



**Eric Mwenda**

## Introduction to Cyber Security

<https://tryhackme.com/p/Ericm>

The screenshot shows a Firefox browser window with the URL <https://tryhackme.com/paths>. The page title is "Introduction to Cyber Security". Below the title, it says: "Cyber Security is a huge topic, and it can be challenging to know where to start. This path will give you a hands-on introduction to different areas within cyber, including:" followed by a bulleted list: "• Careers in Cyber Security", "• Offensive Security; hacking your first application", "• Defensive Security; defending against a live cyber attack", and "• Exploring security topics in the industry". It also states: "Completing this learning path will give you the knowledge to kick start your cyber journey." and "No Prior Knowledge" with the note: "• You need no prerequisite to start this pathway! Just enthusiasm and excitement to learn!". A green button at the bottom left says "► Resume Learning".

### 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**

Offensive Security

Correct Answer

#### 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

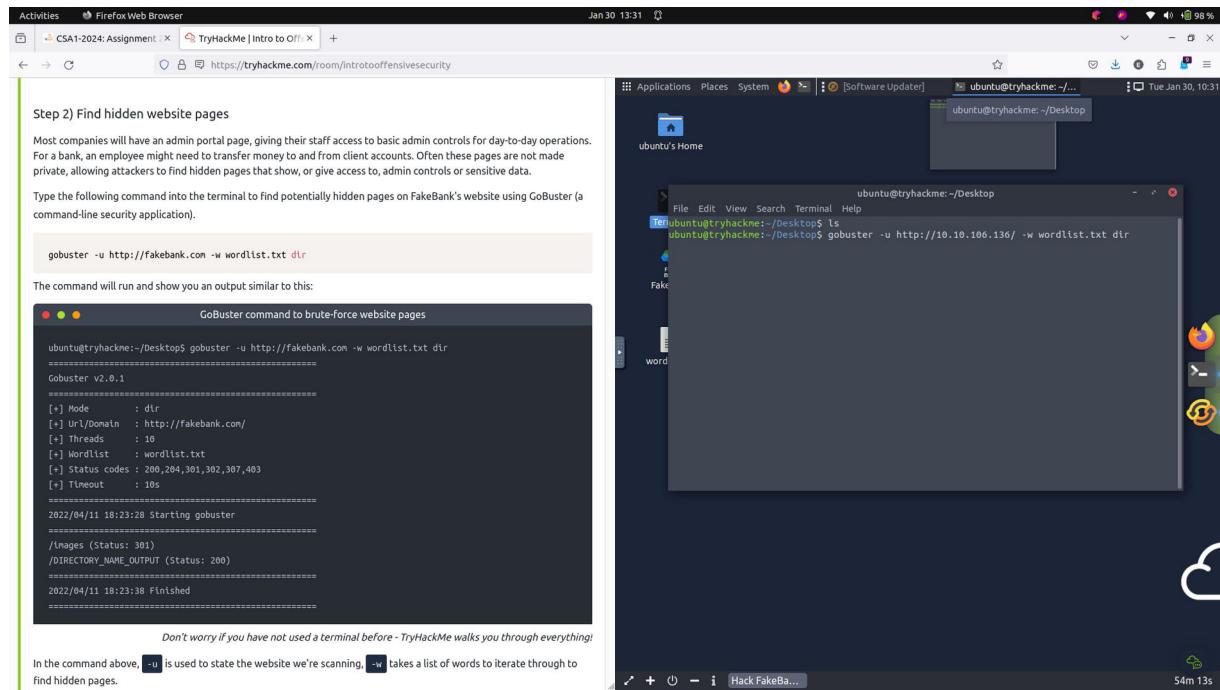
► Start Machine

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

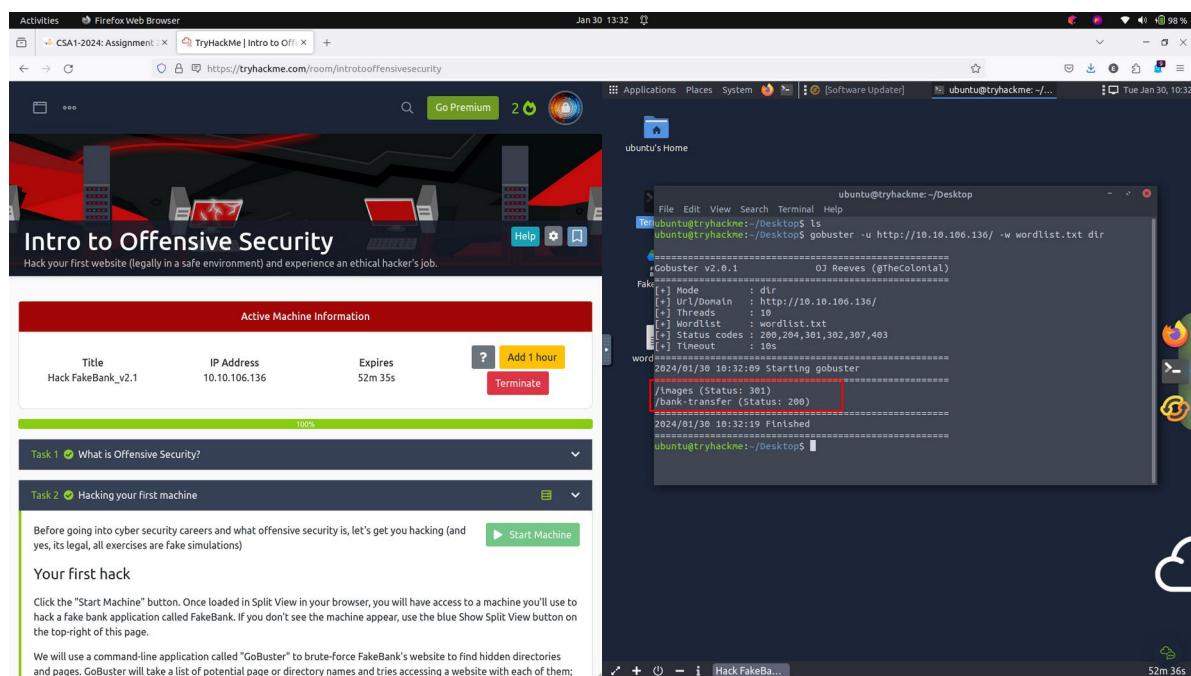
3. Run gobuster tool on the terminal to unveil hidden pages in from the target

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).

A screenshot of a Linux desktop environment. On the left, a terminal window shows the output of a Gobuster scan for the URL `http://fakebank.com/`. The results indicate that the path `/bank-transfer` was found with a status code of 200. On the right, a Firefox browser window displays the `FakeBank | Bank Transfer` page at `10.10.106.136/bank-transfer`. The page features a brown header with the `Fake Bank` logo and navigation links for "Our Products & Services" and "Safe & Secure Internet Banking". Below the header, a section titled "Staff Account" includes a sub-section for "Admin Portal". This portal form has fields for "Send from" (set to 2276), "Send to" (set to 8881), and "Amount to send in USD" (set to 2000). A red box highlights the "Send Money" button.

A screenshot of a Linux desktop environment, similar to the previous one. The terminal window on the left shows the same Gobuster scan results, with the `/bank-transfer` page being highlighted by a red arrow. The Firefox browser window on the right shows the `FakeBank | Bank Transfer` page. In this view, the "Admin Portal" form has been submitted, and a success message is displayed: "Success, transfer completed. You have successfully completed the transfer, here are the details for reference:". The transferred amount is listed as 123, the currency as 2000 USD, and the date of transfer as 2024-01-30. A red box highlights the "Return to Your Account" button.

## 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**

The screenshot shows a Firefox browser window with two tabs open. The left tab displays terminal output from the command-line tool Gobuster, which has found several pages on the target website. The right tab shows a 'FakeBank' account page for 'Mrs G. Benjamin' with a balance of \$767.68. A red box highlights a message box stating 'Congratulations - you hacked the bank! The answer to the TryHackMe question is BANK-HACKED'. Below the message, the account balance is listed as '\$767.68'.

This screenshot is similar to the previous one, but it includes a red box around the 'Correct Answer' button in the bottom-left corner of the challenge interface. This indicates that the user has successfully answered the question correctly.

## 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.**

A screenshot of a Firefox browser window showing the TryHackMe Learning Path interface. The path is titled 'Introduction to Cyber Security'. It includes modules like 'Intro to Offensive Security' (Free), 'Intro to Defensive Security' (VIP), and 'Careers in Cyber'. A red box highlights the 'Intro to Defensive Security' module. To the right, there's a 'Learning Scheduler' section where users can input study hours and a 'Schedule this course' button. Below it is a 'Certificate' section showing a progress bar at 12%.

## Introduction to Offensive Security.

A screenshot of a Firefox browser window showing the TryHackMe Learning Path interface. The path is titled 'Introduction to Offensive Security'. It includes modules like 'Web Application Security' (Free), 'Operating System Security' (VIP), and 'Network Security' (VIP). A red box highlights the 'Web Application Security' module. To the right, there's a 'Learning Scheduler' section where users can input study hours and a 'Schedule this course' button. Below it is a 'Certificate' section showing a progress bar at 12%.

## Task 1: Web Application Security.

Web Application Security  
Learn about web applications and explore some of their common security issues.

Task 1 Introduction

Every one of us uses different programs on our computers. Generally speaking, programs run on our computers, using our computer's processing power and storage. Moreover, to use a program, we need to install it first. What if we can use any program without installation?

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

It's 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: Browser**

Online Shopping Web Application

Products Database

Customers Database

Sales Database

Many companies offer bug bounty programs. A bug bounty program allows the company to offer a reward for anyone who discovers a security vulnerability (weakness) in the company's systems. The main condition is that the found vulnerability is within the bug bounty scope and rules. Among many others, Google, Microsoft, and Facebook have bug bounty programs. Discovering a bug can earn you from a few hundred USD to tens of thousands of USD, depending on the severity of the vulnerability, i.e., the weakness you discovered.

Answer the questions below

What do you need to access a web application?

Correct Answer

Task 2 Web Application Security Risks

Task 3 Practical Example of Web Application Security

Created by [tryhackme](#) and [strategos](#)  
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 270948 users are in here and this room is 645 days old.

## Task 2: Web Application Security Risks

Task 2 ○ Web Application Security Risks

Let's say that you want to buy an item from an online shop. There are certain functions that you would expect to be able to do on this web application. Most straightforwardly, the online order might go as follows:

1. Log in on the website 
2. Search for the product
3. Add the product to the shopping cart
4. Specify the shipping address
5. Provide payment details

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 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**

***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?

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

Activities Firefox Web Browser Jan 30 14:17

CSA1-2024: Assignment TryHackMe | Web Application Security

https://tryhackme.com/room/introwebapplicationsecurity

Don't worry if these techniques look challenging or sophisticated at first. TryHackMe has dedicated in-depth rooms to help you understand and experiment with the various attacks against web applications.

***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?

Task 3 Practical Example of Web Application Security

## Task 3: Practical Example of Web Application Security.

The image shows two screenshots from the TryHackMe platform. On the left, the 'Web Application Security' task page is displayed, showing a sidebar with 'Task 1' (Introduction), 'Task 2' (Web Application Security Risks), and 'Task 3' (Practical Example of Web Application Security). The main content area discusses IDOR (Insecure Direct Object References) under the category of Broken Access Control. It mentions that an attacker can access information or perform actions not intended for them by manipulating object IDs. A 'View Site' button is present. On the right, the 'Inventory Management System' page is shown at the URL <https://inventory-management.thm/>. This page has tabs for Main, Planned Shipments, Inventory, and Your Activity. The 'Planned Shipments' tab is active, displaying images of various vehicles: a bicycle, a scooter, a motorcycle, and another bicycle. A sidebar on the left of this page is titled 'Beginner IDOR'.

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=11)

Activities Firefox Web Browser Jan 30 14:30

CSA1-2024: Assignment TryHackMe | Web Application

has permission to access a photo named `IMG_1003.JPG`. We might guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page <https://store.tryhackme.thm/products/product?id=52>. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL <https://store.tryhackme.thm/customers/user?id=16> would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

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.

**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?

Answer format: \*\*\*{\*\*\*\*\*}

Created by  tryhackme and  strategos

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 270961 users are in here and this room is 645 days old.

Activities Firefox Web Browser Jan 30 14:30

CSA1-2024: Assignment TryHackMe | Web Application

Instructions

This inventory management system manages all the shipments related to tires. A competitor sent a group of malicious actors to sabotage our logistics. The attackers used the account of one of the employees and mixed up the planned shipments. If incorrect shipments are sent, production will be delayed.

https://inventory-management.thm/activity?user\_id=11

Main Planned Shipments Inventory Your Activity

Inventory Management System

Your Activity

Employee Id: 11

Name: Roddy

Position: Warehouse Supervisor

No Recent Activity

Beginner IDOR

## [https://inventory-management.thm/activity?user\\_id=10](https://inventory-management.thm/activity?user_id=10)

Activities Firefox Web Browser Jan 30 14:31

CSA1-2024: Assignment TryHackMe | Web Application

has permission to access a photo named `IMG_1003.JPG`. We might guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page <https://store.tryhackme.thm/products/product?id=52>. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL <https://store.tryhackme.thm/customers/user?id=16> would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

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.

**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?

Answer format: \*\*\*{\*\*\*\*\*}

Created by  tryhackme and  strategos

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 270961 users are in here and this room is 645 days old.

Activities Firefox Web Browser Jan 30 14:31

CSA1-2024: Assignment TryHackMe | Web Application

Instructions

This inventory management system manages all the shipments related to tires. A competitor sent a group of malicious actors to sabotage our logistics. The attackers used the account of one of the employees and mixed up the planned shipments. If incorrect shipments are sent, production will be delayed.

https://inventory-management.thm/activity?user\_id=10

Main Planned Shipments Inventory Your Activity

Inventory Management System

Your Activity

Employee Id: 10

Name: Anton

Position: Warehouse Supervisor

No Recent Activity

Beginner IDOR

## [https://inventory-management.thm/activity?user\\_id=9](https://inventory-management.thm/activity?user_id=9)

Activities Firefox Web Browser Jan 30 14:32

CSA1-2024: Assignment TryHackMe | Web Application security

has permission to access a photo named `IMG_1003.JPG`. We might guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page <https://store.tryhackme.thm/products/product?id=52>. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL <https://store.tryhackme.thm/customers/user?id=16> would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

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.

**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?

Answer format: \*\*\*{\*\*\*\*\*}

Created by  tryhackme and  strategos

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 270961 users are in here and this room is 645 days old.

Instructions

This inventory management system manages all the shipments related to tires. A competitor sent a group of malicious actors to sabotage our logistics. The attackers used the account of one of the employees and mixed up the planned shipments. If incorrect shipments are sent, production will be delayed.

Inventory Management System

Your Activity

Employee Id: 9  
Name: Alya  
Position: Database Administrator

Type	Data	Action
SKU Change	Inventory SKU0013 Changed	Revert
SKU Change	Inventory SKU0015 Changed	Revert
SKU Change	Inventory SKU0233 Changed	Revert
SKU Change	Inventory SKU0237 Changed	Revert
SKU Change	Inventory SKU0522 Changed	Revert
SKU Change	Inventory SKU0524 Changed	Revert

Beginner IDOR

## Lets revert all changes made.

Activities Firefox Web Browser Jan 30 14:33

CSA1-2024: Assignment TryHackMe | Web Application security

has permission to access a photo named `IMG_1003.JPG`. We might guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page <https://store.tryhackme.thm/products/product?id=52>. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL <https://store.tryhackme.thm/customers/user?id=16> would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

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.

**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?

Answer format: \*\*\*{\*\*\*\*\*}

Created by  tryhackme and  strategos

This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 270961 users are in here and this room is 645 days old.

Instructions

This inventory management system manages all the shipments related to tires. Alya fixed the Inventory Management System!

THM{IDOR\_EXPLORED}

Alya  
Database Administrator

Type Data Action

Beginner IDOR

## Task 1: Introduction to Digital Forensics.

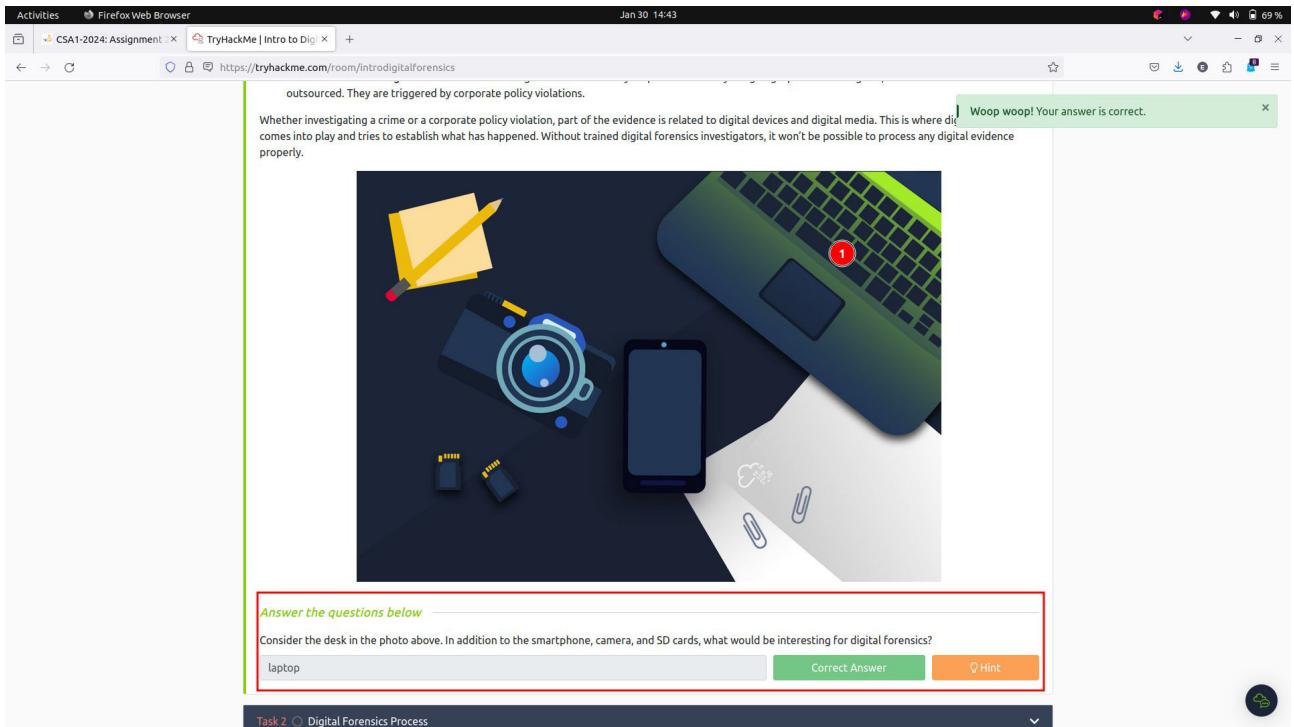


The screenshot shows the TryHackMe platform interface. At the top, there's a navigation bar with 'Activities', 'CSA1-2024: Assignment.', 'TryHackMe | Intro to Dig...', and a '+' button. The date 'Jan 30 14:40' is at the top right. Below the bar, there's a dark-themed header with the TryHackMe logo, a 'Dashboard' button, 'Learn' button, 'Compete' button, 'Other' button, 'Access Machines' button, a search icon, a notification bell, a 'Go Premium' button, and a user icon. The main content area has a banner for 'Intro to Digital Forensics' with a magnifying glass icon and the text 'Learn about digital forensics and related processes and experiment with a practical example.' There are also 'Start AttackBox', 'Help', 'Settings', and 'Bookmarks' buttons.

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.

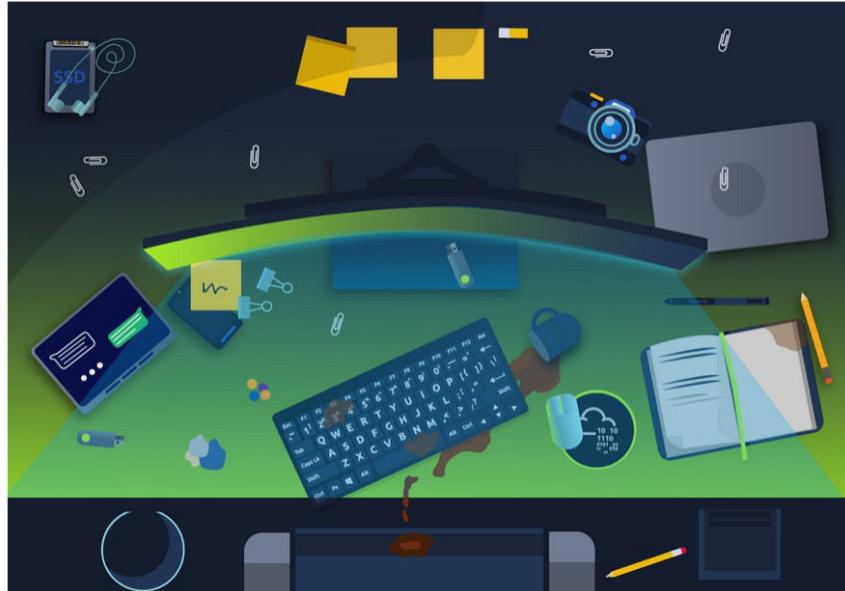
### Answer the questions below

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**



The screenshot shows the TryHackMe platform interface for the 'Intro to Digital Forensics' room. The question asks: "Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics?" A red box highlights the input field where the user typed 'laptop'. To the right of the input field are 'Correct Answer' and 'Hint' buttons. Above the input field, a green box displays the message 'Woop woop! Your answer is correct.' The background features a stylized illustration of a desk with a laptop, smartphone, camera, and other office items.

## 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**

Activities Firefox Web Browser Jan 30 14:48

CSA1-2024: Assignment TryHackMe | Intro to Digi + https://tryhackme.com/room/introdigitalforensics

As a digital forensics investigator, you arrive at a scene similar to the one shown in the image above. What should you do as a digital forensics investigator? Woop woop! Your answer is correct.

1. Acquire the evidence: Collect the digital devices such as laptops, storage devices, and digital cameras. (Note that laptops and computers require special handling if they are turned on; however, this is outside the scope of this room.)  
2. Establish a chain of custody: Fill out the related form appropriately ([Sample form](#)). The purpose is to ensure that only the authorized investigators had access to the evidence and no one could have tampered with it.  
3. Place the evidence in a secure container: You want to ensure that the evidence does not get damaged. In the case of smartphones, you want to ensure that they cannot access the network, so they don't get wiped remotely.  
4. Transport the evidence to your digital forensics lab.

At the lab, the process goes as follows:

1. Retrieve the digital evidence from the secure container.
2. Create a forensic copy of the evidence: The forensic copy requires advanced software to avoid modifying the original data.
3. Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you can always create a new one.
4. Start processing the copy on your forensics workstation.

The above steps have been adapted from [Guide to Computer Forensics and Investigations, 6th Edition](#).

More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:

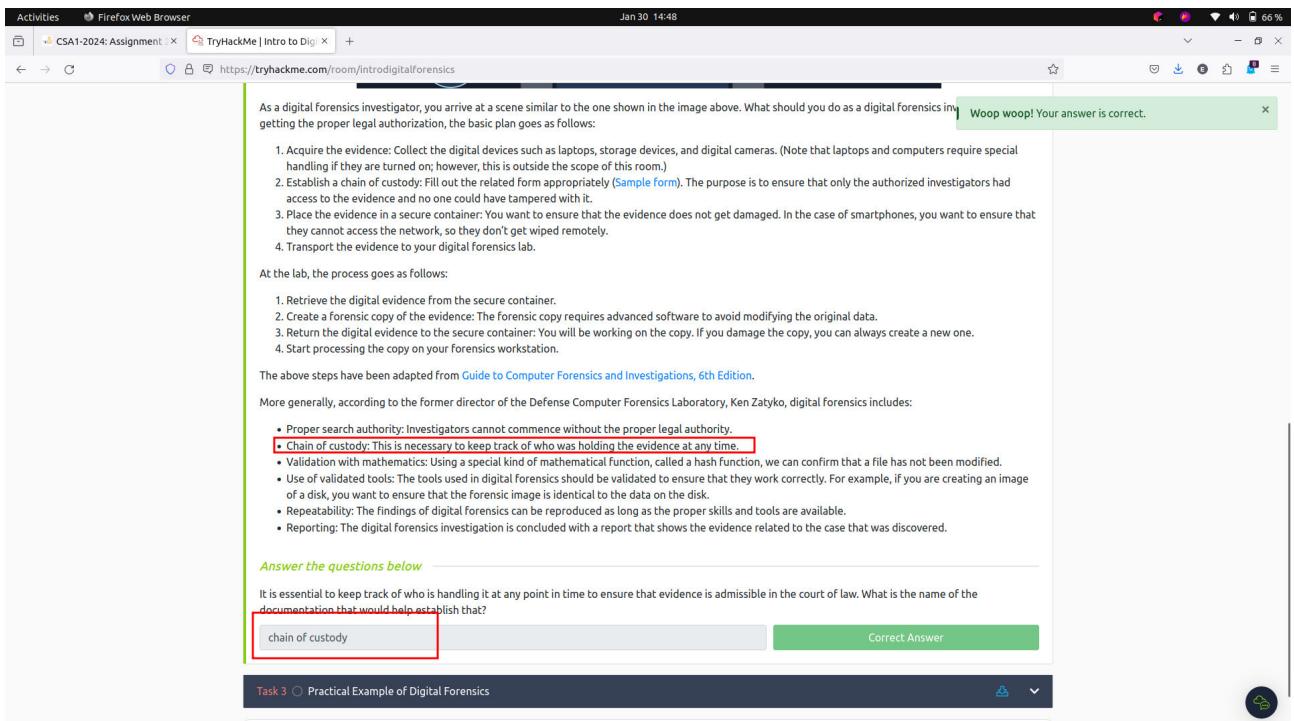
- Proper search authority: Investigators cannot commence without the proper legal authority.
- Chain of custody: This is necessary to keep track of who was holding the evidence at any time.
- Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm 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?

chain of custody chain of custody Correct Answer

Task 3 ○ Practical Example of Digital Forensics



## Task 3: Practical Example of Digital Forensics

Activities Firefox Web Browser Jan 30 14:54

CSA1-2024: Assignment TryHackMe | Intro to Digi + https://tryhackme.com/room/introdigitalforensics

Try Hack Me Dashboard Learn Compete Other Access Machines Go Premium 2 🔒

Intro to Digital Forensics 3198 Learn about digital forensics and related processes and experiment with a practical example.

40% Task 1 ✓ Introduction To Digital Forensics

Task 2 ✓ Digital Forensics Process

Task 3 ○ Practical Example of Digital Forensics

Everything we do on our digital devices, from smartphones to computers, leaves traces. Let's see how we can use this in the [Download Task Files](#)



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.

```

Archive: ransomletter2.zip
  inflating: letter-image.jpg
  inflating: ransom-letter.doc
  inflating: ransom-letter.pdf
  inflating: ransom-letter2.zip
  inflating: Sample report.pdf
root@coderic:~/Downloads (master)~ ls
PTI_MAIN_CAMPUS_TT_JAN-APRIL.xlsx
ransom-letter.doc
ransom-letter.pdf
ransomletter2.zip
Sample report.pdf

```

**Document Metadata**

When you create a text file, some metadata gets saved within the file's metadata when you open it. This information gets kept within the file's metadata when you might open them within their official viewer/editor or use a suitable forensic tool. Note that exporting the file to other formats, such as PDF, would maintain most of the metadata of the original document, depending on the PDF writer used.

Let's see what we can learn from the PDF file. We can try to read the metadata using the program pdfinfo. Pdfinfo displays various metadata related to a PDF file, such as title, subject, author, creator, and creation date. (The AttackBox already has pdfinfo installed; however, if you are using Kali Linux and don't have pdfinfo installed, you can install it using sudo apt install poppler-utils.) Consider the following example of using pdfinfo DOCUMENT.pdf

```

user@TryHackMe$ pdfinfo DOCUMENT.pdf
Creator: Microsoft Word for Office 365
Producer: Microsoft Word for Office 365
CreationDate: Wed Oct 10 21:47:53 2018 EEST
ModDate: Wed Oct 10 21:47:53 2018 EEST
Tagged: yes
UserProperties: no
Suspects: no
Form: none
JavaScript: no

```

## 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

```

fish /home/coderic/Downloads
'yt2mate.com - URBAN REGGEA GOSPEL VIDEO MIX 2024 DJ MACDEE.mp3'
Projects
'pst Fred Anniversary'
coderic@coderic-ThinkPad-X1-Carbon-4th ~/Downloads (master)> pdfinfo ransom-letter.pdf
Title: Pay NOW
Subject: We Have Gato
Author: Ann Gree Shepherd
Creator: Microsoft® Word 2016
Producer: Microsoft® Word 2016
CreationDate: Wed Feb 23 12:10:36 2022 EAT
ModDate: Wed Feb 23 12:10:36 2022 EAT
Custom Metadata: no
Metadata Stream: yes
Tagged: yes
UserProperties: no
Suspects: no
Form: none
JavaScript: no
Pages: 1
Encrypted: no
Page size: 595.44 x 842.04 pts (A4)
Page rot: 0
File size: 71371 bytes
Optimized: no
PDF version: 1.7
coderic@coderic-ThinkPad-X1-Carbon-4th ~/Downloads (master)>

```

**Answer the questions below**

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

Ann Grie Shepherd

Correct Answer

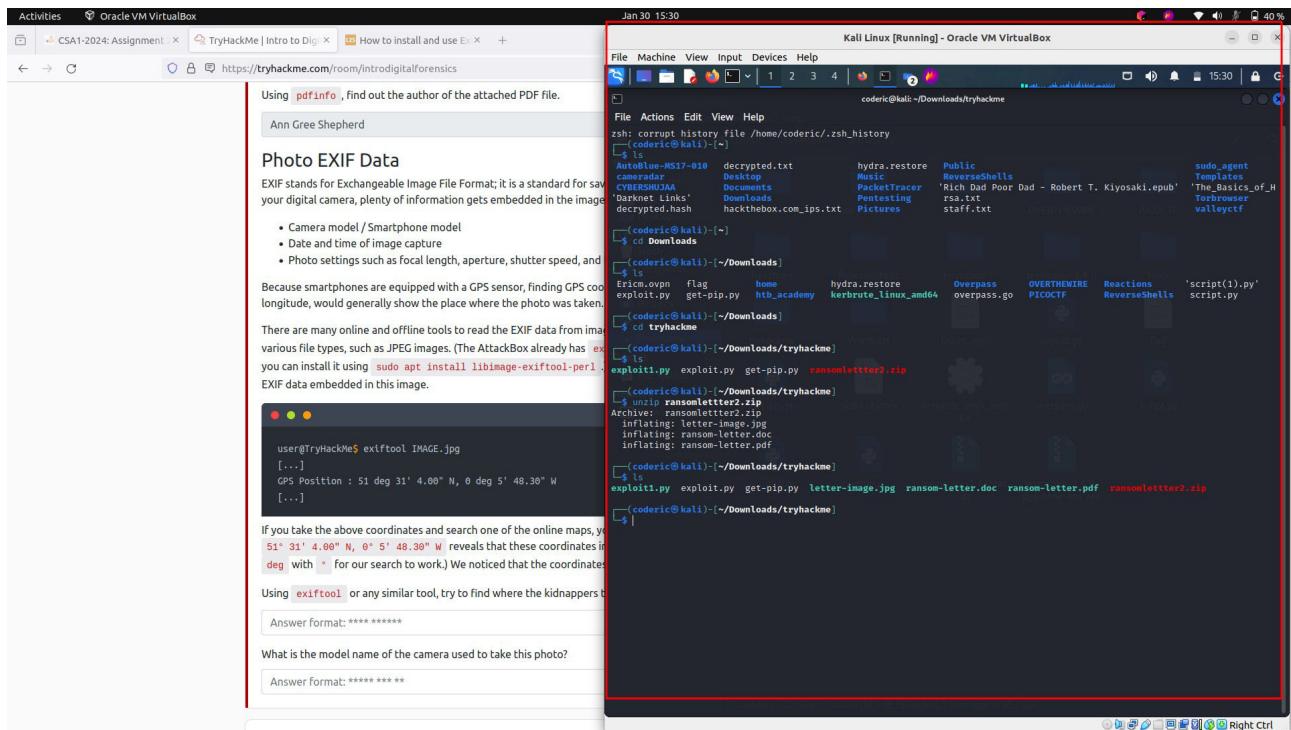
## Photo EXIF Data

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:- **exittool letter-image.jpg**

```

File Machine View Input Devices Help
File Actions Edit View Help
exploit.py exploit.py get-pip.py ransomletter2.zip
(coderic㉿kali):~/Downloads/tryhackme$ ls
exploit.py exploit.py get-pip.py letter-image.jpg ransom-letter.doc ransom-letter.pdf ransomletter2.zip
(coderic㉿kali):~/Downloads/tryhackme$ exiftool letter-image.jpg
ExifTool Version Number : 12.57
File Name : letter-image.jpg
Directory : .
File Size : 127 kB
File Modification Date/Time : 2022:02:25 11:53:53+03:00
File Access Date/Time : 2022:02:25 11:53:53+03:00
File Inode Change Date/Time : 2024:01:30 10:29:21+03:00
File Permissions : rwxr-xr-x
File Type : JPEG
File Extension : jpg
MIME Type : image/jpeg
JFIF Version : 1.01
Exif Byte Order : Little-endian (Intel, II)
Compression : JPEG (old-style)
Make : Canon
Camera Model Name : Canon EOS R6
Orientation : Horizontal (normal)
X Resolution : 300
Y Resolution : 200
Resolution Unit : inches
Software : GIMP 2.10.28
Modify Date : 2022:02:19 17:23:40
Exposure Program : Manual
F Number : 2.8
Exposure Compensation : 0
Recommended Exposure Index : 640
Exif Version : 0231
Date/Time Original : 2022:02:25 13:37:33
Create Date : 2022:02:25 13:37:33
Offset Time : +01:00
Offset Time Original : +03:00
Offset Time Digitized : +03:00
Shutter Speed Value : 1/200
Aperture Value : 2.8
Exposure Compensation : 0
Max Aperture Value : 1.0
Metering Mode : Multi-segment

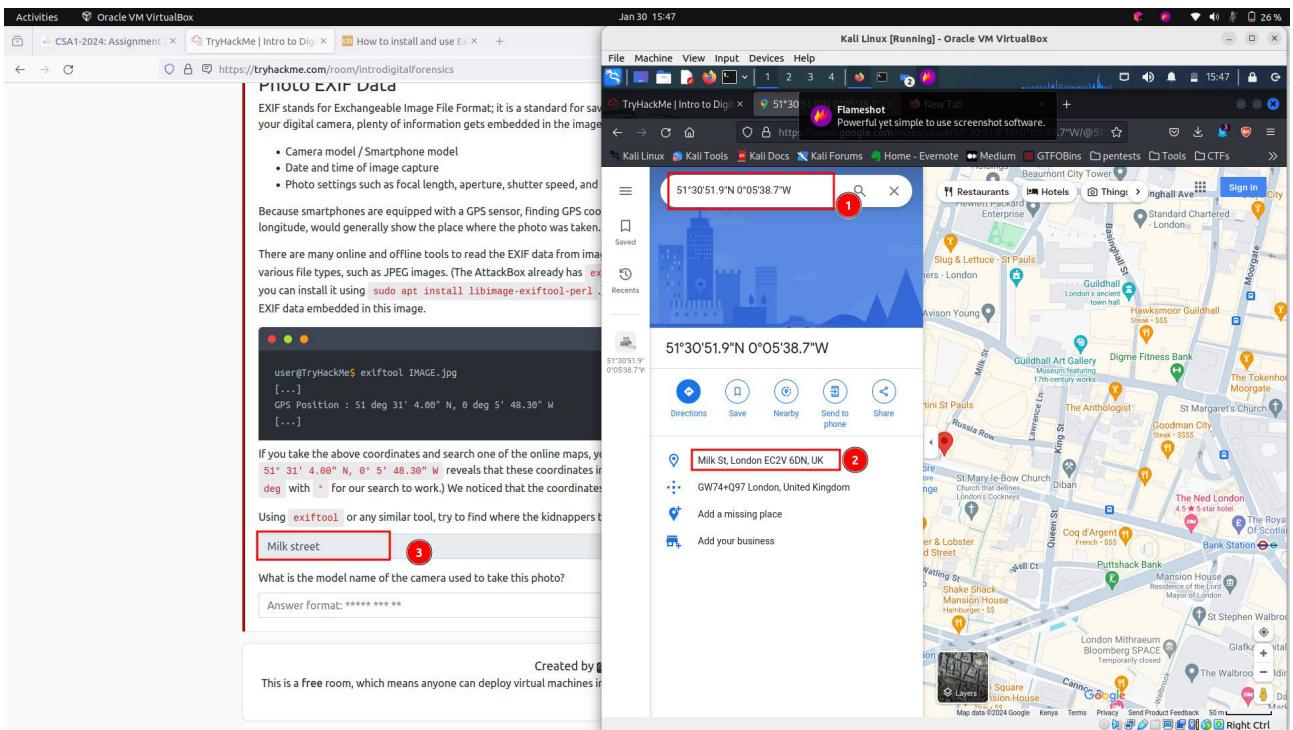
```

## 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.

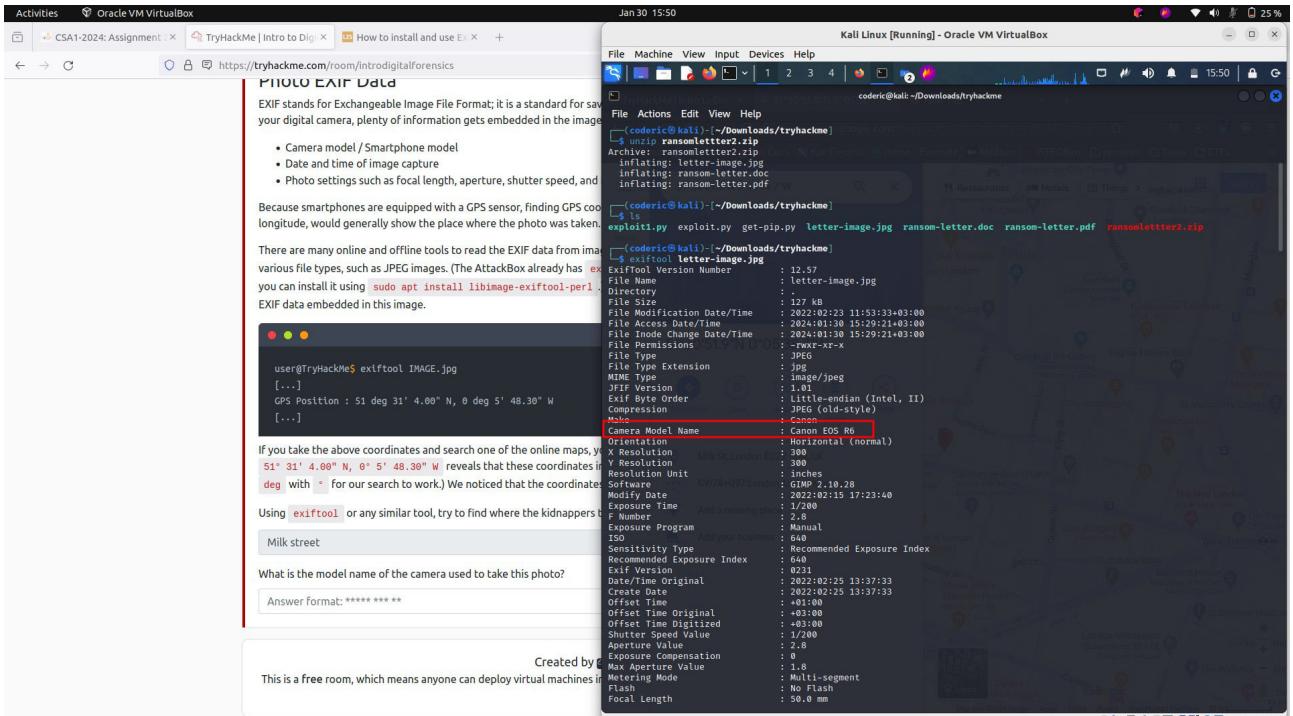
GPS Position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W



- 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.**