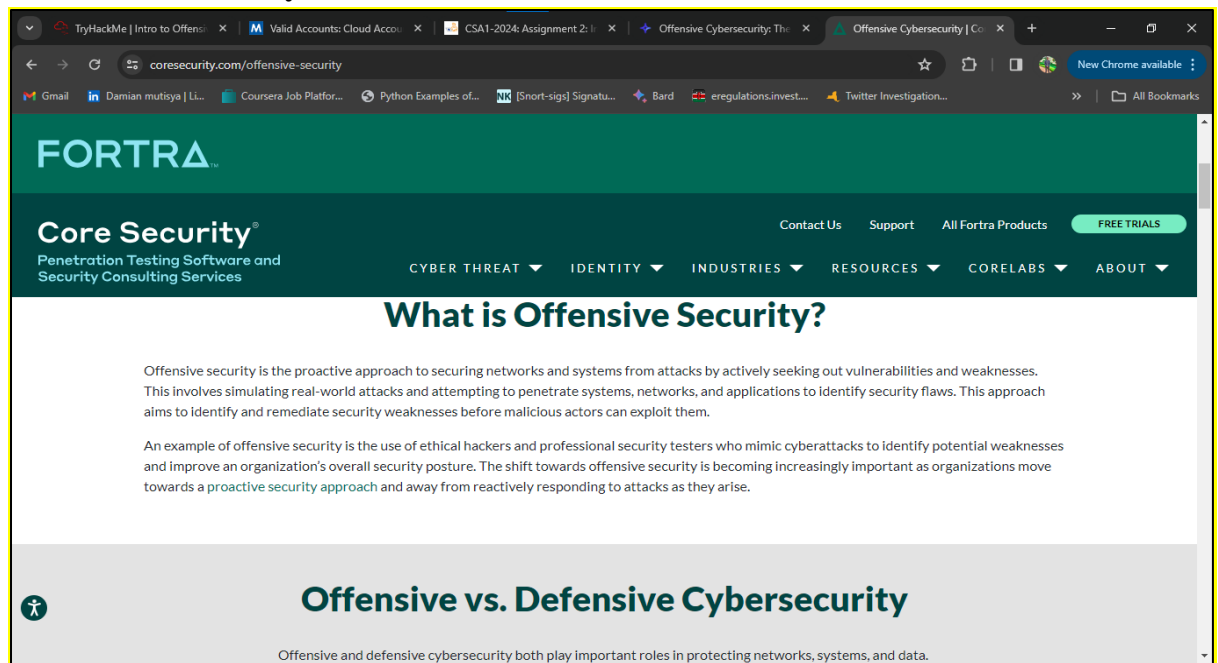


1. Intro to Offensive Security

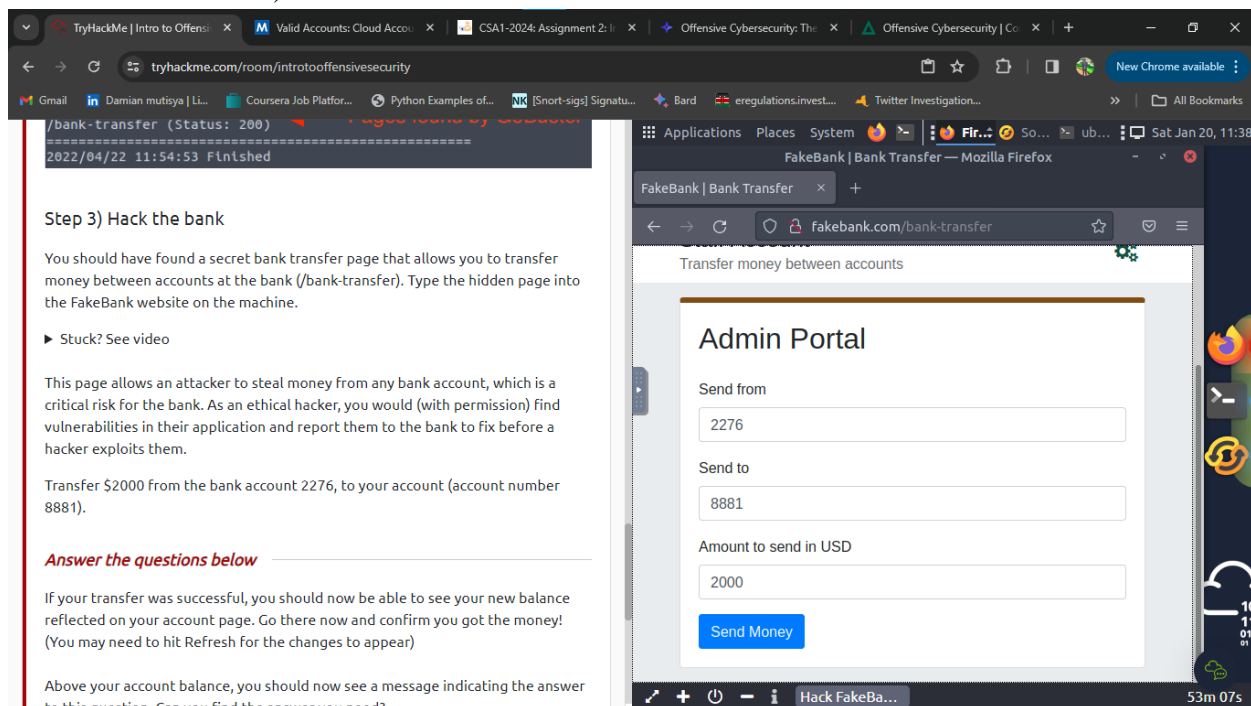
Concept Overview: Offensive security involves proactive measures to find vulnerabilities in systems by simulating hacker's actions. It's an essential part of cybersecurity, aiming to identify and fix security holes before they can be exploited maliciously.

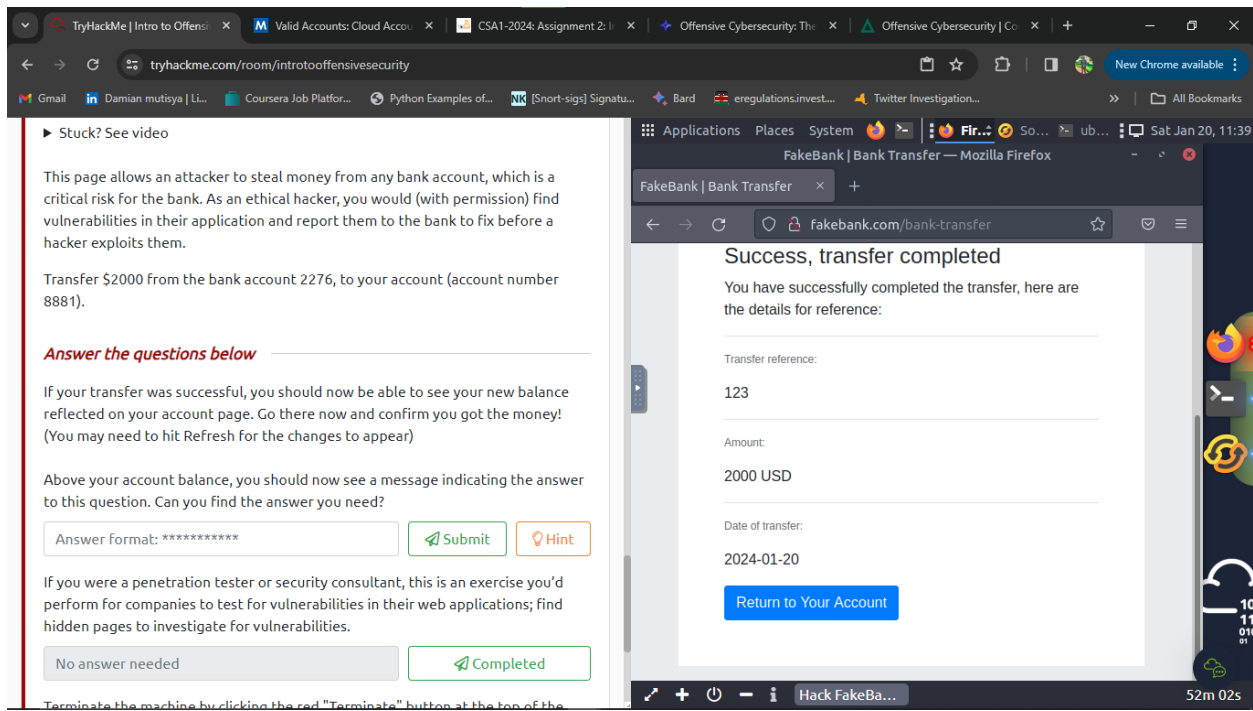
Key Questions and Answers:

- Q: Which option better represents the process of simulating a hacker's actions to find vulnerabilities?
 - A. Offensive Security
 - B. Defensive Security
- A: Offensive Security

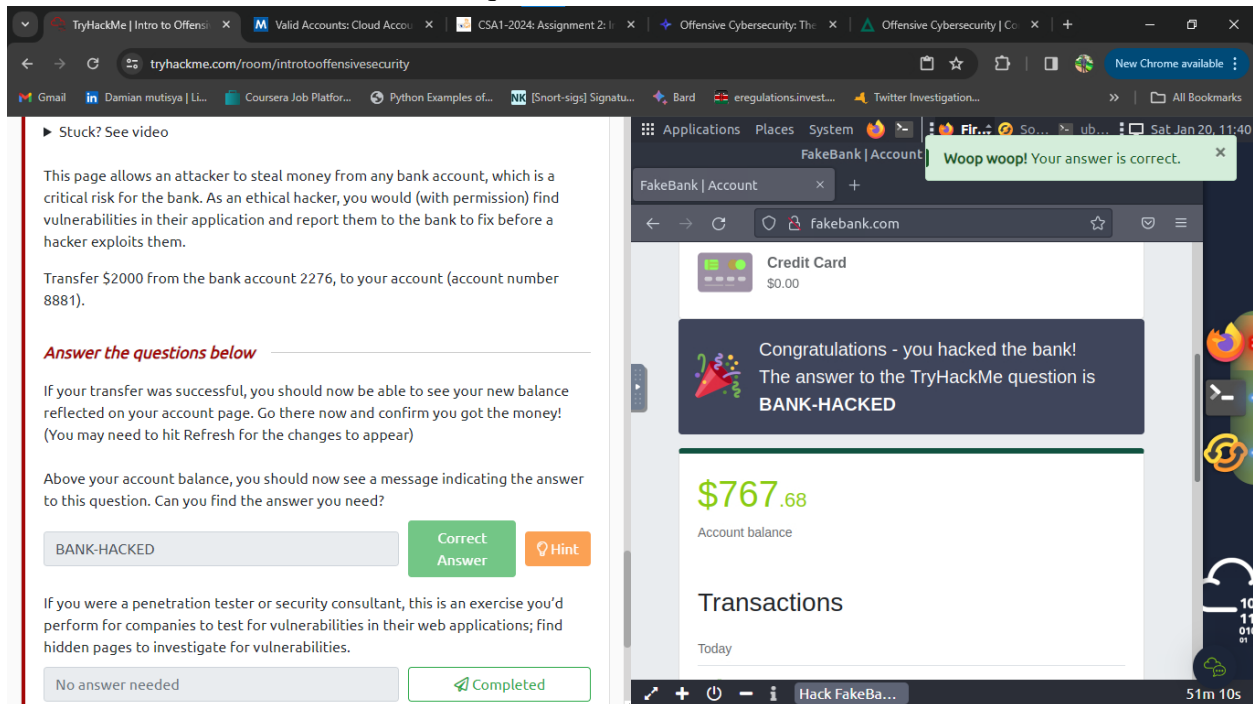


- Q: What is the indication of a successful transfer in the simulated bank hack scenario?
 - A: The message "BANK-HACKED" above the account balance.
- Transfer \$2000 from the bank account 2276, to your account (account number 8881).





- Above your account balance, you should now see a message indicating the answer to this question.



2. Web Application Security

Concept Overview: Web application security focuses on protecting websites and online services against different security threats that exploit vulnerabilities in an application's code. It's crucial for maintaining the confidentiality, integrity, and availability of web services.

Key Questions and Answers:

- Q: What do you need to access a web application?
 - **A: Browser**

The screenshot shows the Riverbed website. The header includes the Riverbed logo and navigation links: PRODUCTS, SOLUTIONS, CUSTOMERS, PARTNERS, RESOURCES, COMPANY. There are also buttons for 'REQUEST DEMO' and 'CONTACT US'. The main content area is titled 'Defining web applications' and contains the following text: 'In computer system, a web application is a client-side and server-side software application in which the client runs or request in a web browser. Common web applications include email, online retail sales, online auctions, wikis, instant messaging services and more. Many companies are shifting their focus to web applications that can be delivered as Software-as-a-Service (SaaS), such as moving to Microsoft 365.' Below this, a section titled 'How a web application works step-by-step' lists three steps: 'Step 1: The user accesses a web application via a web browser or mobile application, triggering a request to the web server over the Internet. Note that there may be security measures (i.e. firewalls or cloud access security brokers) and load balancers.' 'Step 2: The web server forwards the request to the web application server. The web application server performs the requested task – such as querying the database or processing the data – then generates the results of the requested data.' 'Step 3: The web application server sends the results back to the web server.'

- Q: What security risk is identified with unlimited login attempts on a login page?
 - **A: Identification and Authentication Failure**

The screenshot shows a lesson page on TryHackMe titled 'Identification and Authentication Failure'. It includes a green notification box that says 'Woop woop! Your answer is correct.' The main text discusses common attacks against web applications and lists three categories: '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.' '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.' 'Provide payment details: The attacker would check if the payment details are sent in plaintext or using weak encryption. Encryption refers to making the data unreadable without knowing the secret key or password.' Below this, it states 'We cannot cover everything, but we will present a few formal categories from OWASP Top Ten. Don't worry if these techniques sound alien to you; TryHackMe walks you through each vulnerability.' The section 'Identification and Authentication Failure' explains that identification refers to the ability to identify a user uniquely, while authentication refers to the ability to prove that the user is whom they claim to be. It notes that an online shop must confirm the user's identity and authenticate them before they can use the system, and that this step is prone to different types of weaknesses. Example weaknesses include: 'Allowing the attacker to use brute force, i.e., try many passwords, usually using automated tools, to find valid login credentials.' 'Allowing the user to choose a weak password. A weak password is usually easy to guess.' 'Storing the users' passwords in plain text. If the attacker manages to read the file containing the passwords, we don't want them to be able to learn the stored password.'

Username	Password
Anne	freedom1

- Q: What security risk is present when username and password are sent in cleartext?

• A: Cryptographic Failures

An injection attack refers to a vulnerability in the web application where the user can insert malicious code as part of their input. This is the lack of proper validation and sanitization of the user's input.

Cryptographic Failures

This category refers to the failures related to cryptography. Cryptography focuses on 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. In other words, encryption ensures that no one can read the data without knowing the secret key. Decryption converts the ciphertext back into the original cleartext using the secret key. Examples of cryptographic failures include:

- Sending sensitive data in clear text, for example, using HTTP instead of HTTPS. HTTP is the protocol used to access the web, while HTTPS is the secure version of HTTP. Others can read everything you send over HTTP, but not HTTPS.
- Relying on a weak cryptographic algorithm. One old cryptographic algorithm is to shift each letter by one. For instance, "TRY HACK ME" becomes "USZ IBDL NF." This cryptographic algorithm is trivial to break.
- Using default or weak keys for cryptographic functions. It won't be challenging to break the encryption that used 1234 as the secret key.

- Q: After reverting malicious changes made by another user, what is the flag received?
- A: THM{IDOR_EXPLORED}

Question Hint

On the site on the right, click "Your Activity" and try to enter numbers between 5 and 10 instead of 11 in the user_id=11.

Entered user id number 5 but there was no user with that id.

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)! 267201 users are in here and this room is 635 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.

[Main](#) [Planned Shipments](#) [Inventory](#) [Your Activity](#)

Inventory Management System

User Not Found

[Beginner IDOR](#)

Entered user id number 10 with name Anton but he had no recent activity which meant he didn't tamper with the database.

TryHackMe | Web Ap... x Valid Accounts: Clou... x Web Application Vs... x Bard x How Does a Web Ap... x What is Web Applica... x +

tryhackme.com/room/introwebapplicationsecurity

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)! 267201 users are in here and this room is 635 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.

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

Finally entered user_id 9 which gave me credentials for the database administrator and was able to reverse but the changes made on the database.

TryHackMe | Web Ap... x Valid Accounts: Clou... x Web Application Vs... x Bard x How Does a Web Ap... x What is Web Applica... x +

tryhackme.com/room/introwebapplicationsecurity

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)! 267201 users are in here and this room is 635 days old.

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=9

Main Planned Shipments Inventory Your Activity

Inventory Management System

Your Activity

Employee Id: 9
Name: Alya
Position: Database Administrator

Type	Data	Action
SKU Change	Inventory SKU0013 Changed	<input type="button" value="Revert"/>
SKU Change	Inventory SKU0015 Changed	<input type="button" value="Revert"/>
SKU Change	Inventory SKU0253 Changed	<input type="button" value="Revert"/>
SKU Change	Inventory SKU0257 Changed	<input type="button" value="Revert"/>
SKU Change	Inventory SKU0522 Changed	<input type="button" value="Revert"/>
SKU Change	Inventory SKU0524 Changed	<input type="button" value="Revert"/>

Beginner IDOR

Finally, after reverting the changes was able to get the flag as shown below.

TryHackMe | Web Ap...Valid Accounts: Cloud...Web Application Vs...BardHow Does a Web Ap...What is Web Applica...New Chrome available

tryhackme.com/room/introwebapplicationsecurity

GmailDamian mutiya | Li...Coursera Job Platfor...Python Examples of...[Snort-sigs] Signatu...Barderegulations.invest...Twitter Investigation...All Bookmarks

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?

Correct Answer

Hint


Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 267201 users are in here and this room is 635 days old.

Instructions


This inventory management system manages all the shipmen... group of
malicious attackers
used the plan
mixed up
re sent,

Alya fixed the Inventory Management System!



THM{IDOR_EXPLORED}

MainPlanned

Alya

Database Administrator

Type	Data	Action
------	------	--------

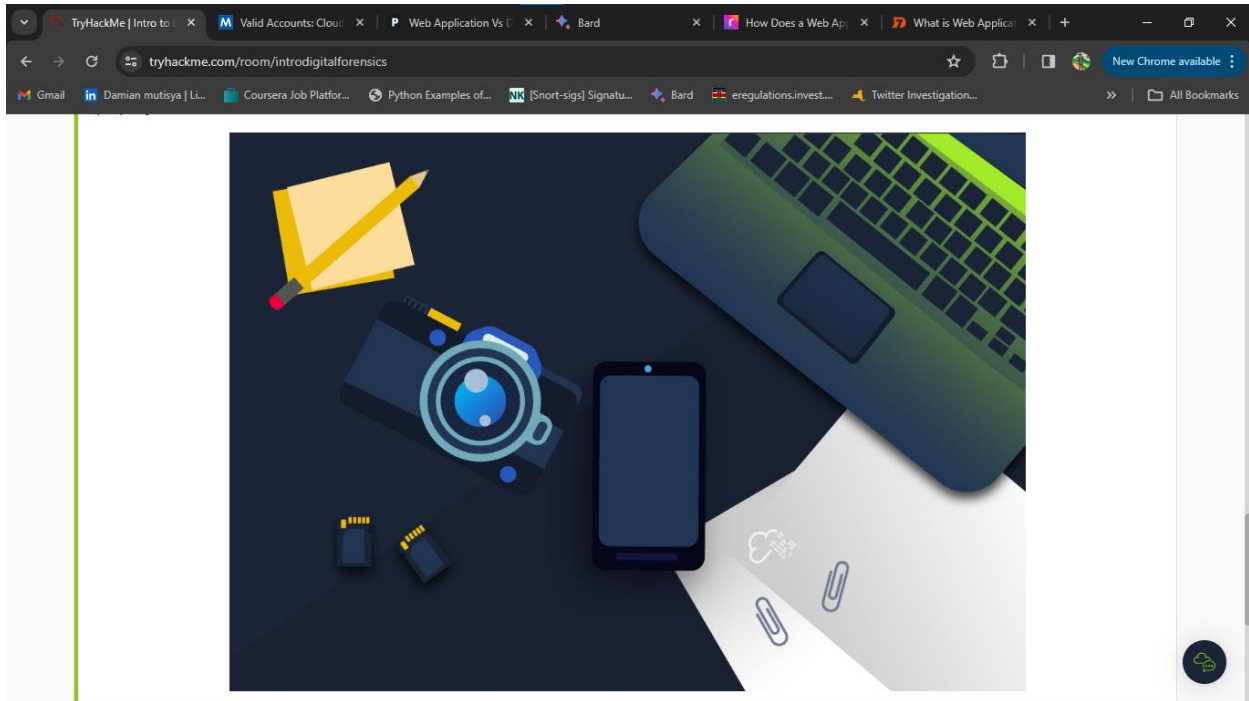
Beginner IDOR

3. Intro to Digital Forensics

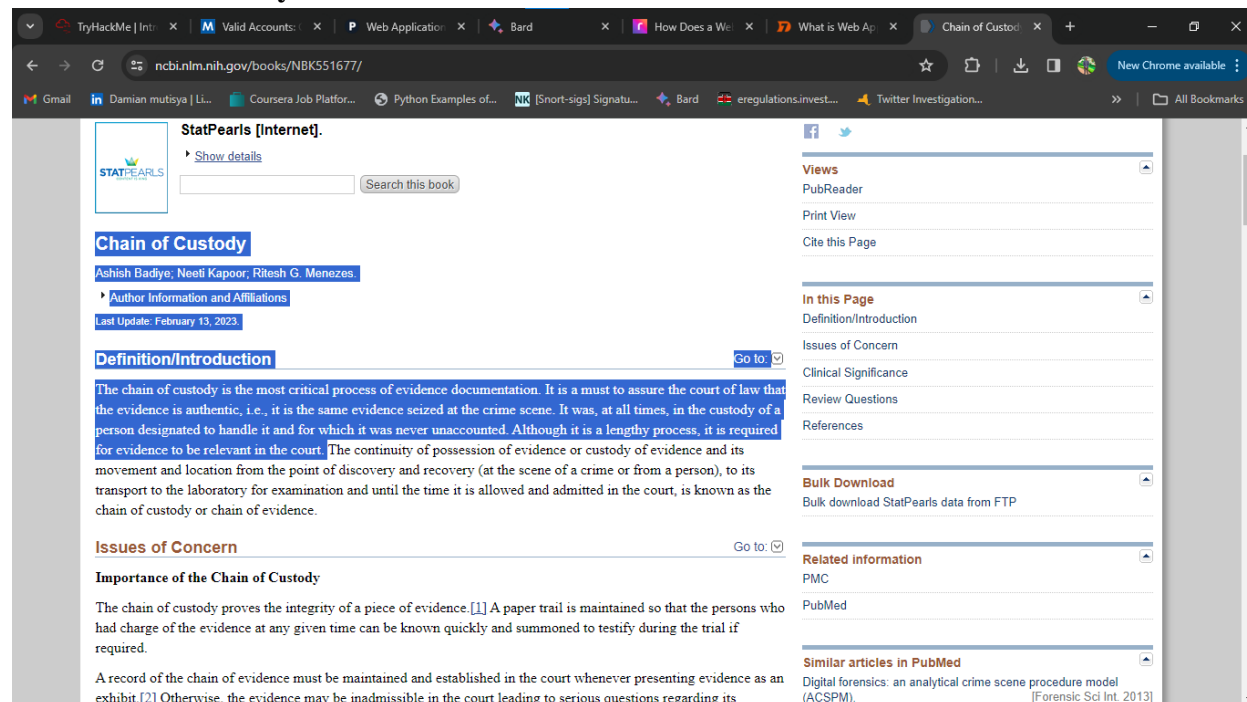
Concept Overview: Digital forensics involves the recovery and investigation of material found in digital devices, often in relation to computer crime. The goal is to preserve the evidence in its most original form while performing a structured investigation.

Key Questions and Answers:

- **Q:** In addition to the smartphone, camera, and SD cards, what is interesting for digital forensics in the provided photo?
- **A: Laptop**

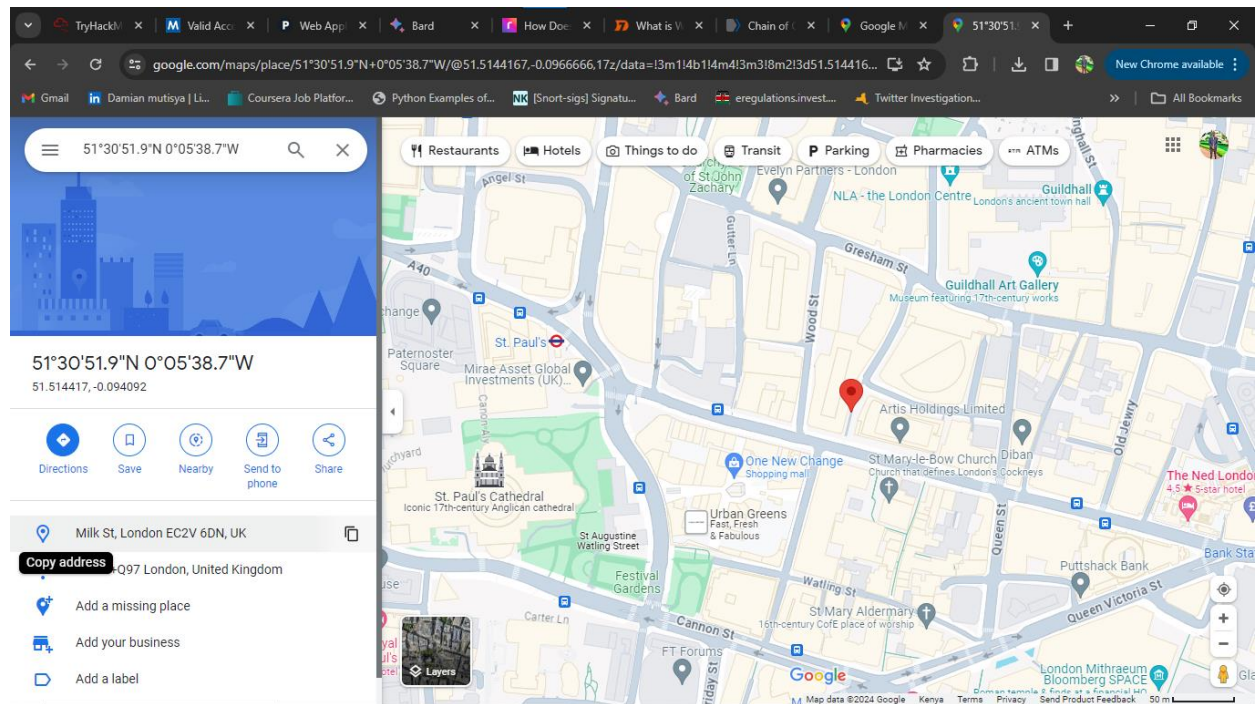


- **Q:** What documentation helps establish the chain of custody for evidence?
- **A: Chain of Custody**

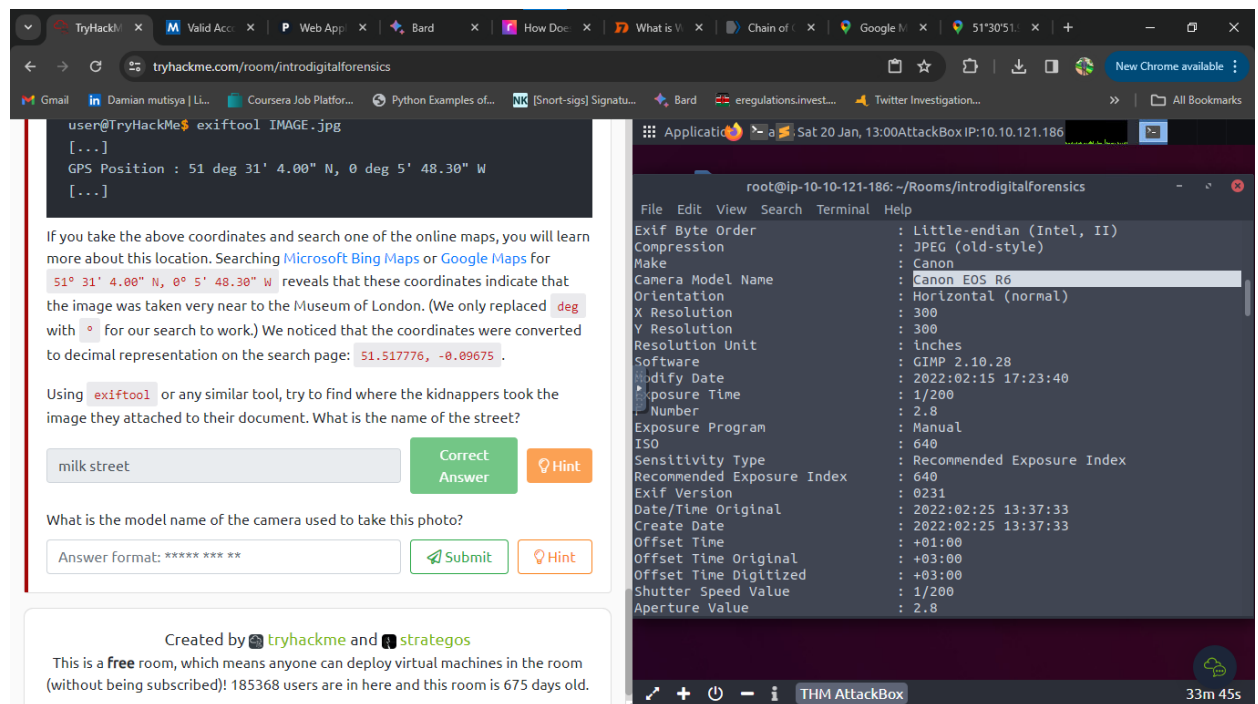


- **Q:** Using a tool like exiftool, what is the identified street where the kidnappers took an image?

- **A: Milk Street**



- **Q: What is the model's name of the camera used to take the photo in question?**
- **A: Canon EOS R6**



Conclusion

Each module of the "Introduction to Cybersecurity" course presents essential aspects of cybersecurity, ranging from offensive strategies to protect systems, to the intricacies of securing web applications and the meticulous nature of digital forensics. Understanding these topics is crucial for anyone pursuing a career in cybersecurity, as they cover foundational concepts and practical skills required in the field.

<https://tryhackme.com/p/Damiano254>

TryHackMe | Damiano254 | CSAT-2024: Assignment 2: Intro | CYBER SHUIJAA ONBOARDING | tryhackme - Google Search

tryhackme.com/p/Damiano254

Gmail | Damian mutiya | Li... | Coursera Job Platfor... | Python Examples of... | [Short-sigs] Signatu... | Bard | eregulations.invest... | Twitter Investigation...

TryHackMe | Dashboard | Learn | Compete | Other

Go Premium

453163 Rank | 5 Rooms Complete | 3 Level | 0 Badges

Damiano254 [0x3]

Get Profile Badge ID | Share Room Badges

Rooms Complete | Badges | Created Rooms | Yearly Activity | Tickets

Web Application...
Learn about web applications and explore...

Intro to Offensiv...
Hack your first website (legally in a safe...)

Intro to Digital...
Learn about digital forensics and related...

MITRE
This room will discuss the various resources MITRE h...

Simple CTF
Beginner level ctf 010

06:13 22/01/2024