INTRODUCTION TO CYBERSECURITY

ASSIGNMENT REPORT

Introduction to Cyber Security

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:

- Careers in Cyber Security
- Offensive Security; hacking your first application
- Defensive Security; defending against a live cyber attack
- Exploring security topics in the industry

Completing this learning path will give you the knowledge to kick start your cyber journey.

No Prior Knowledge

- You need no prerequisite to start this pathway! Just enthusiasm and excitement to learn!

Peter Kinyumu,
cs-sa07-24067,
May 15th, 2024.

1. INTRODUCTION

This module provides an introduction to cybersecurity and foundational knowledge of the different careers in cybersecurity. It introduces the two major paths in cybersecurity: offensive security and defensive security. The offensive security room guides us through hacking our first application, a fake bank, and exploiting IDOR within a web app. In contrast, the defensive security room introduces us to the world of digital forensics and teaches us how to uncover traces left behind by attackers by exploring file metadata information.

2. ANSWERS TO QUESTIONS

1. Introduction to cybersecurity

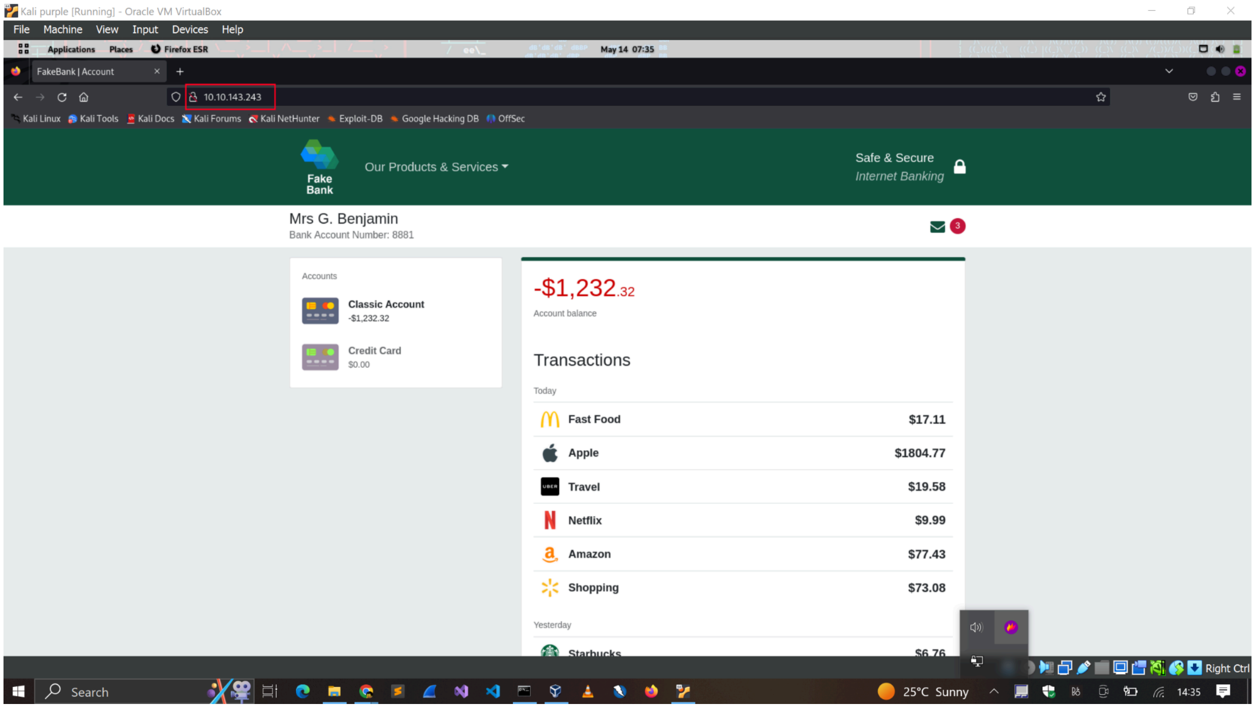
a. Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

- **Offensive Security**
- **Defensive Security**

Offensive security is the correct answer because it involves breaking into computer systems to find loopholes and mitigate them before the attacker finds them.

b. Hacking your first machine

The machine I had access to from the challenge is the web application below called FakeBank.


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Firefox ESR
May 14 07:35
FakeBank | Account
10.10.143.243
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Fake Bank
Our Products & Services
Safe & Secure
Internet Banking
3
Search
25°C Sunny
Right Ctrl
14:35

Mrs G. Benjamin
Bank Account Number: 8881

Accounts

Classic Account
-$1,232.32

Credit Card
$0.00

-$1,232.32
Account balance

Transactions

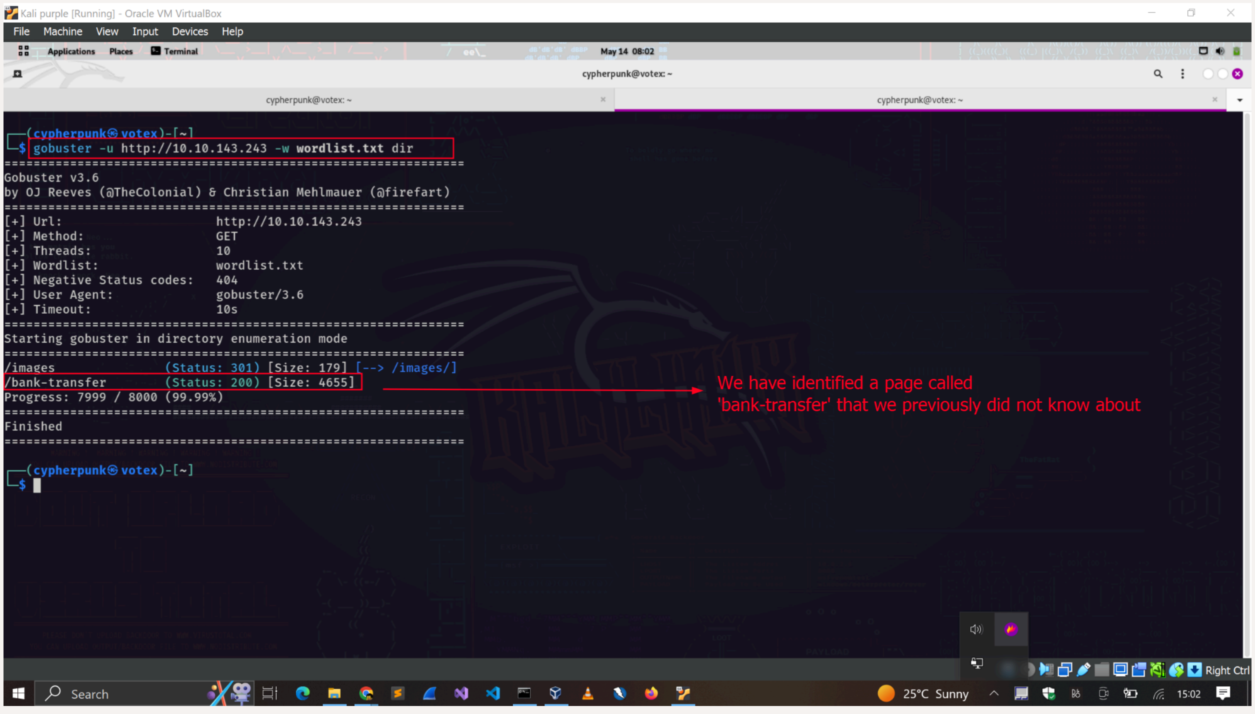
Today

Fast Food	$17.11
Apple	$1804.77
Travel	$19.58
Netflix	$9.99
Amazon	$77.43
Shopping	$73.08

Yesterday

Starbucks	$6.76

The first step was to use a tool called gobuster to perform a directory enumeration of the site, a brute-force approach to listing all pages that exist on the site using a list of potential directory names. The command used was `gobuster -u http://fakebank.com -w wordlist.txt dir.`

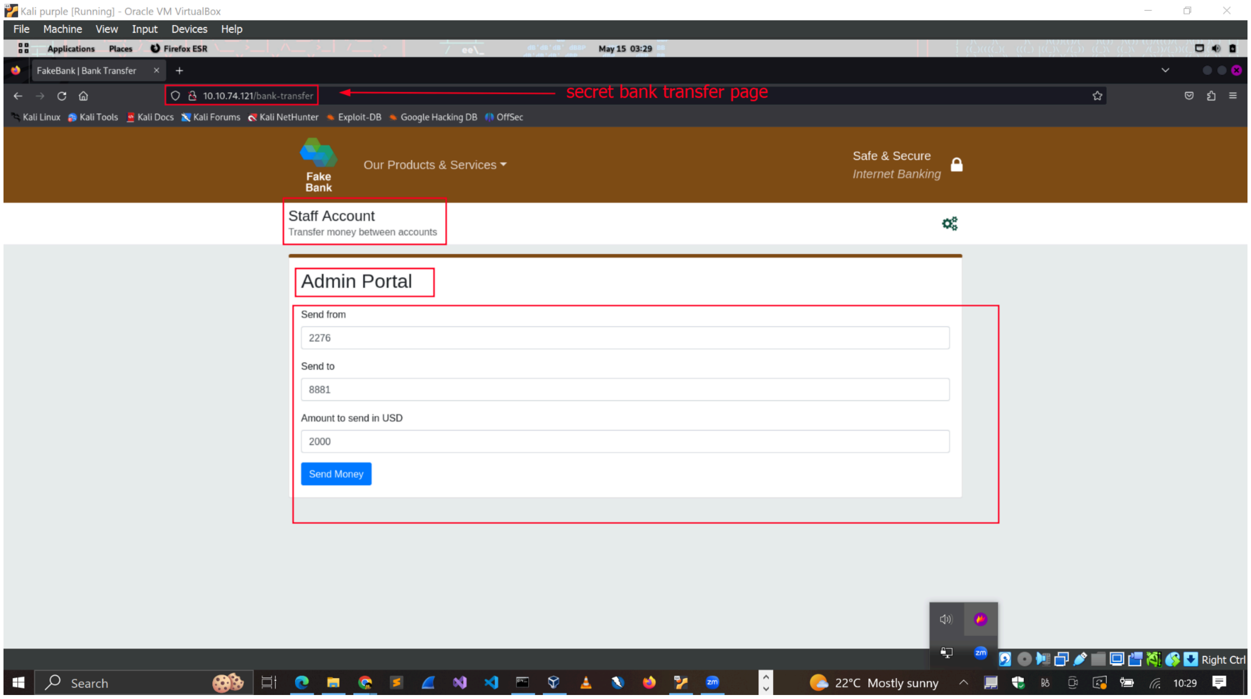

Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
May 14 08:02
cypherpunk@votex: ~
25°C Sunny
15:02
Right Ctrl
Search

```
┌──(cypherpunk㉿votex)-[~]
└─$ gobuster -u http://10.10.143.243 -w wordlist.txt dir
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.143.243
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                wordlist.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 179] [--> /images/]
/bank-transfer        (Status: 200) [Size: 4655]
Progress: 7999 / 8000 (99.99%)
===============================================================
Finished
===============================================================

┌──(cypherpunk㉿votex)-[~]
└─$ 
```

We have identified a page called 'bank-transfer' that we previously did not know about

From the command output, we uncovered a hidden path(directory) within the website that we did not know about before, the/bank-transfer page. With the secret page we've identified, we can try to access it from the fakebank site.


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
FakeBank | Bank Transfer
10.10.74.121/bank-transfer
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Fake Bank
Our Products & Services
Safe & Secure
Internet Banking
Search
22°C Mostly sunny
10:29

secret bank transfer page

Staff Account
Transfer money between accounts

Admin Portal

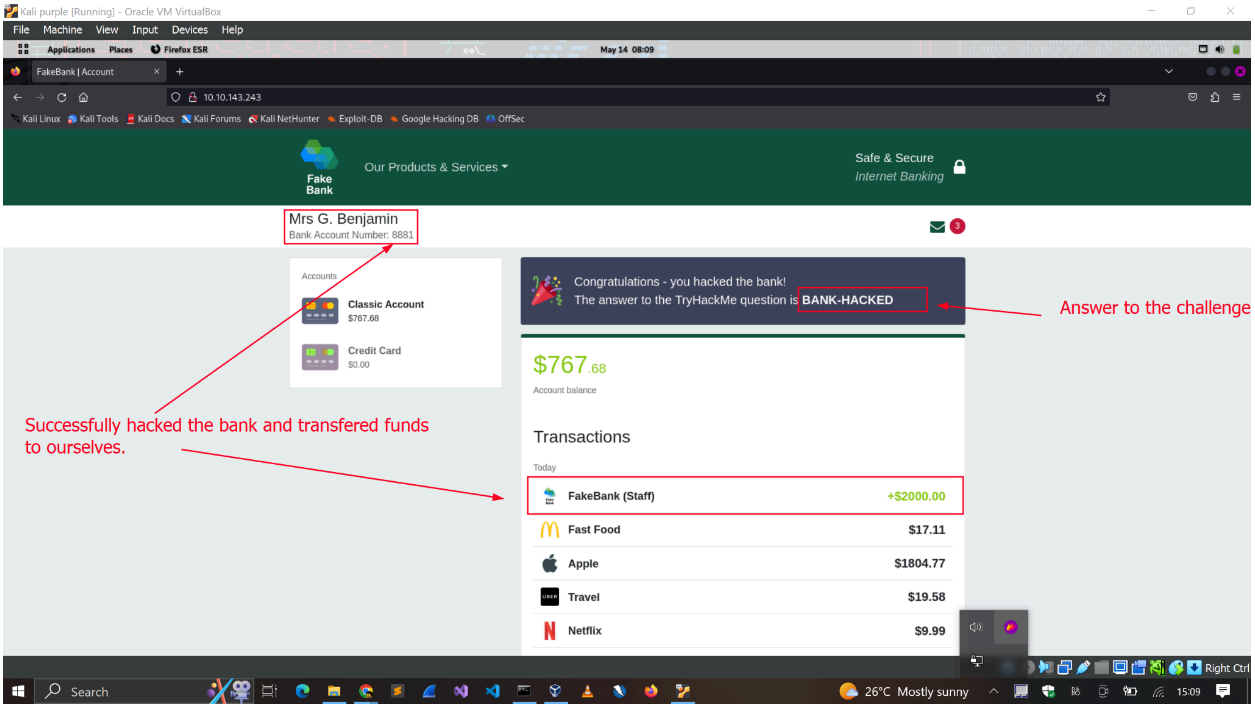
Send from
2276

Send to
8881

Amount to send in USD
2000

Send Money

Viola! We have access to an admin page that allows us to transfer funds between accounts! When we transfer $2000 to ourselves as per the challenge, we get the answer to the question.


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
FakeBank | Account
10.10.143.243
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Fake Bank
Our Products & Services
Safe & Secure
Internet Banking
3
Search
26°C Mostly sunny
15:09

Mrs G. Benjamin
Bank Account Number: 8881

Accounts
Classic Account
$767.68
Credit Card
$0.00

Congratulations - you hacked the bank!
The answer to the TryHackMe question is BANK-HACKED

Answer to the challenge

$767.68
Account balance

Transactions

Today

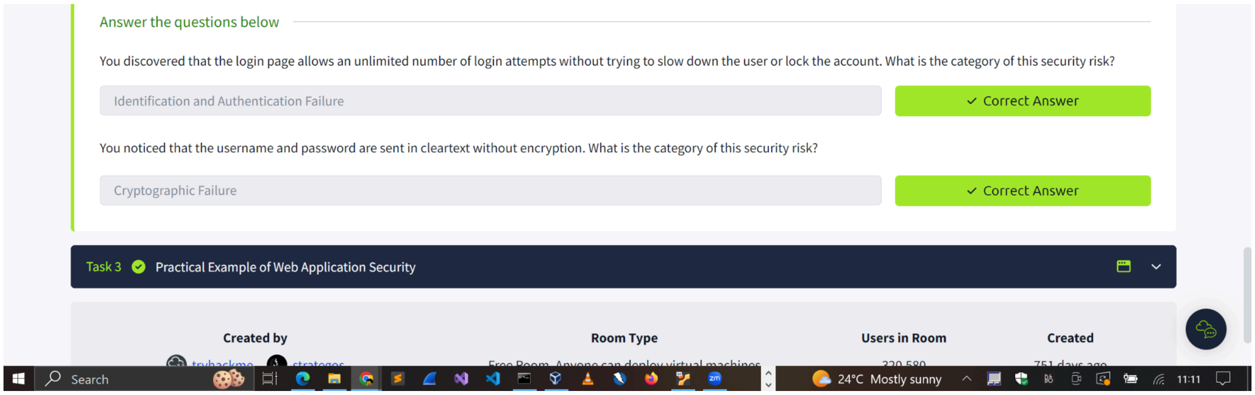
FakeBank (Staff)	+$2000.00
Fast Food	$17.11
Apple	$1804.77
Travel	$19.58
Netflix	$9.99

Successfully hacked the bank and transfered funds to ourselves.

2. Introduction to Offensive Security

Web application security risks

Being able to brute-force a login for unlimited attempts without locking down the account falls under Identification and Authentication Failure. Saving passwords in cleartext is a vulnerability that falls under cryptographic 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?

Identification and Authentication Failure

✓ Correct Answer

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

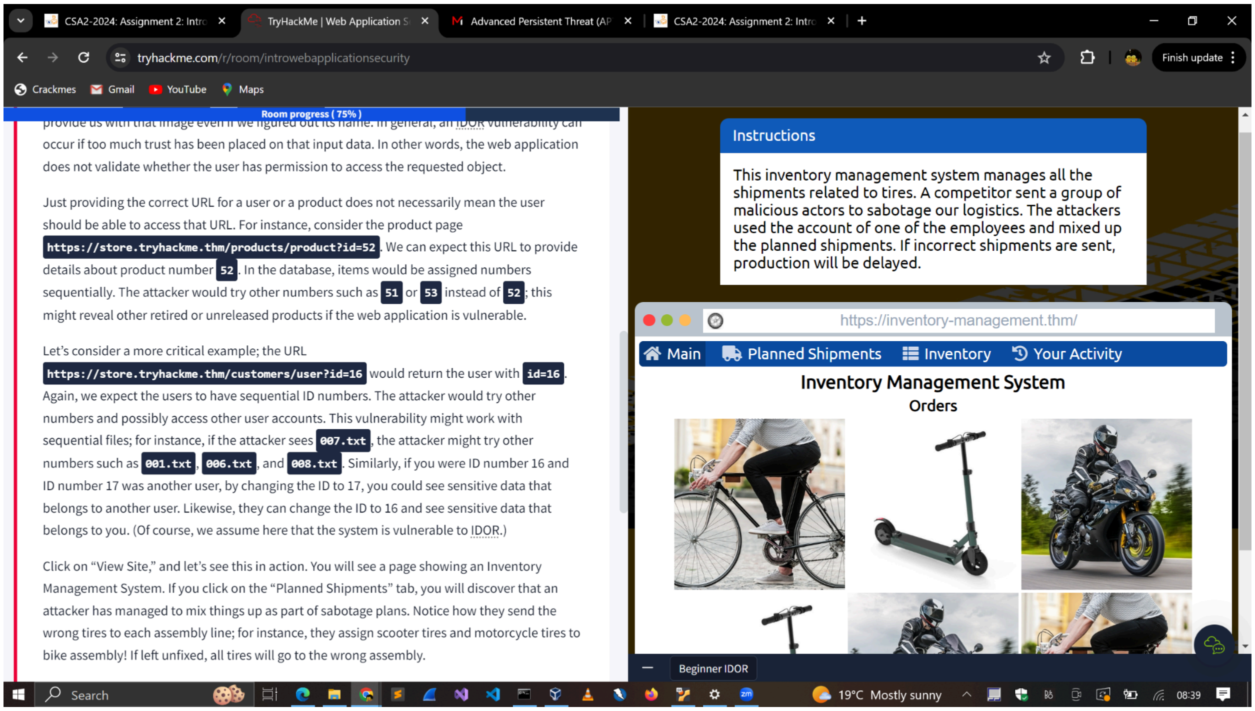
Cryptographic Failure

✓ Correct Answer

Task 3 ✓ Practical Example of Web Application Security

Created by	Room Type	Users in Room	Created
tryhackme strategos	Free Room. Anyone can deploy virtual machines	320,580	751 days ago

In this section, we'll be exploiting the Inventory management system shown below.



CSA2-2024: Assignment 2: Intro
TryHackMe | Web Application S
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introwebapplicationsecurity
Finish update
Crackmes
Gmail
YouTube
Maps
Room progress (75%)

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.

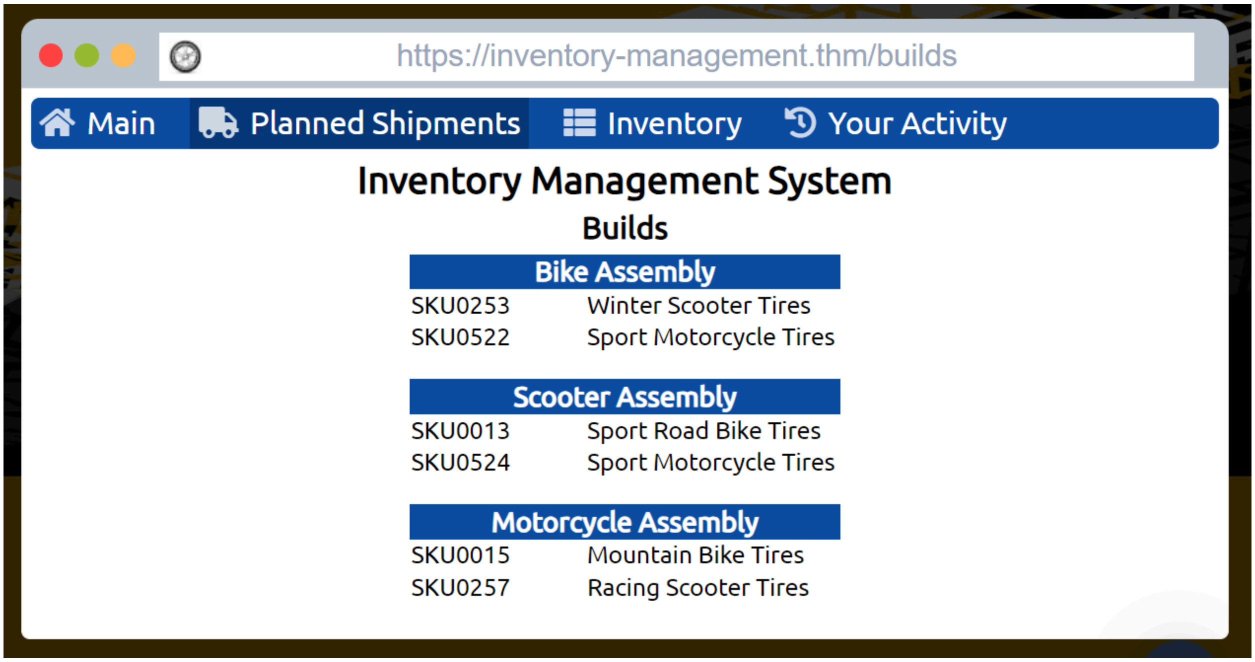
Let's consider a more critical example; the URL `https://store.tryhackme.thm/customers/user?id=16` would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work 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.

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.

When we access planned shipments, we discover that somethings have been mixed up. An attacker has hacked the system and sent the wrong tyres to the wrong assembly line. Our job is to hack back and revert the changes.



Inventory Management System

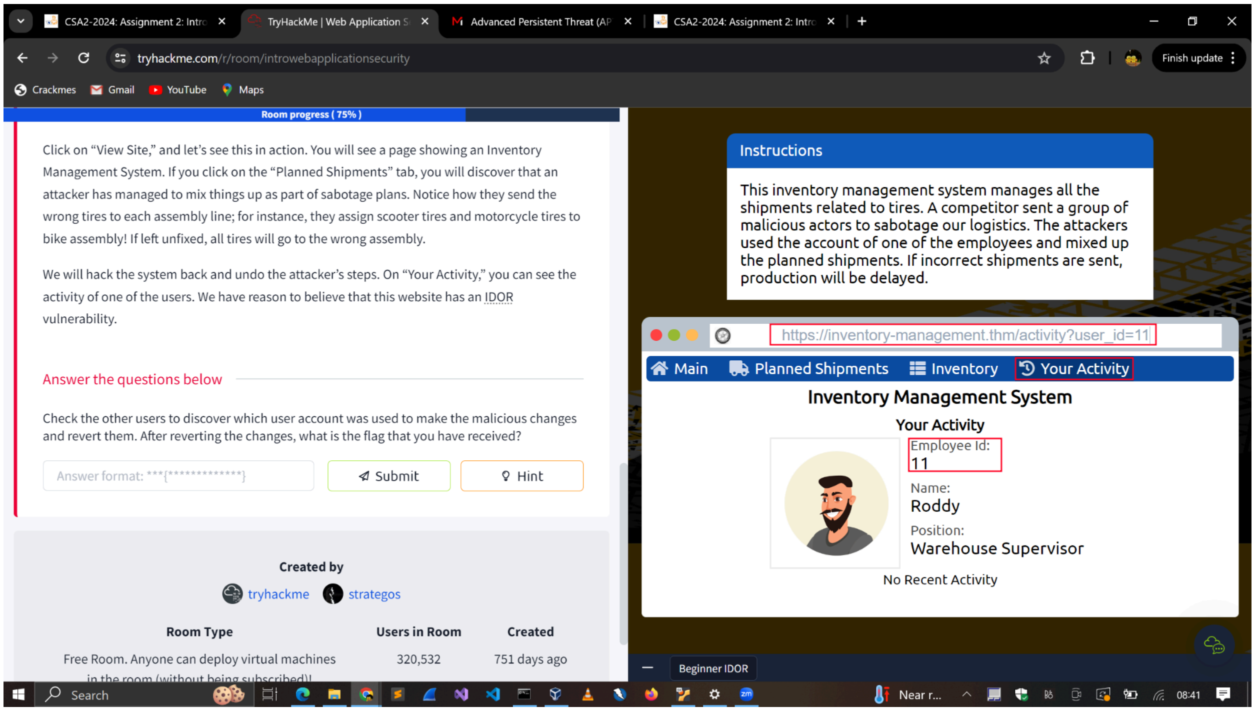
Builds

Bike Assembly	
SKU0253	Winter Scooter Tires
SKU0522	Sport Motorcycle Tires

Scooter Assembly	
SKU0013	Sport Road Bike Tires
SKU0524	Sport Motorcycle Tires

Motorcycle Assembly	
SKU0015	Mountain Bike Tires
SKU0257	Racing Scooter Tires

When we look at your Your activity tab, we note that the employee id is used in the request to access the employee information. That means we can pass any employee idlike 12 and perhaps we can view information of other employees. This poses a risk called IDOR(Indirect Object Reference)



CSA2-2024: Assignment 2: Intro
TryHackMe | Web Application S
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introwebapplicationsecurity
Crackmes
Gmail
YouTube
Maps
Finish update
Room progress (75%)

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 strategos

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	320,532	751 days ago

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

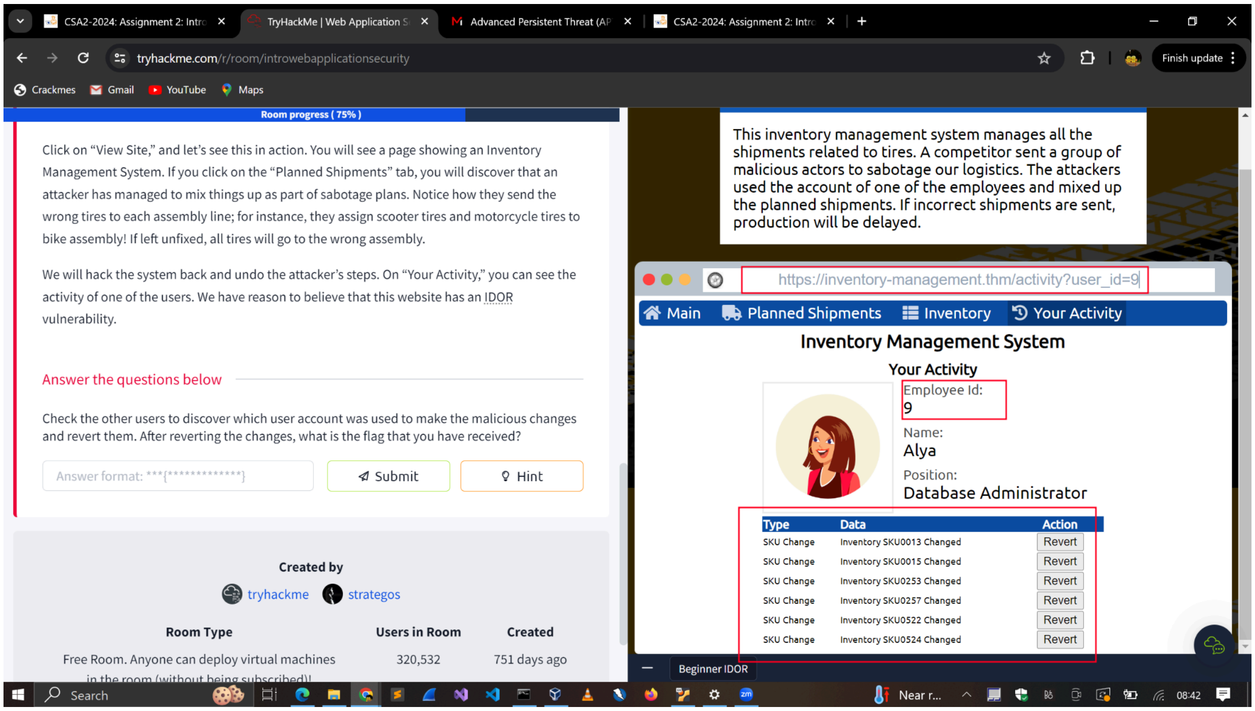
Employee Id:
11

Name:
Roddy

Position:
Warehouse Supervisor

No Recent Activity

So,our goal is discover which user account was used to make the malicious changes and revert them. Guessing different employee id's from 1… we uncover that the suer account with employee with id 9(Database administrator) was used to make the malicious changes.


CSA2-2024: Assignment 2: Intro
TryHackMe | Web Application S
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introwebapplicationsecurity
Finish update
Crackmes
Gmail
YouTube
Maps
Room progress (75%)

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?

Created by

tryhackme strategos

Room Type Users in Room Created

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! 320,532 751 days ago

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=9

Inventory Management System

Your Activity

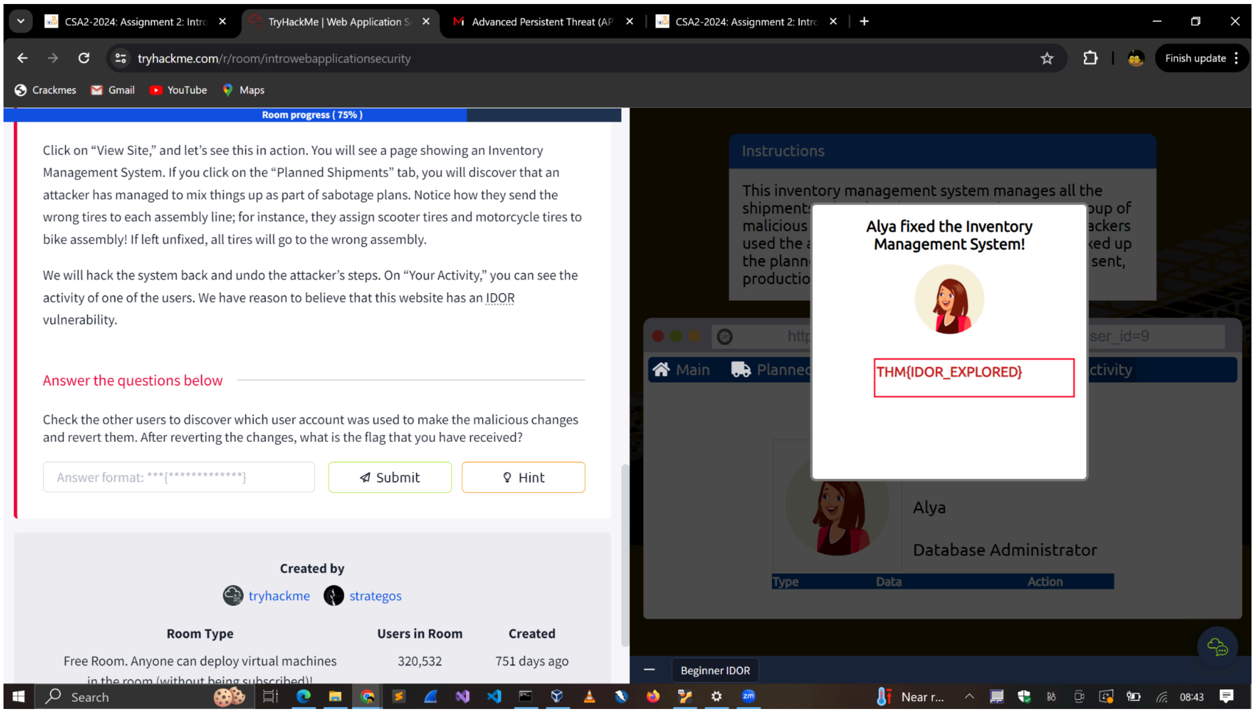
Employee Id:
9

Name:
Alya

Position:
Database Administrator

Type	Data	Action
SKU Change	Inventory SKU0013 Changed	Revert
SKU Change	Inventory SKU0015 Changed	Revert
SKU Change	Inventory SKU0253 Changed	Revert
SKU Change	Inventory SKU0257 Changed	Revert
SKU Change	Inventory SKU0522 Changed	Revert
SKU Change	Inventory SKU0524 Changed	Revert

Let's revert the changes. We get the flag.


CSA2-2024: Assignment 2: Intro
TryHackMe | Web Application S
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introwebapplicationsecurity
Finish update
Crackmes
Gmail
YouTube
Maps
Room progress (75%)

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?

Created by

tryhackme strategos

Room Type Users in Room Created

Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! 320,532 751 days ago

Instructions

Alya fixed the Inventory Management System!

THM{IDOR_EXPLORED}

Alya

Database Administrator

3. Introduction to Defensive Security

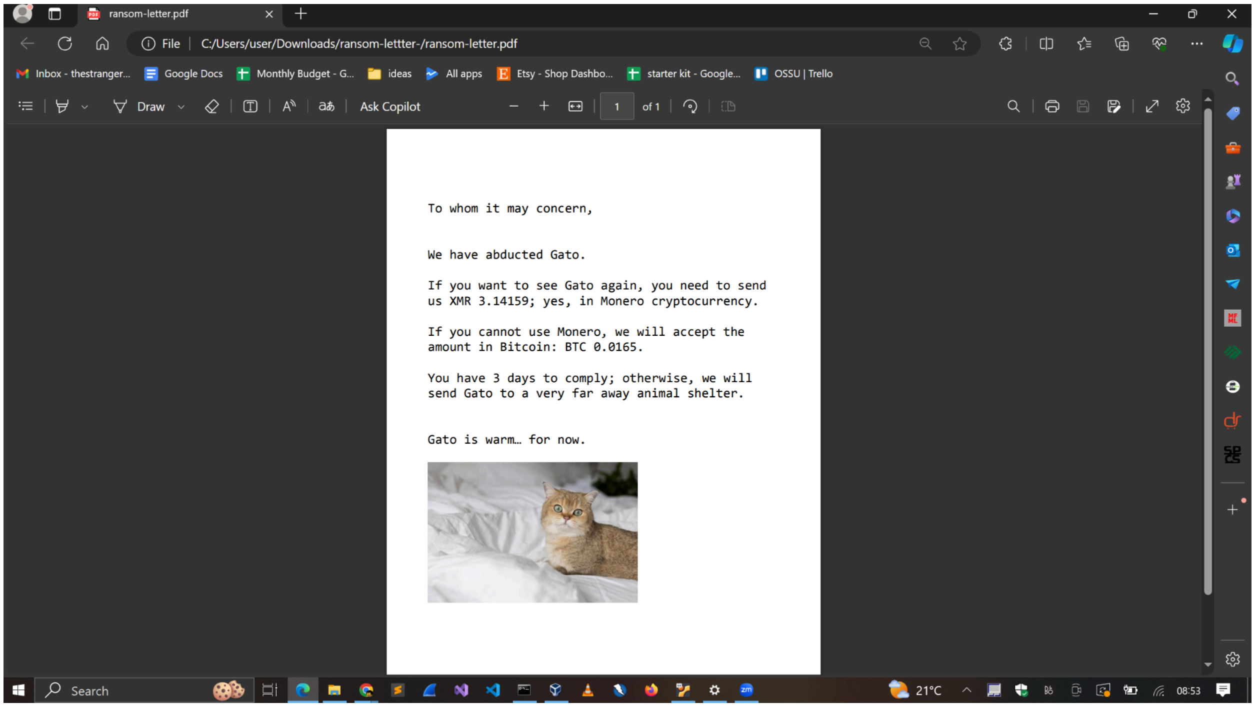
Introduction to Digital Forensics

a. **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, in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. This protects its integrity and ensures it is admissible in court.

b. **Our cat, Gado, has been kidnapped. The kidnapper has sent us a document with their requests.**

Our goal is to analyze the metadata information to uncover some evidence details about the hacker.



To whom it may concern,

We have abducted Gato.

If you want to see Gato again, you need to send us XMR 3.14159; yes, in Monero cryptocurrency.

If you cannot use Monero, we will accept the amount in Bitcoin: BTC 0.0165.

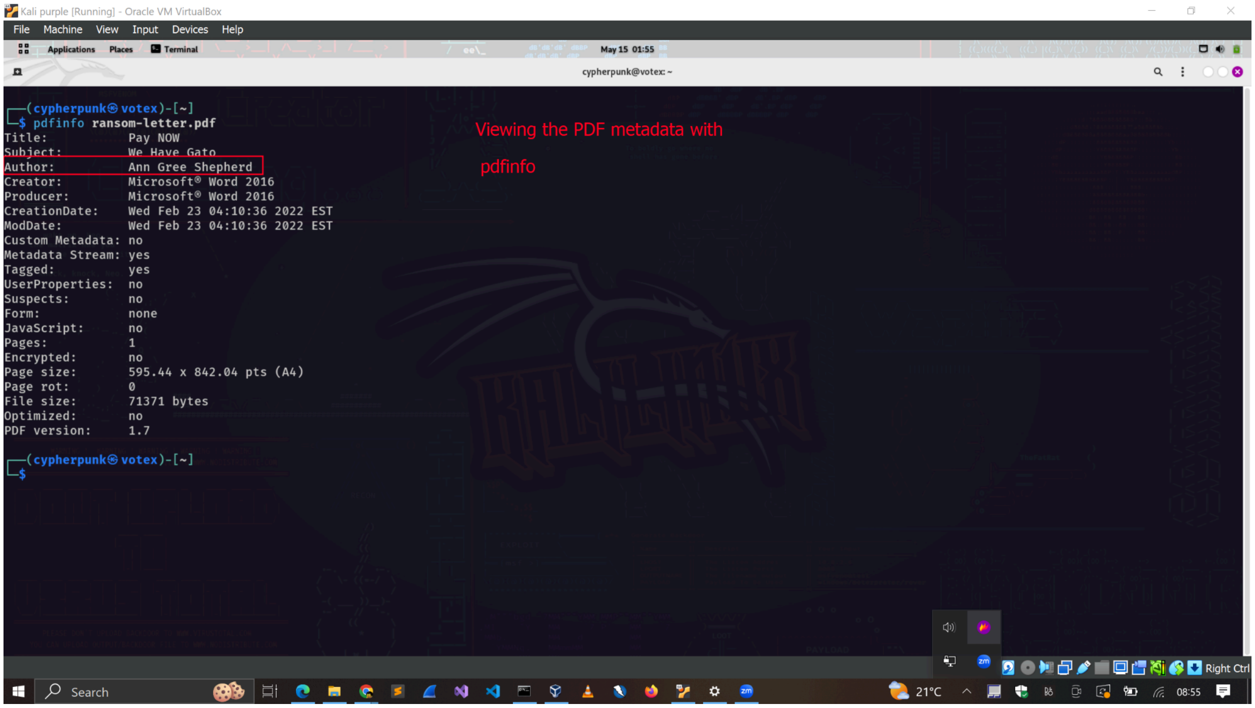
You have 3 days to comply; otherwise, we will send Gato to a very far away animal shelter.

Gato is warm… for now.

Metadata refers to data about data. Every file contains some properties about itself like the creation time, modification time, size, sometimes even geolocation information for images. We can leverage this to analyze the information of the files sent by the attacker and see what we can identify.

The **pdfinfo** command can be used to view the metadata information of any pdf file.

I. Using pdfinfo, find out the author of the attached PDF file, ransom-letter.pdf.



Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
May 15 01:55
cypherpunk@votex: ~
Right Ctrl
Search
21°C
08:55

```
┌──(cypherpunk㉿votex)-[~]
└─$ 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 04:10:36 2022 EST
ModDate:         Wed Feb 23 04:10:36 2022 EST
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

┌──(cypherpunk㉿votex)-[~]
└─$
```

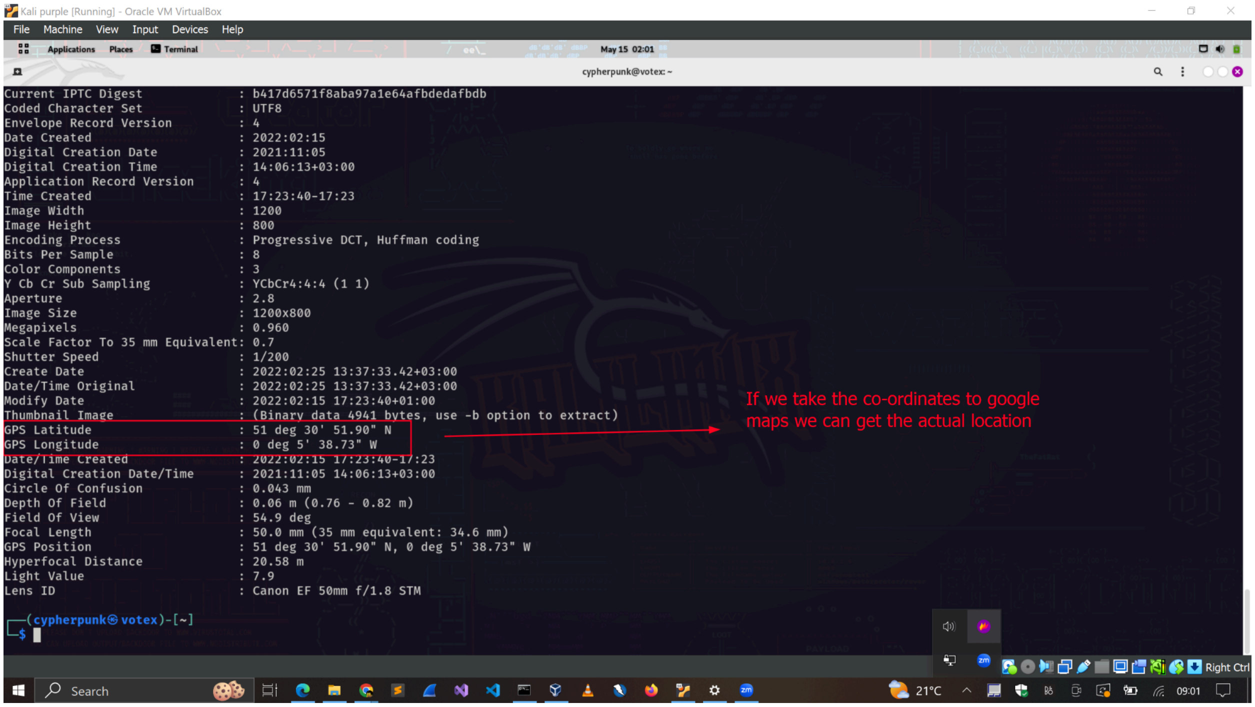
Viewing the PDF metadata with

pdfinfo

EXIF(Exchangeable Image File Format) is the metadata information for image files. This information may contain the camera model used to capture the info, date and time and sometimes the geolocation position where the image was captured.

II. 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?

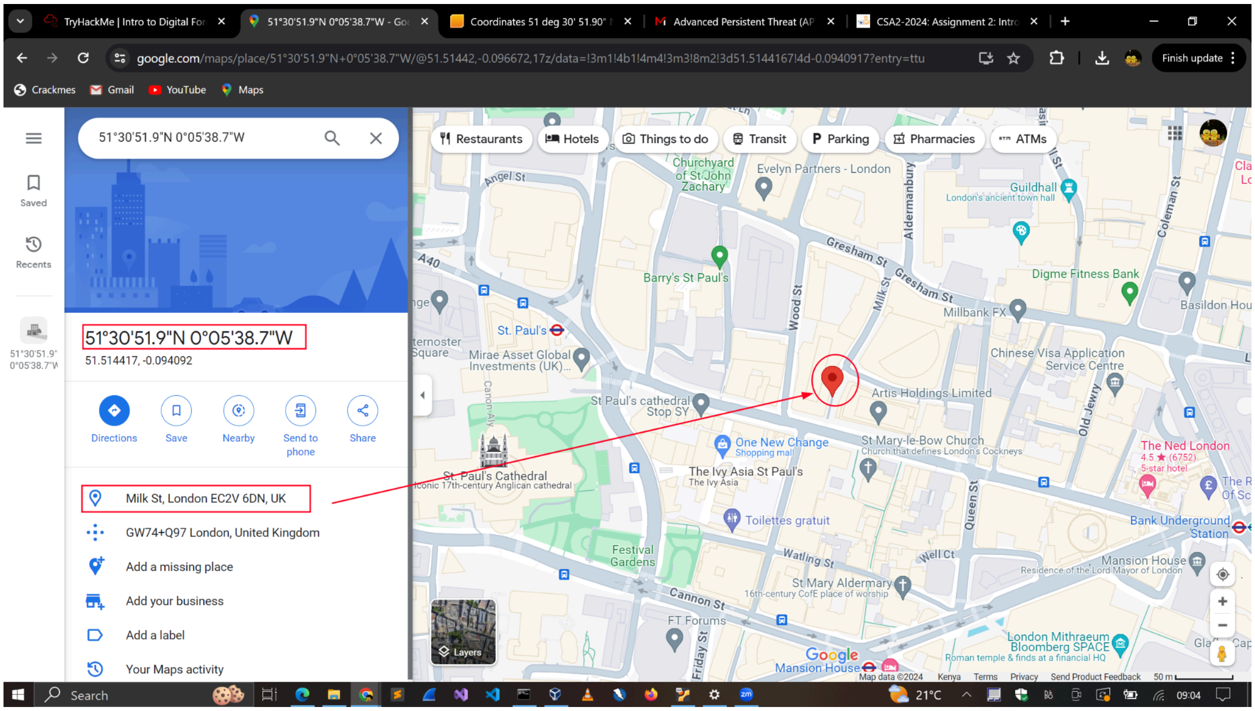
```
exiftool image-letter.jpg
```


Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
May 15 02:01
cypherpunk@votex: ~
Search
21°C
09:01
Right Ctrl

```
Current IPTC Digest             : b417d6571f8aba97a1e64afbdedafbdb
Coded Character Set             : UTF8
Envelope Record Version         : 4
Date Created                    : 2022:02:15
Digital Creation Date           : 2021:11:05
Digital Creation Time           : 14:06:13+03:00
Application Record Version      : 4
Time Created                    : 17:23:40-17:23
Image Width                     : 1200
Image Height                    : 800
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Aperture                        : 2.8
Image Size                      : 1200x800
Megapixels                      : 0.960
Scale Factor To 35 mm Equivalent: 0.7
Shutter Speed                   : 1/200
Create Date                     : 2022:02:25 13:37:33.42+03:00
Date/Time Original              : 2022:02:25 13:37:33.42+03:00
Modify Date                     : 2022:02:15 17:23:40+01:00
Thumbnail Image                 : (Binary data 4941 bytes, use -b option to extract)
GPS Latitude                    : 51 deg 30' 51.90" N
GPS Longitude                   : 0 deg 5' 38.73" W
Date/Time Created               : 2022:02:15 17:23:40-17:23
Digital Creation Date/Time      : 2021:11:05 14:06:13+03:00
Circle Of Confusion             : 0.043 mm
Depth Of Field                  : 0.06 m (0.76 - 0.82 m)
Field Of View                   : 54.9 deg
Focal Length                    : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position                    : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance             : 20.58 m
Light Value                     : 7.9
Lens ID                         : Canon EF 50mm f/1.8 STM

┌──(cypherpunk㉿votex)-[~]
└─$ 
```

If we take the co-ordinates to google maps we can get the actual location


TryHackMe | Intro to Digital For
51°30'51.9"N 0°05'38.7"W - Go
Coordinates 51 deg 30' 51.90"
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
google.com/maps/place/51°30'51.9"N+0°05'38.7"W/@51.51442,-0.096672,17z/data=!3m1!4b1!4m4!3m3!8m2!3d51.5144167!4d-0.0940917?entry=ttu
Finish update
Crackmes Gmail YouTube Maps
Saved
Recents
51°30'51.9" 0°05'38.7"W
Directions
Save
Nearby
Send to phone
Share
Add a missing place
Add your business
Add a label
Your Maps activity
Restaurants
Hotels
Things to do
Transit
Parking
Pharmacies
ATMs
Churchyard of St John Zachary
Evelyn Partners - London
Guildhall
London's ancient town hall
Gresham St
Barry's St Paul's
Digme Fitness Bank
Millbank FX
Basildon Hou
St. Paul's
Mirae Asset Global Investments (UK)...
Chinese Visa Application Service Centre
Artis Holdings Limited
St Paul's cathedral Stop SY
One New Change
Shopping mall
St Mary-le-Bow Church
Church that defines London's Cockneys
The Ned London
4.5 ★ (6752)
5-star hotel
St. Paul's Cathedral
Iconic 17th-century Anglican cathedral
The Ivy Asia St Paul's
The Ivy Asia
Toilettes gratuit
Bank Underground Station
Festival Gardens
Watling St
Mansion House
Residence of the Lord Mayor of London
St Mary Aldermary
16th-century CofE place of worship
Cannon St
FT Forums
London Mithraeum Bloomberg SPACE
Roman temple & finds at a financial HQ
Layers
Google
Mansion House
Map data ©2024 Kenya Terms Privacy Send Product Feedback 50 m
Search
21°C
09:04

51°30'51.9"N 0°05'38.7"W

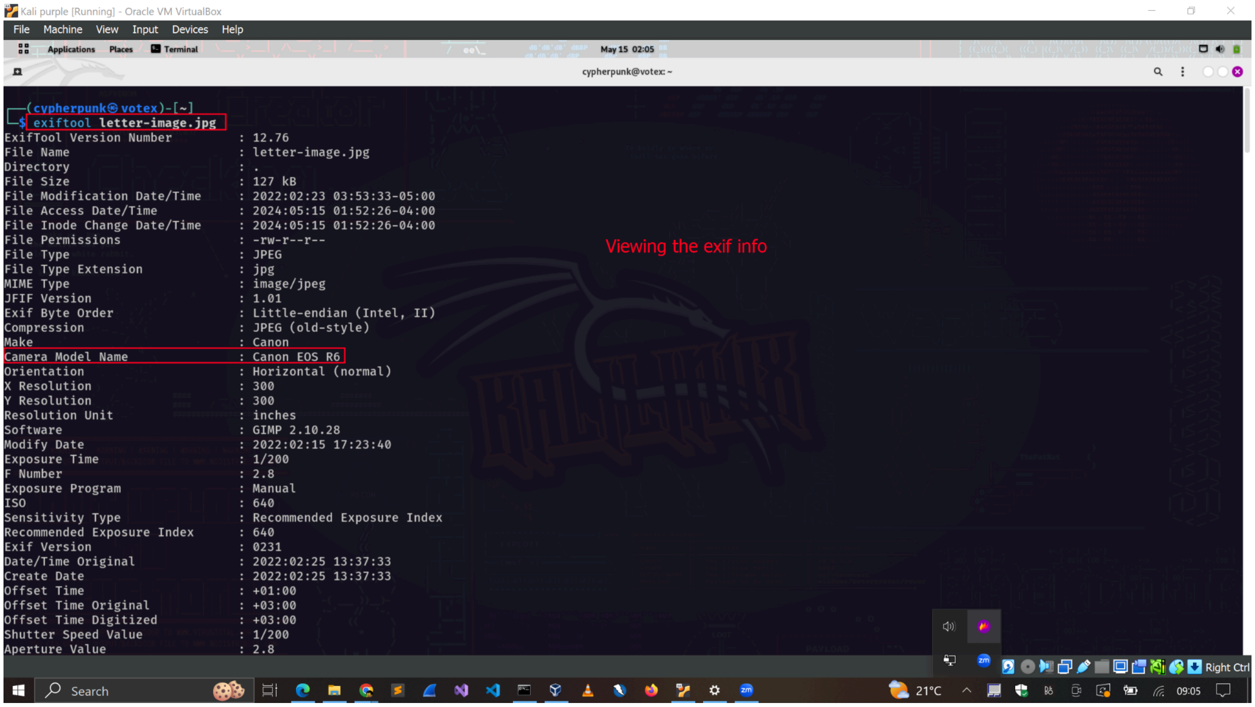
51.514417, -0.094092

Milk St, London EC2V 6DN, UK

GW74+Q97 London, United Kingdom

The street where the image was captured is the **Milk Street** in London.

III. What is the model name of the camera used to take this photo?



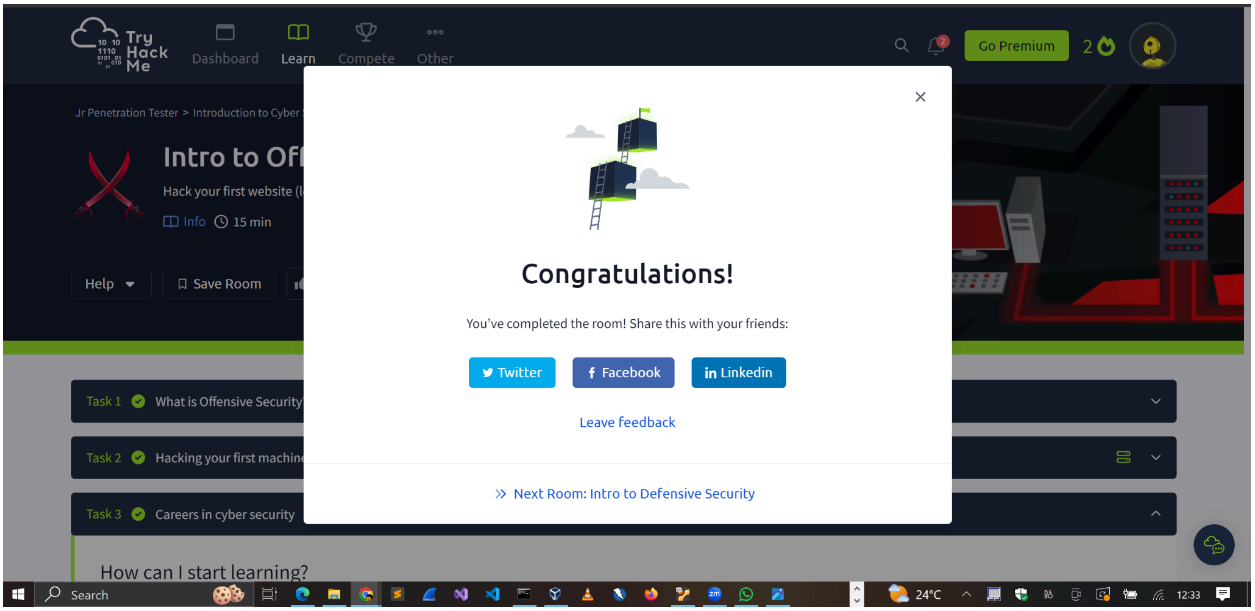
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
May 15 02:05
cypherpunk@votex: ~
Search
21°C
09:05
Right Ctrl

```
┌──(cypherpunk㉿votex)-[~]
└─$ exiftool letter-image.jpg
ExifTool Version Number         : 12.76
File Name                       : letter-image.jpg
Directory                       : .
File Size                       : 127 kB
File Modification Date/Time     : 2022:02:23 03:53:33-05:00
File Access Date/Time           : 2024:05:15 01:52:26-04:00
File Inode Change Date/Time     : 2024:05:15 01:52:26-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type 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                    : 300
Resolution Unit                 : inches
Software                        : GIMP 2.10.28
Modify Date                     : 2022:02:15 17:23:40
Exposure Time                   : 1/200
F Number                        : 2.8
Exposure Program                : Manual
ISO                             : 640
Sensitivity Type                : Recommended Exposure Index
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
```

Viewing the exif info

3. MODULE COMPLETION

There was no sharable link provided for the completion of the three specific rooms.



Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook in Linkedin

Leave feedback

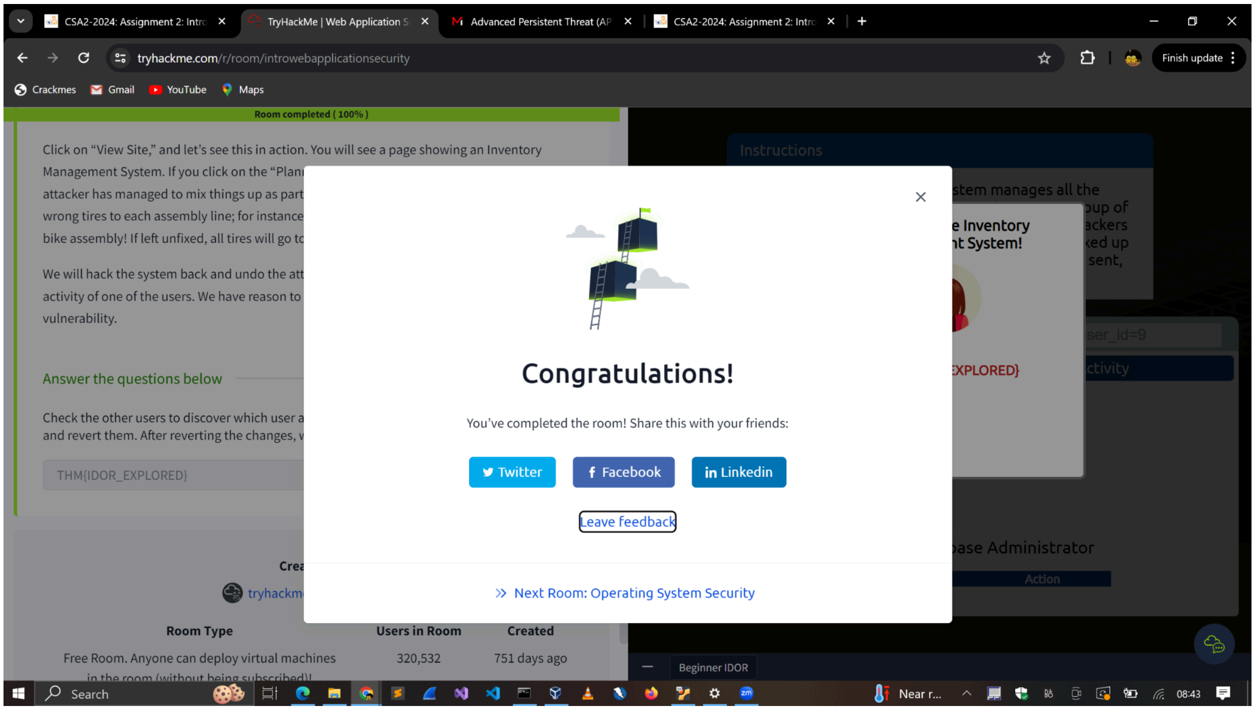
» Next Room: Intro to Defensive Security

Task 1 ✓ What is Offensive Security

Task 2 ✓ Hacking your first machin

Task 3 ✓ Careers in cyber security

How can I start learning?


CSA2-2024: Assignment 2: Intro
TryHackMe | Web Application S
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introwebapplicationsecurity
Finish update
Crackmes
Gmail
YouTube
Maps
Search
Near r...
08:43

Room completed (100%)

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 "Plan
attacker has managed to mix things up as part
wrong tires to each assembly line; for instance
bike assembly! If left unfixed, all tires will go to

We will hack the system back and undo the att
activity of one of the users. We have reason to
vulnerability.

Answer the questions below

Check the other users to discover which user a
and revert them. After reverting the changes, v

THM{IDOR_EXPLORED}

Instructions

stem manages all the
oup of
e Inventory
ackers
nt System!
ked up
sent,

XPLORED}

ser_id=9

ctivity

base Administrator

Action

Crea
tryhackm

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	320,532	751 days ago

Beginner IDOR

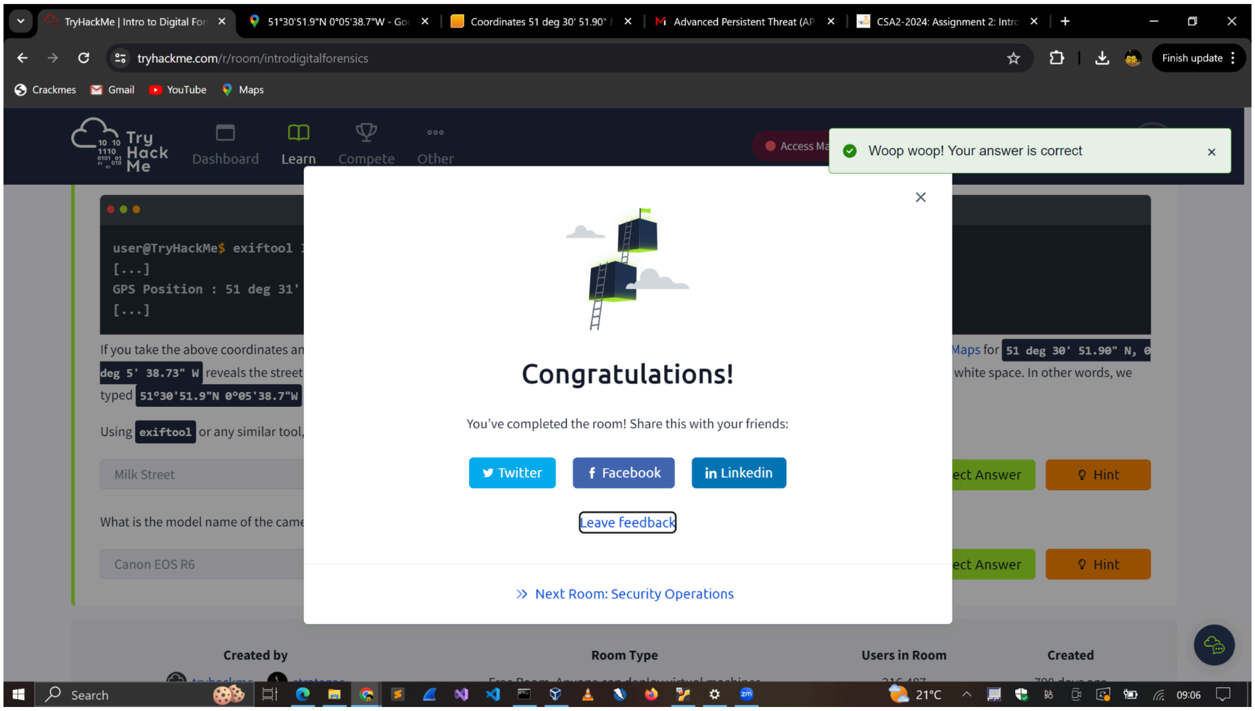
Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook in Linkedin

Leave feedback

» Next Room: Operating System Security


TryHackMe | Intro to Digital For
51°30'51.9"N 0°05'38.7"W - Go
Coordinates 51 deg 30' 51.90"
Advanced Persistent Threat (AP
CSA2-2024: Assignment 2: Intro
tryhackme.com/r/room/introdigitalforensics
Finish update
Crackmes
Gmail
YouTube
Maps
Try Hack Me
Dashboard
Learn
Compete
Other
Access Ma
Search
21°C
09:06

Woop woop! Your answer is correct

```
user@TryHackMe$ exiftool 
[...]
GPS Position : 51 deg 31'
[...]
```

If you take the above coordinates an Maps for `51 deg 30' 51.90" N, 0`
`deg 5' 38.73" W` reveals the street white space. In other words, we
typed `51°30'51.9"N 0°05'38.7"W`

Using `exiftool` or any similar tool,

Milk Street

ect Answer Hint

What is the model name of the came

Canon EOS R6

ect Answer Hint

Created by	Room Type	Users in Room	Created

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook in Linkedin

Leave feedback

» Next Room: Security Operations

4. CONCLUSION

This was a very insightful lesson on the introduction to cybersecurity. I have learnt about directory enumeration, which is discovering hidden directories within a web application that could provide a way to gain unauthorised access. I learned how to achieve this using a tool called **gobuster**. Additionally, I have learned about web application security risks and vulnerabilities like Brocken access control and Cryptographic failures and managed to exploit an IDOR vulnerability within a web application. Lastly, I learned about digital forensics and how to use tools like **exiftool and pdfinfo** to investigate the metadata information of files.

This was a fun experience, and I look forward to exploiting more web vulnerabilities and catching attackers with more digital forensics skills.