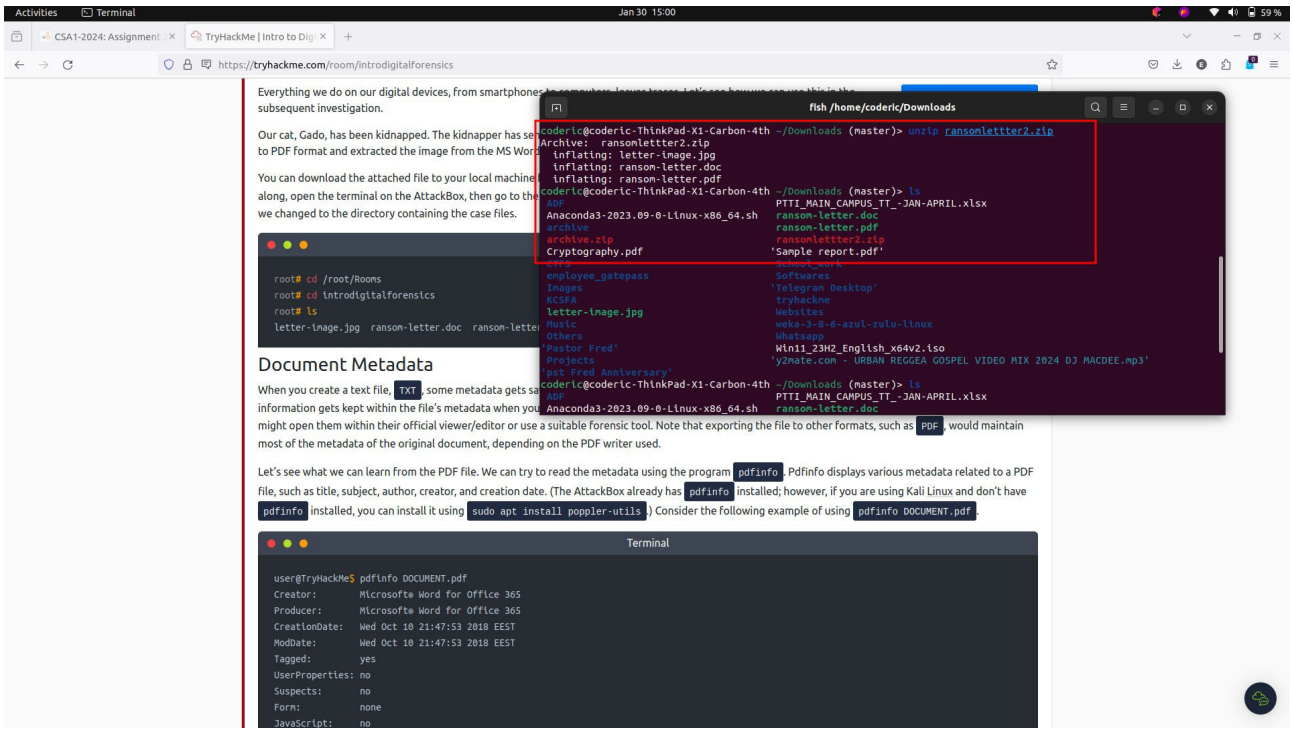
It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that? **ANS: Chain of Custody**



Task 3: Practical Example of Digital Forensics

I first downloaded the task file provided in my Local Machine.

Once the file was downloaded, I located it using the terminal and once I found it, it was in a zipped state therefore I first unzipped the file in my terminal.



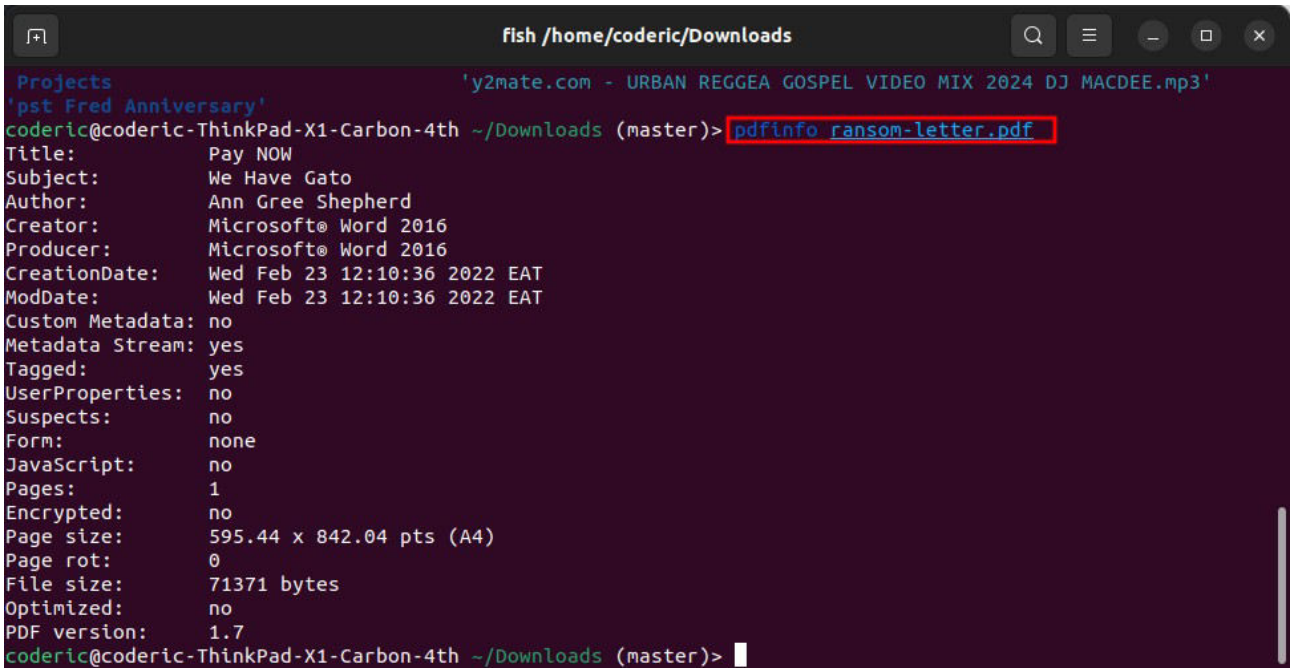
Document Metadata

This is data about documents that gets saved by the Operating System, such as file creation date and last modification date.

Answer the questions below

Using pdfinfo, find out the author of the attached PDF file. **ANS: Ann Gree Shepherd**

Command used:- pdfinfo ransom-letter.pdf



Answer the questions below

Using `pdfinfo`, find out the author of the attached PDF file.

Ann Gree Shepherd — Correct Answer

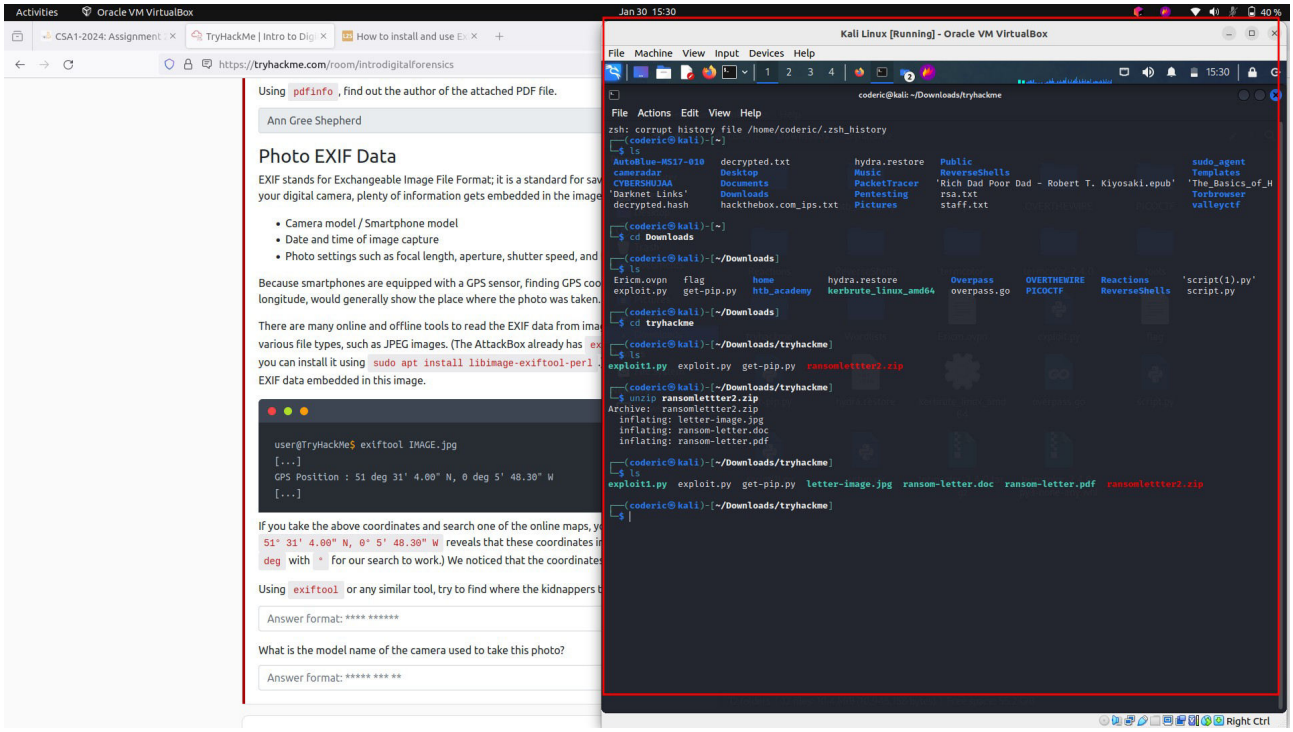
Photo EXIF Data

EXIF stands for Exchangeable Image File Format; it is a standard for saving metadata to image files. Whenever you take a photo with your smartphone or with your digital camera, plenty of information gets embedded in the image. The following are examples of metadata that can be found in the original digital images:

To get more data about an image we use the tool **ExifTool,** this tool is used to read and write metadata in various file types, such as JPEG images

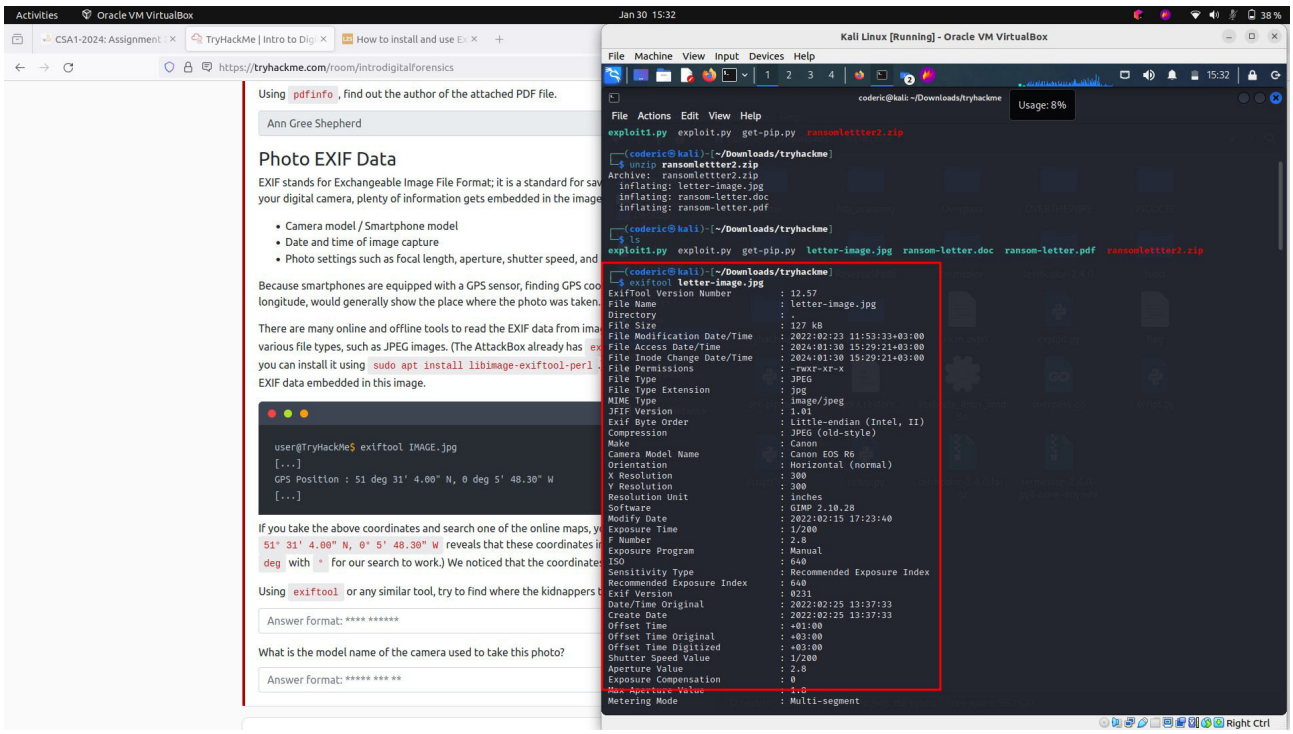
I had a problem installing the ExifTool in my Local Machine, therefore I had to use my Virtual machine for the exercises.

Here we are:-



When my virtual machine was up, next I run the exittool.

Command used:- **exiftool letter-image.jpg**

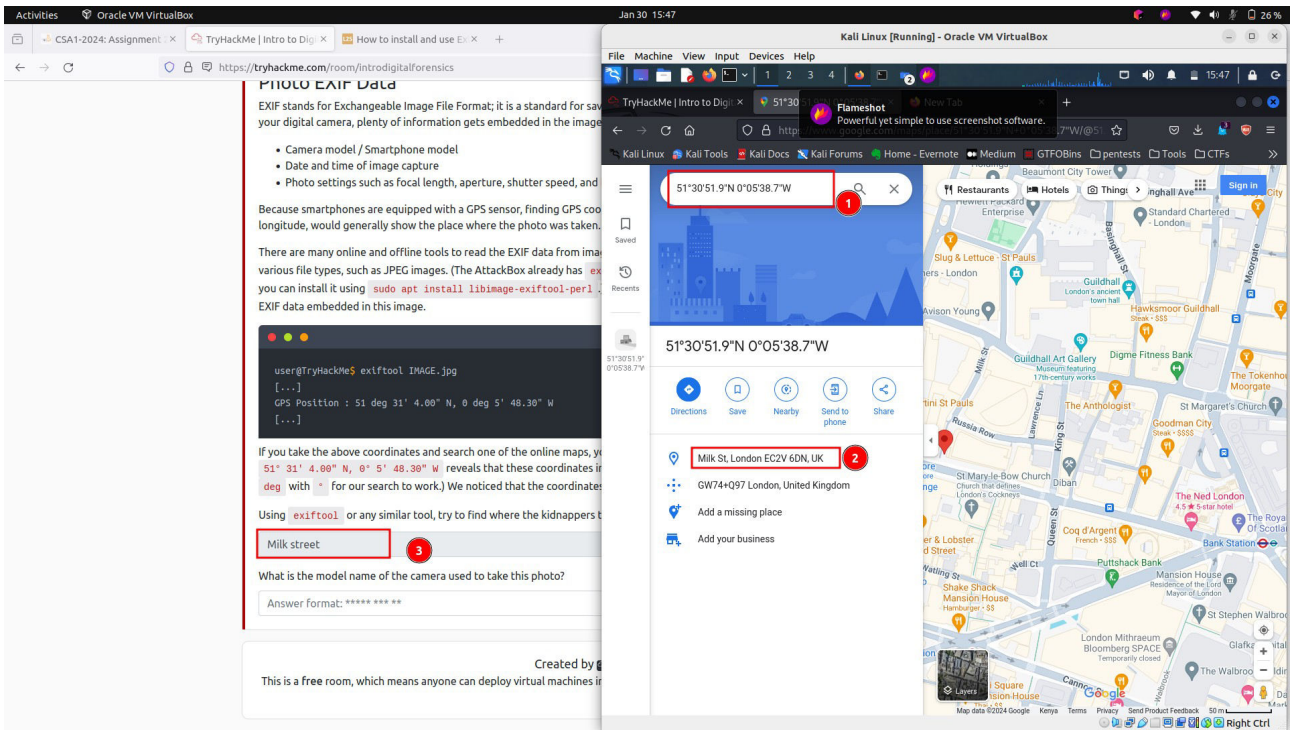


Questions

Using ExifTool or any similar tool, try to find where the kidnappers took the image they attached to their document. What is the name of the street? **ANS: Milk Street**

Having a gps position:- all I am left to is to look for this coordinates with the help of google maps.

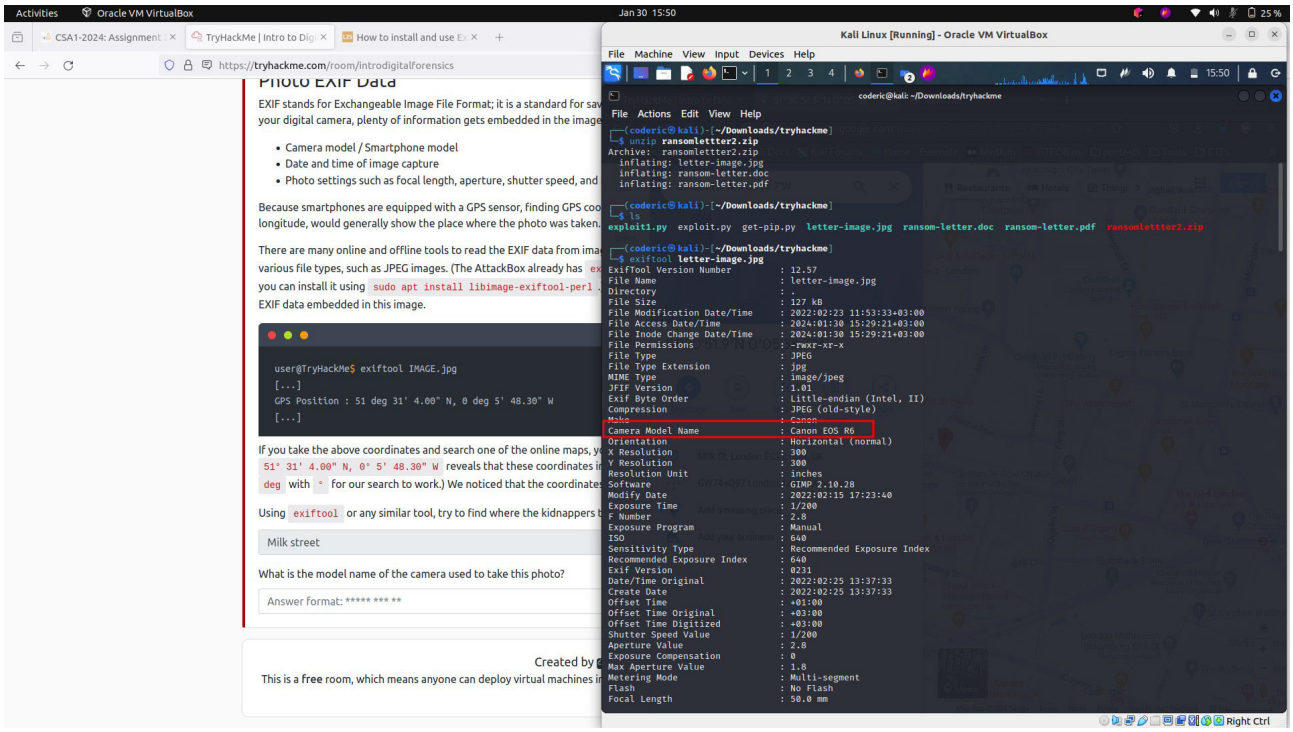
```
GPS Position                    : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
```



- With the help of google map and the co-ordinates provided after using the ExifTool I found the exact street in which the photo was taken in.

Co-ordinates used:- **51°30'51.9"N 0°05'38.7"W**

What is the model name of the camera used to take this photo? **ANS: Canon EOS R6**



Conclusion

The introduction to Cybersecurity in TryHackMe has given me a comprehensive overview on the fundamental concepts and principles which are definitely essential for anyone looking to explore more in the field of Cybersecurity.

This module has exposed me to various aspects including networking, cryptography, web security and more. The practical, hands-on nature of TryHackMe's approach enables one to develop practical skills, making it an effective platform to us as learners.

Thank you.