Intro to offensive security

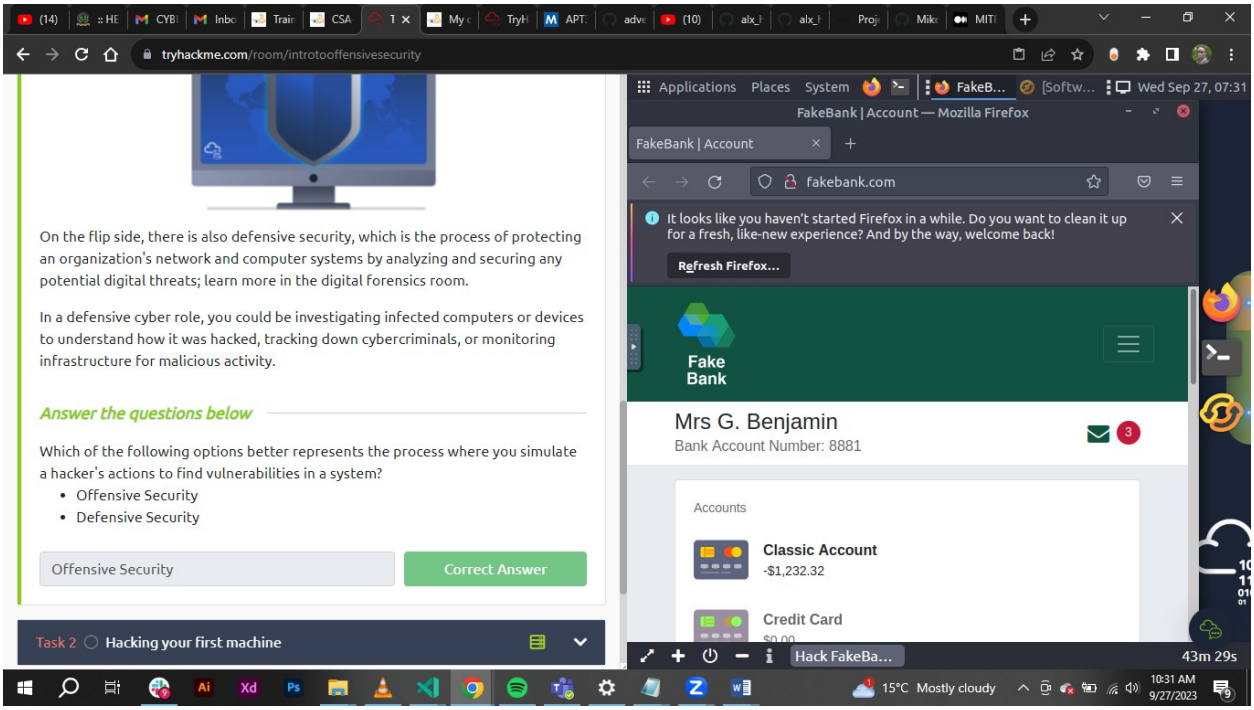
Introduction

The module assignment introduces the learner to offensive security in which it is the process of breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access to them.

Also flipping the side of security there's defensive security - the process of protecting an organization's network and computer systems by analyzing and securing any potential digital threats; learn more in the digital forensics room. In defensive security infected computers or devices are investigated to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.

Activities

Task 1: What is Offensive Security?

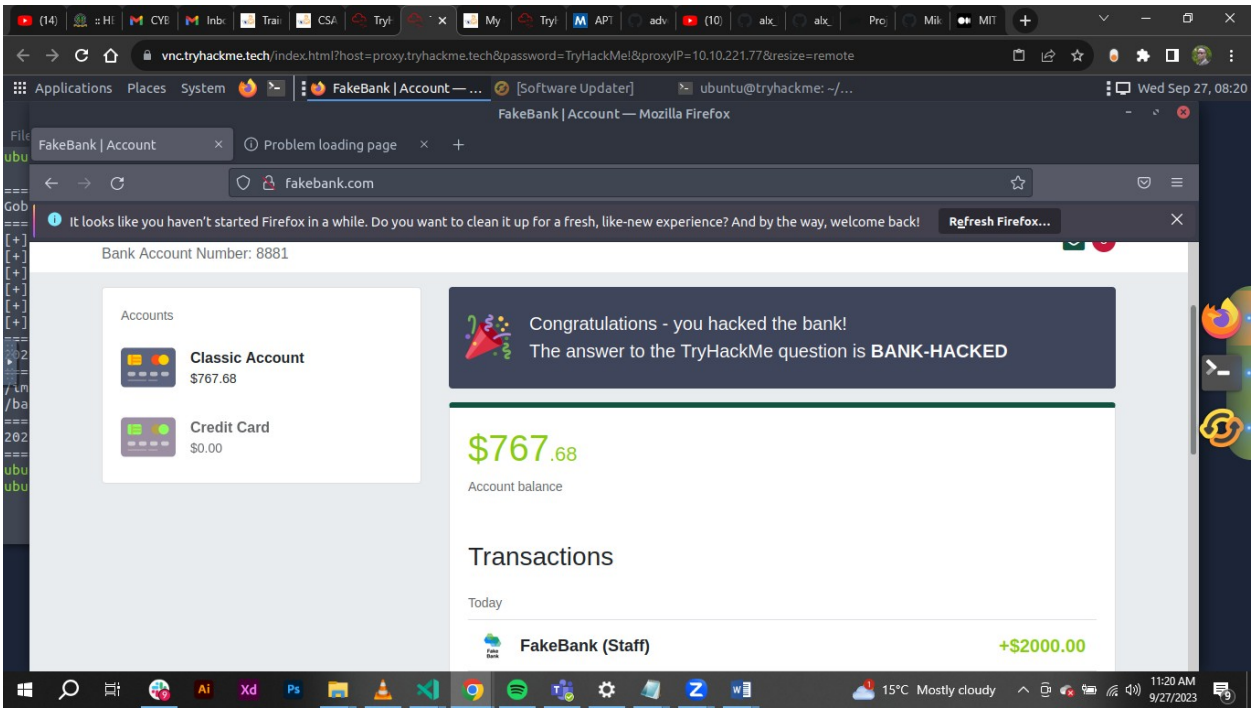


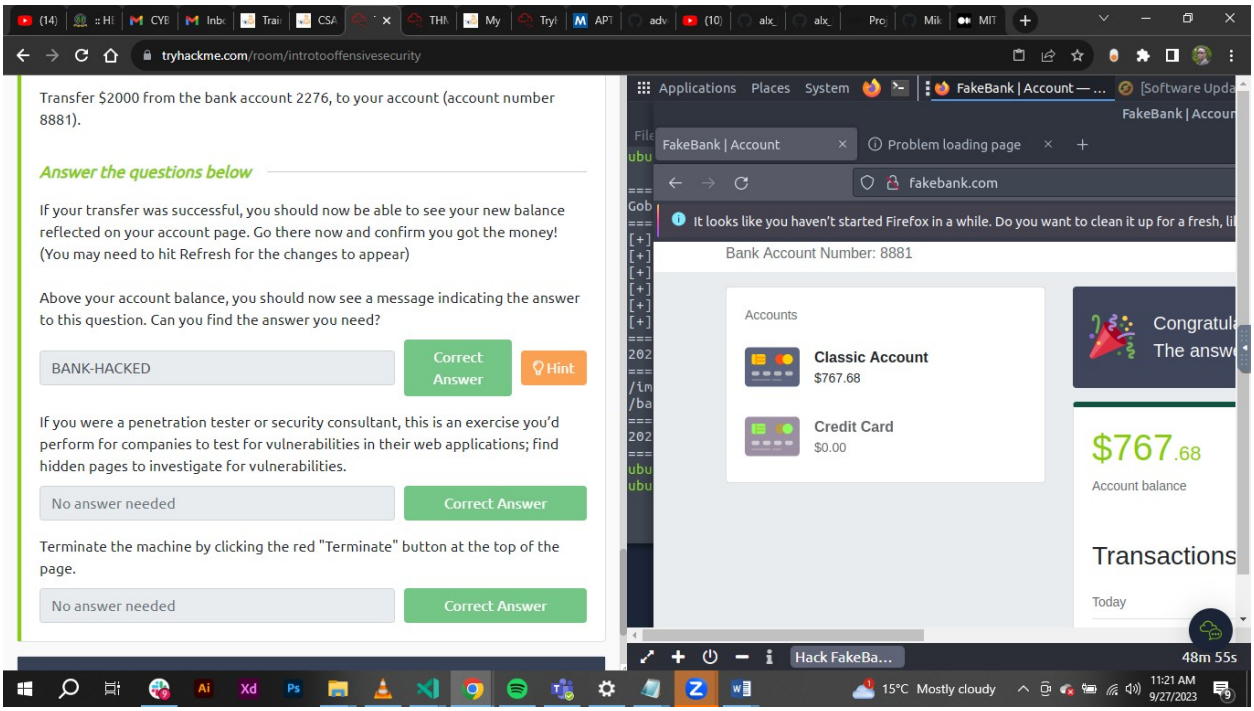
Task 2: Hacking your first machine.

In this task the learner run the command: gobuster -u http://fakebank.com -w wordlist.txt dir – the –u command is used to state the website being scanned whereas –w takes a list of words to iterate through to find hidden pages.

GoBuster scans the website with each word in the list when the above command is fired and find pages that exist on the site. GoBuster will tells pages it found in the list of page/directory names.

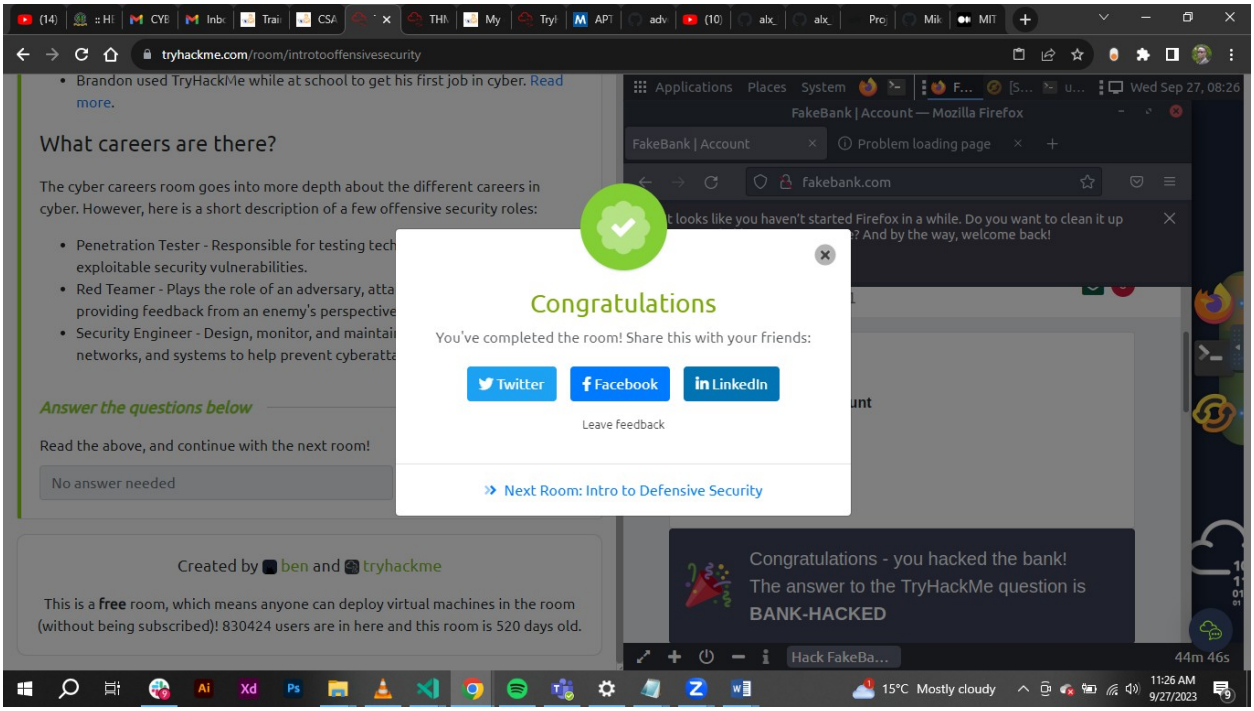
The exercise entailed transferring of $2000 from the bank account 2276, to my account with account number as 8881 with money stolen from any bank account.





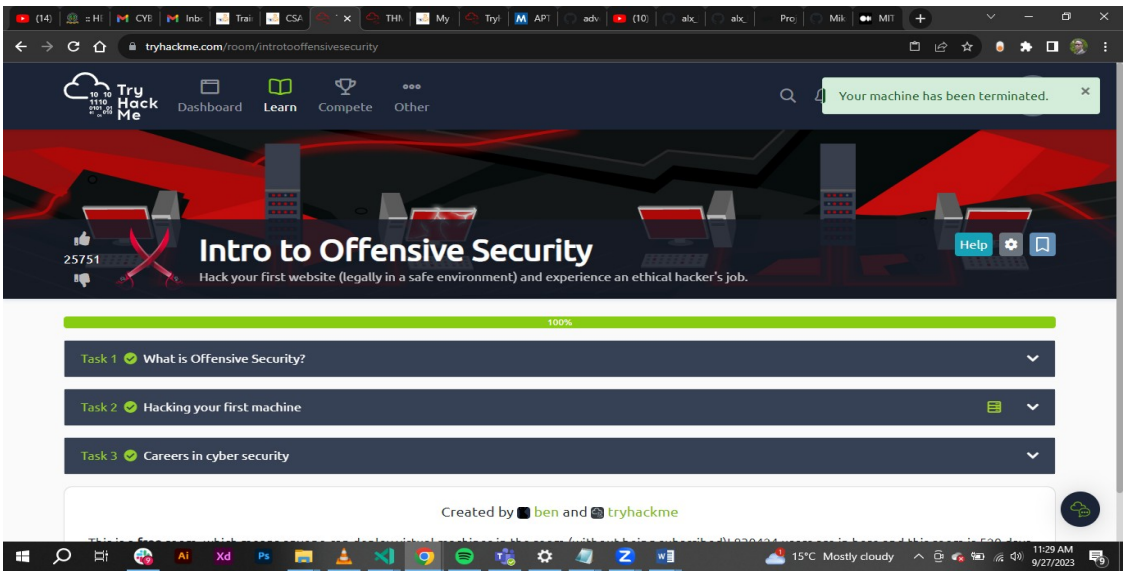
Task 3: Careers in cyber security.

The module finishes by outlining how anyone can start their security journey and also by providing fellows who made into the field.



Conclusion

The learner successfully completed the task/assignment.



Web application security

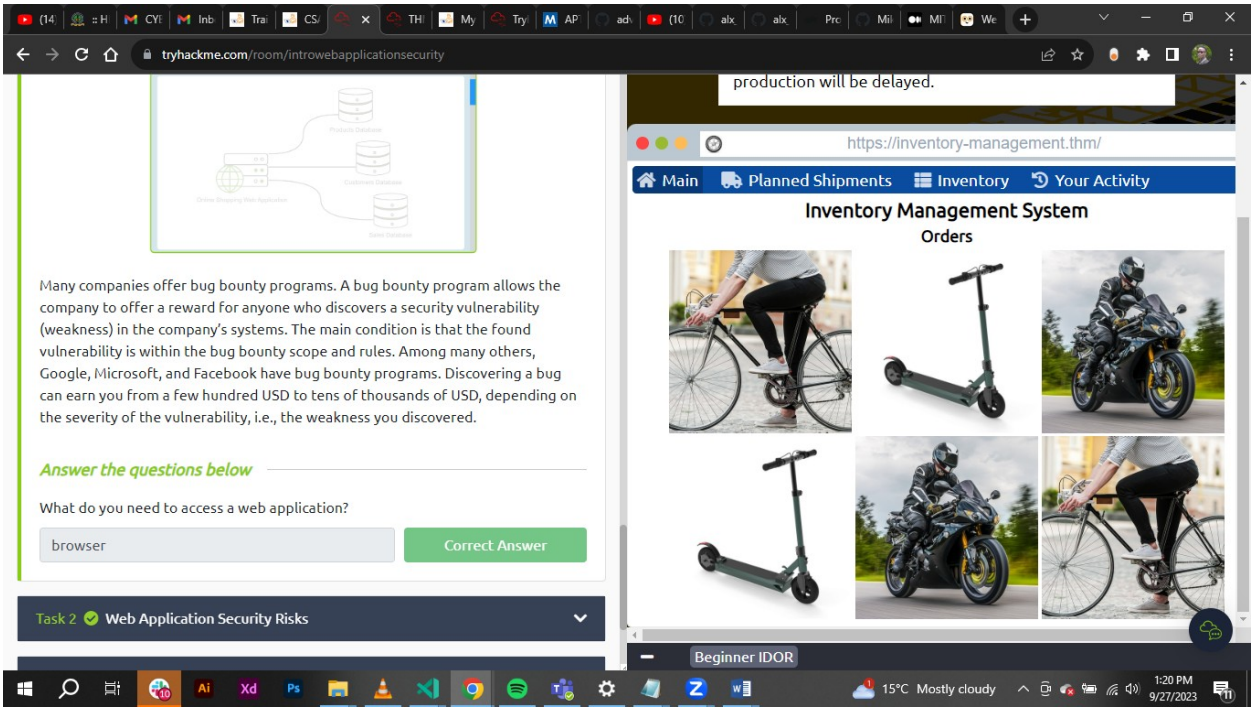
Introduction

Web application is the use of an ‘application’ run on the modern web browser without installation to the local machine.

Activities

Task 1: Introduction

The sub tasks touches Web application is the use of an ‘application’ run on the modern web browser without installation to the local machine. It covers web servers and browsers deeply thereafter to how web applications are accessed.



Task 2: Web Application Security Risks

The sub task covers the risk associated with accessing the web applications. Some of the security risks mentioned are:

Identification and authentication failure.

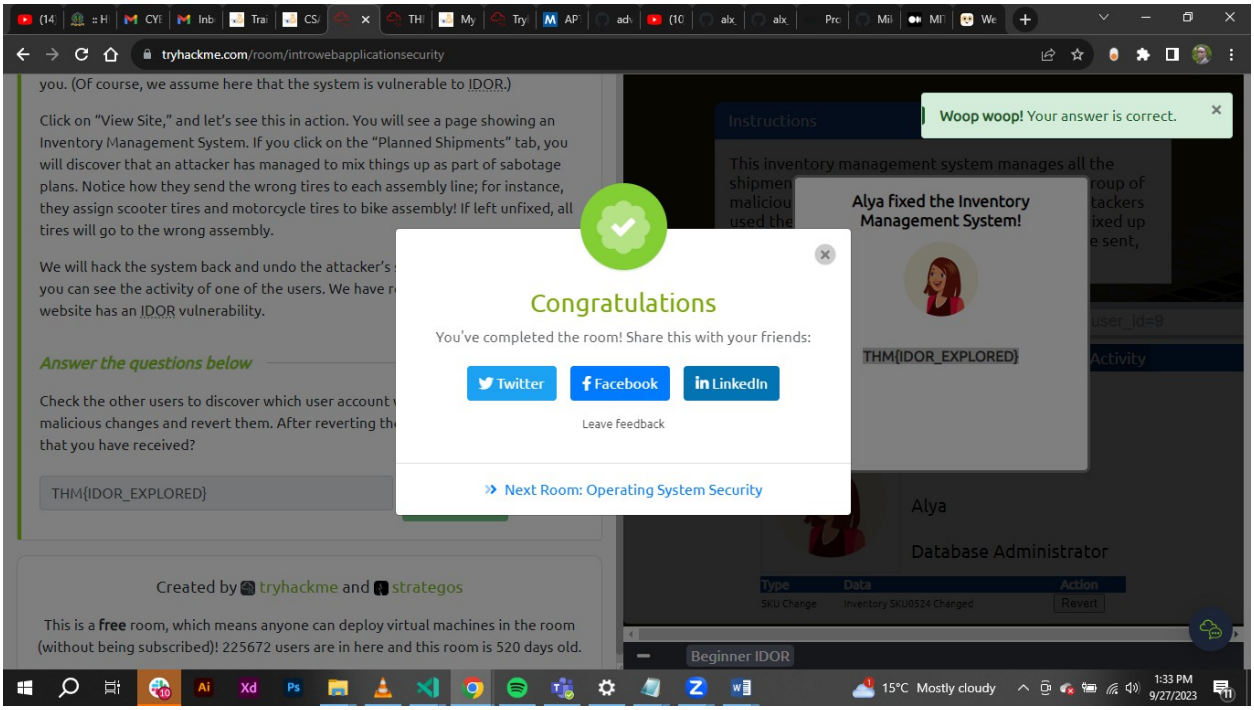
Broken access control - an attacker can access information or perform actions not intended for them.

Injection.

Cryptographic failure.

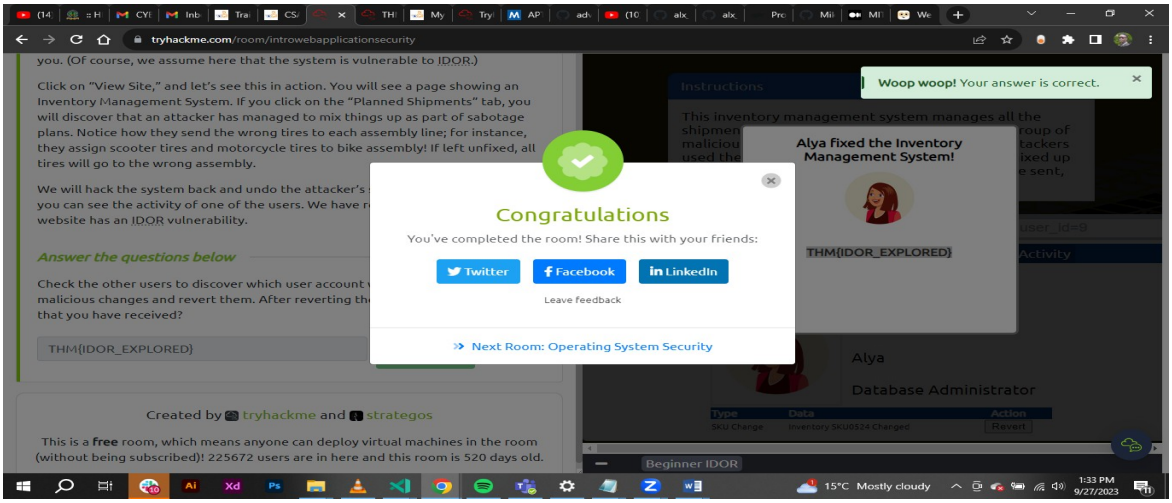
Task 3: Practical Example of Web Application Security

This task investigates a vulnerable website that uses Insecure Direct Object References (IDOR). Insecure Direct Object References falls under the category of Broken Access Control. Broken access control means that an attacker can access information or perform actions not intended for them.



Conclusion

This task enabled the student to understand what web security is, the vulnerabilities entailed in web application and a practical use case of the vulnerabilities associated with live applications.



Intro to Digital Forensics

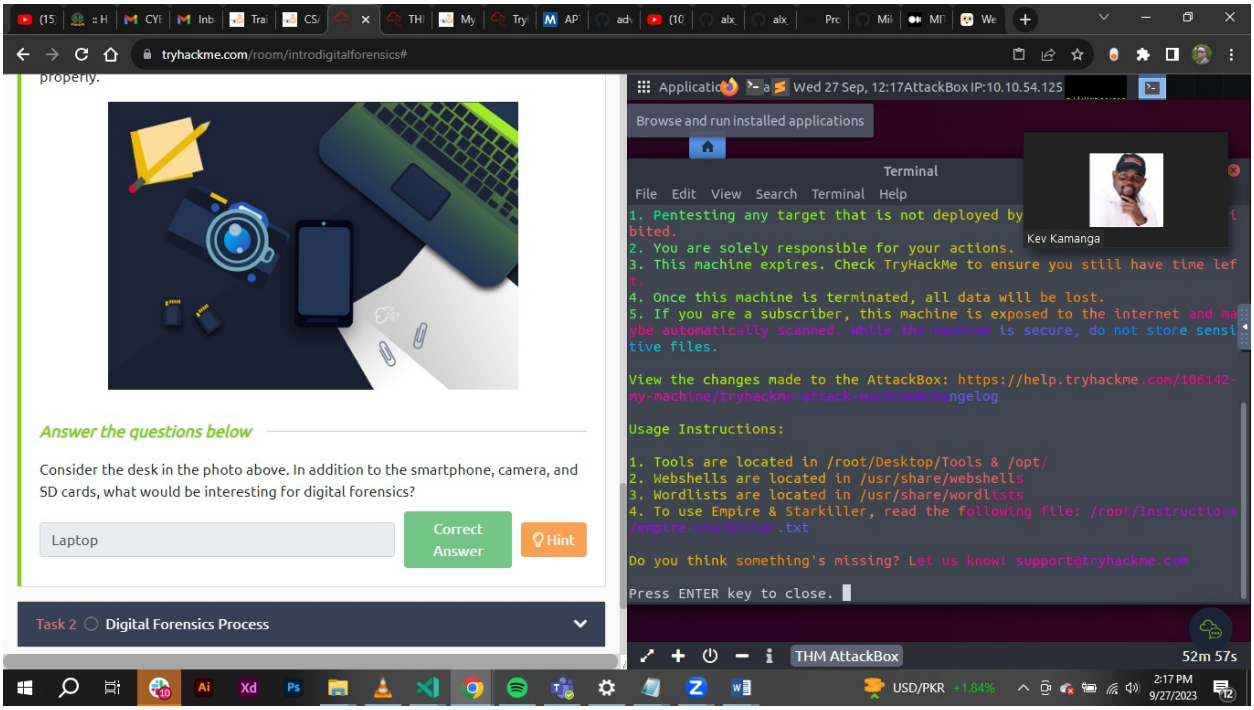
Introduction

This task starts by grooming the learner what Digital Forensics is. Topics covered are: introduction to digital forensics, digital forensics process and practical example of digital forensics.

Activities

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*.



Task 2: Digital Forensics Process

This sub task makes the learner know and understand the process – right one, to be followed after being allowed/permitted to conduct the digital forensic investigation.

The process outline is as follows:

1. Acquire the evidence: Collect the digital devices such as laptops, storage devices, and digital cameras.

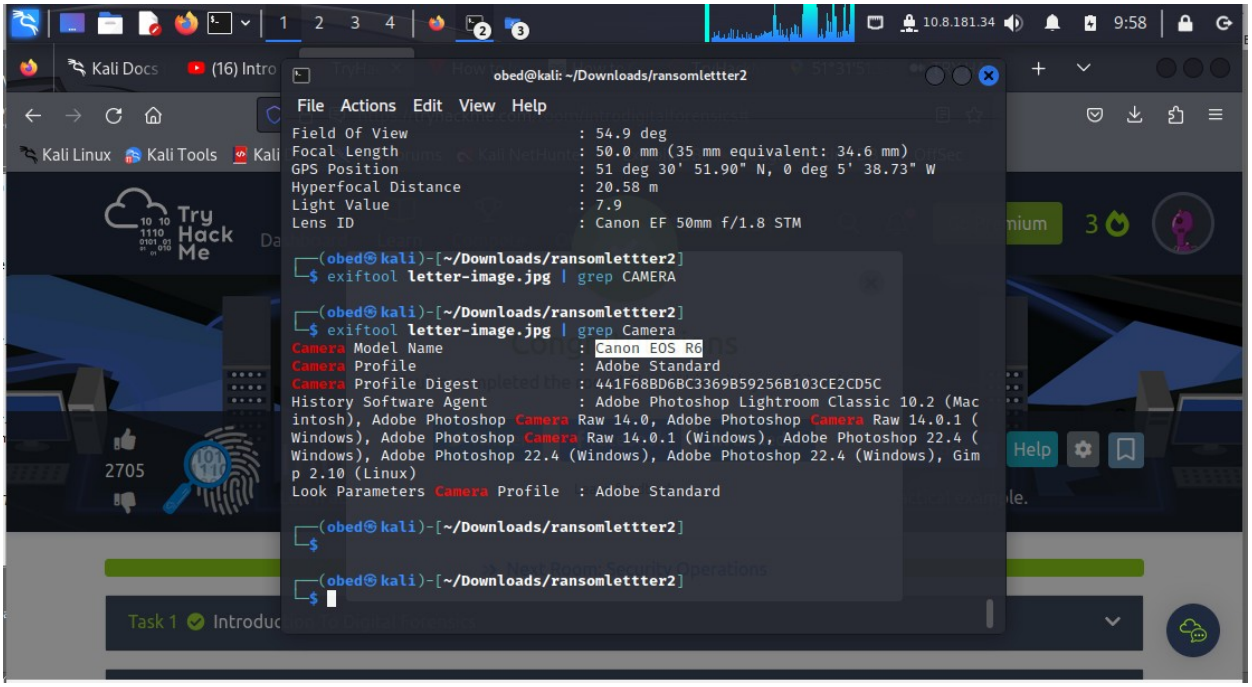
2. Establish a chain of custody: Fill out the related form appropriately. The purpose is to ensure that only the authorized investigators had access to the evidence and no one could have tampered with it.
3. Establish a chain of custody: Fill out the related form appropriately (Sample form). The purpose is to ensure that only the authorized investigators had access to the evidence and no one could have tampered with it.
4. 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.

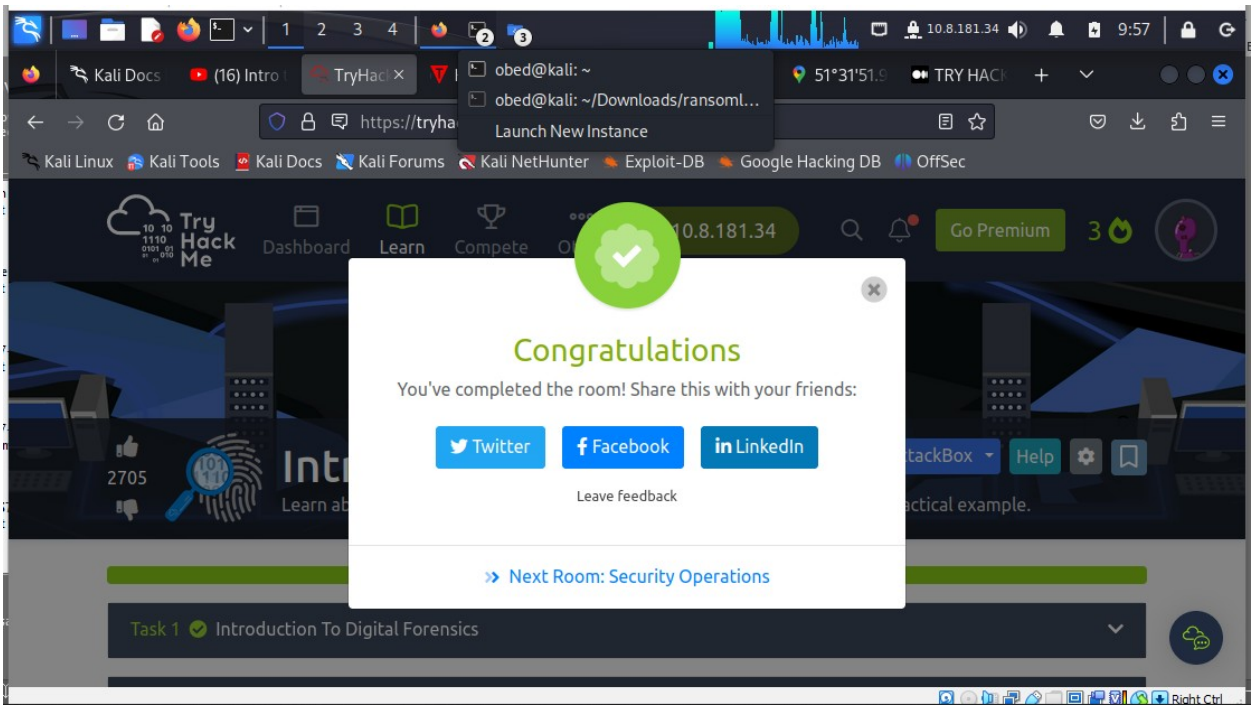
At the lab, the process goes as follows:

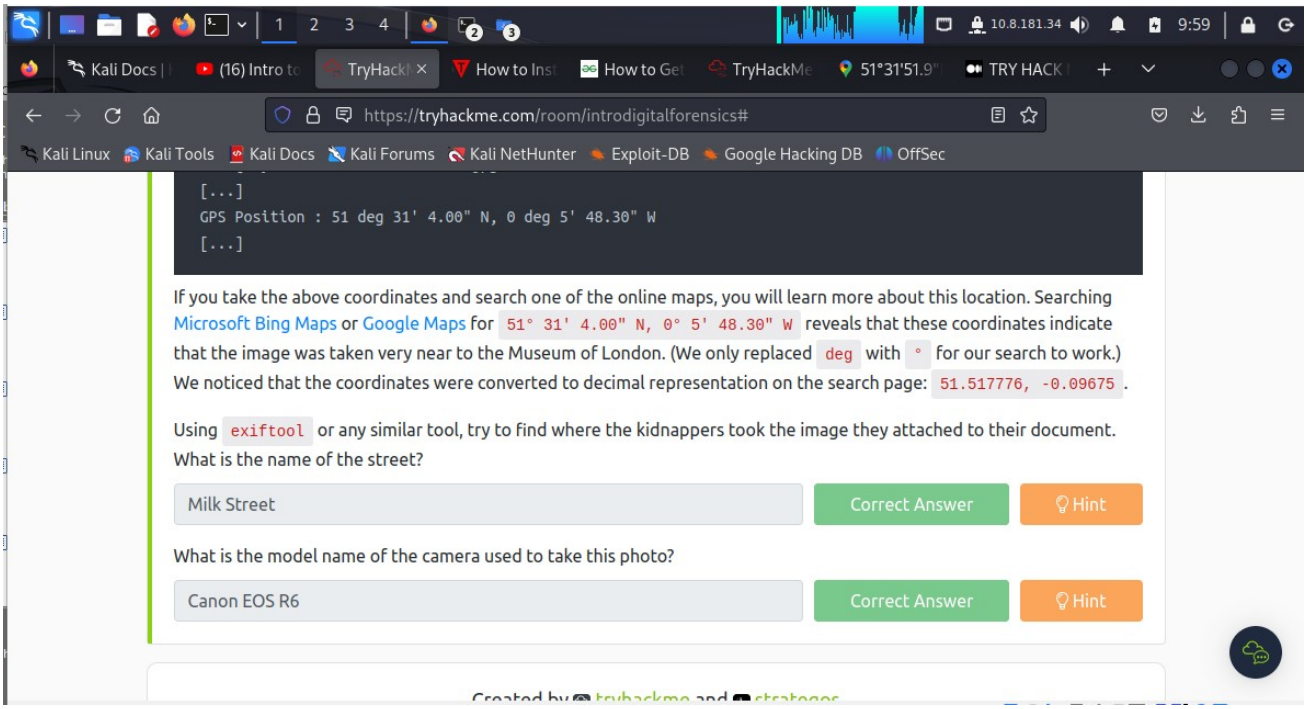
1. Retrieve the digital evidence from the secure container.
2. Create a forensic copy of the evidence: The forensic copy requires advanced software to avoid modifying the original data.
3. Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you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

Task 3: Practical Example of Digital Forensics

In this task assessment the learner learnt how to locate places using GPS coordinates from meta data of files assigned to the task.







Conclusion

Digital forensic is important aspect of security analysis as it enables the learner to investigate crimes and establish facts with the use and spread of digital systems.

Also learnt is the digital forensic process:

The process outline is as follows:

1. Acquire the evidence: Collect the digital devices such as laptops, storage devices, and digital cameras.

2. Establish a chain of custody: Fill out the related form appropriately. The purpose is to ensure that only the authorized investigators had access to the evidence and no one could have tampered with it.

3. 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.

4. 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.

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.