

INTRODUCTION TO CYBERSECURITY

INTRODUCTION TO OFFENSIVE SECURITY

offensive security is the process of breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access to them.

Q & A

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

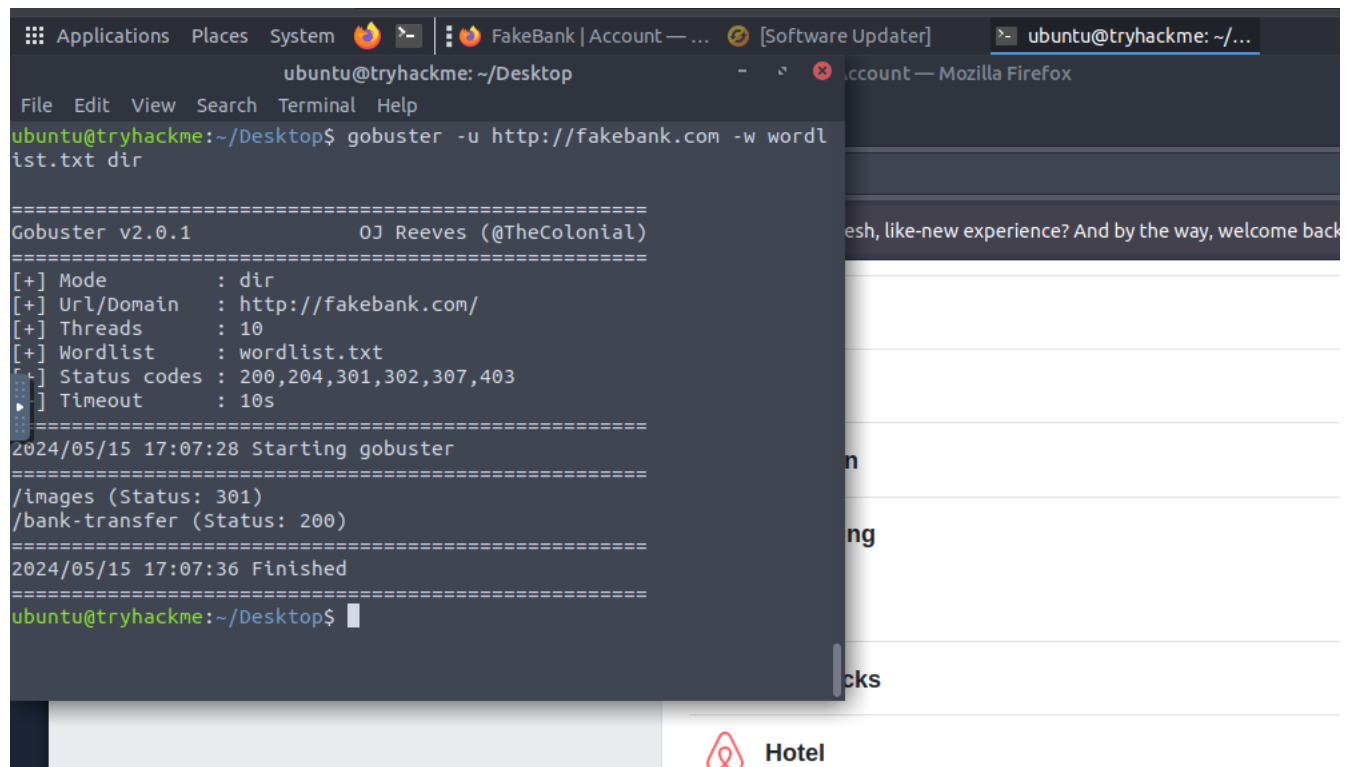
- Offensive Security
- Defensive Security

Offensive Security

✓ Correct Answer

Now in the next task I was supposed to hack into a bank and do some transfer. Now I was presented with a web page called fakebank.com.

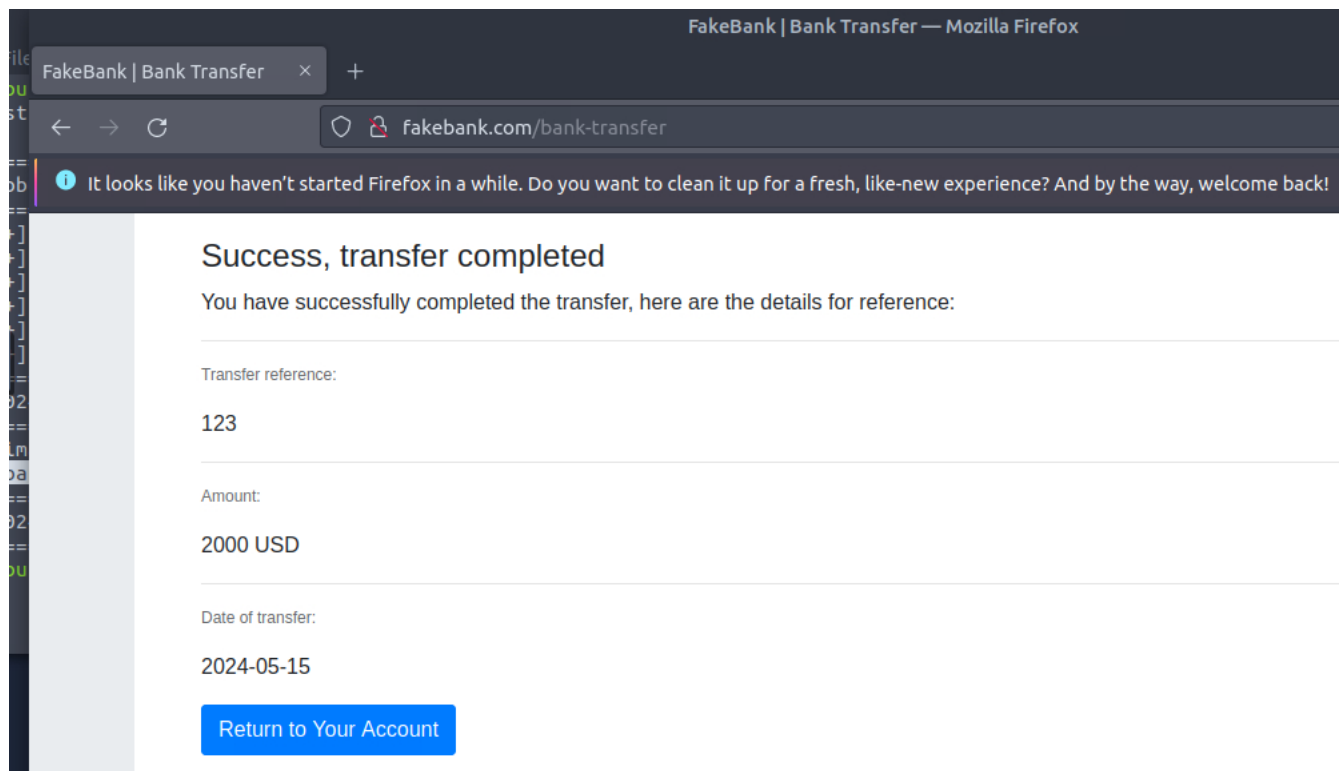
I checked for hidden directories by bruteforcing for hidden directories using the gobuster tool and luckily enough, there was a hidden directory.



```
ubuntu@tryhackme: ~/Desktop
File Edit View Search Terminal Help
ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.txt -t dir

=====
Gobuster v2.0.1                OJ Reeves (@TheColonial)
=====
[+] Mode          : dir
[+] Url/Domain     : http://fakebank.com/
[+] Threads       : 10
[+] Wordlist       : wordlist.txt
[+] Status codes  : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2024/05/15 17:07:28 Starting gobuster
=====
/images (Status: 301)
/bank-transfer (Status: 200)
=====
2024/05/15 17:07:36 Finished
=====
ubuntu@tryhackme:~/Desktop$
```

Visiting the url path having /bank-transfer, I am presented with a transaction webpage.



And as you can see I successfully transferred money to my account.

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED



Congratulations - you hacked the bank!

The answer to the TryHackMe question is **BANK-HACKED**

\$767.68

Account balance

Transactions

Today



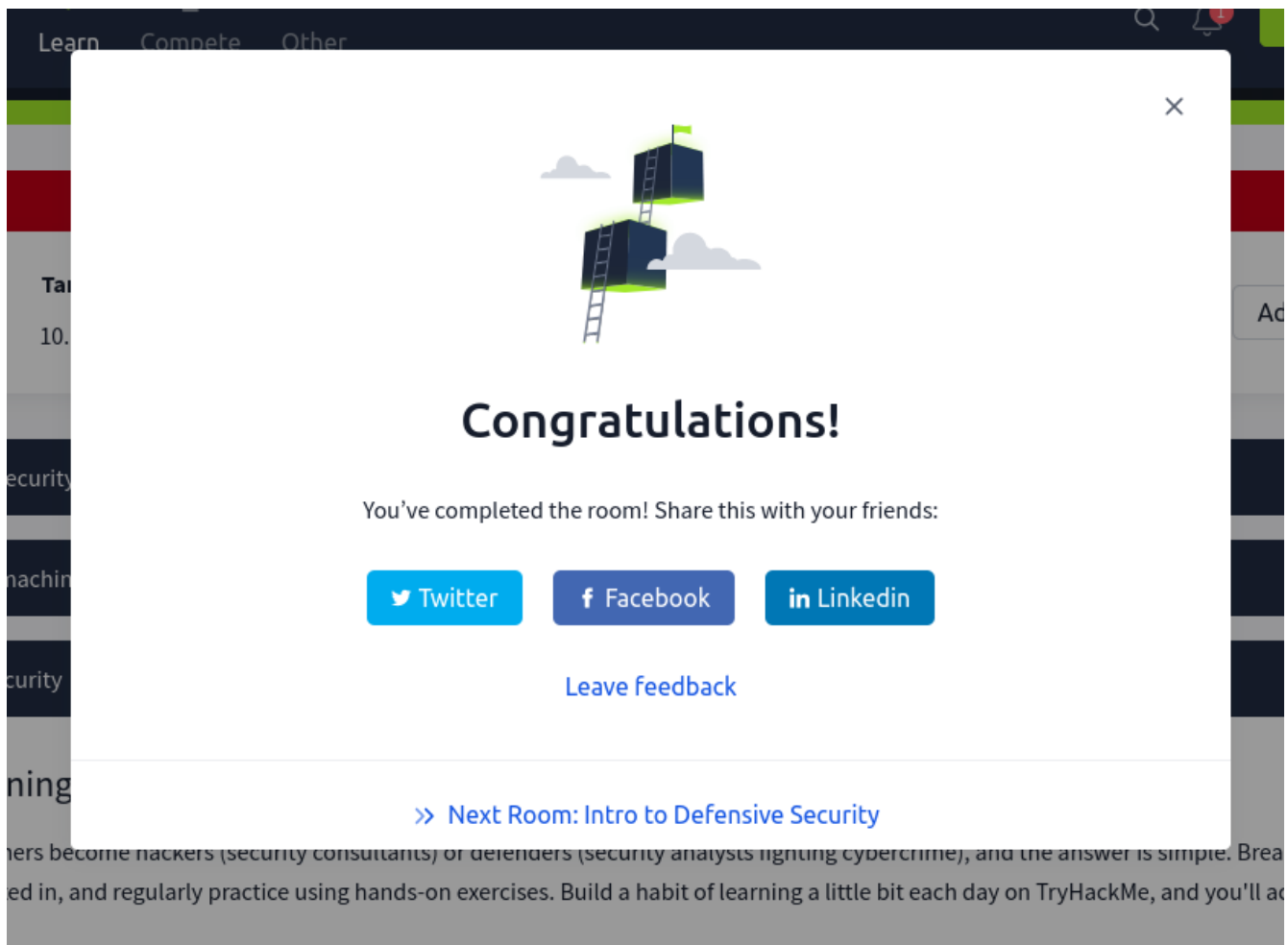
FakeBank (Staff)

+\$2000.00

X

NOTE: This website had a INFORMATION DISCLOSURE or SENSITIVE DATA EXPOSURE vulnerability that an attacker can abuse to gain access to sensitive information that are not ment for normal users.

I exploited this vulnerability and boom! Managed to transact.



WEB APPLICATION SECURITY

INTRODUCTION

In today's interconnected world, 90% of programs run on web applications and for that reason here comes the need for security of the data and informations that are exchanged.

Q & A

What do you need to access a web application?

browser

✓ Correct Answer

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 Failures

✓ Correct Answer

q

since we are dealing with data over the internet, there is a great need for encryption of this data so that it might be of no sense to any one who tempts to intercept. And here cryptography come to play a handy job.

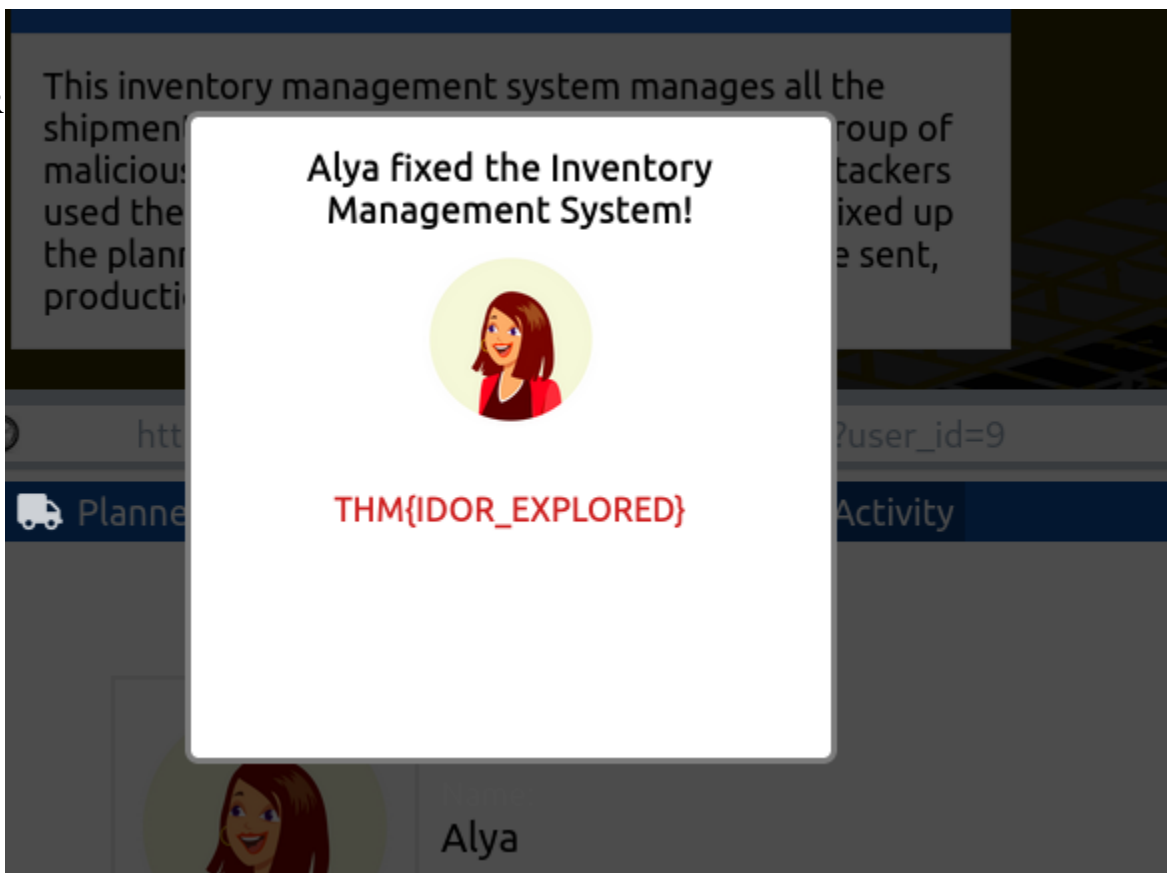
Check the other users to discover which user account was used to make the malicious changes and revert them. After reverting the changes, what is the flag that you have received?

THM{IDOR_EXPLORED}

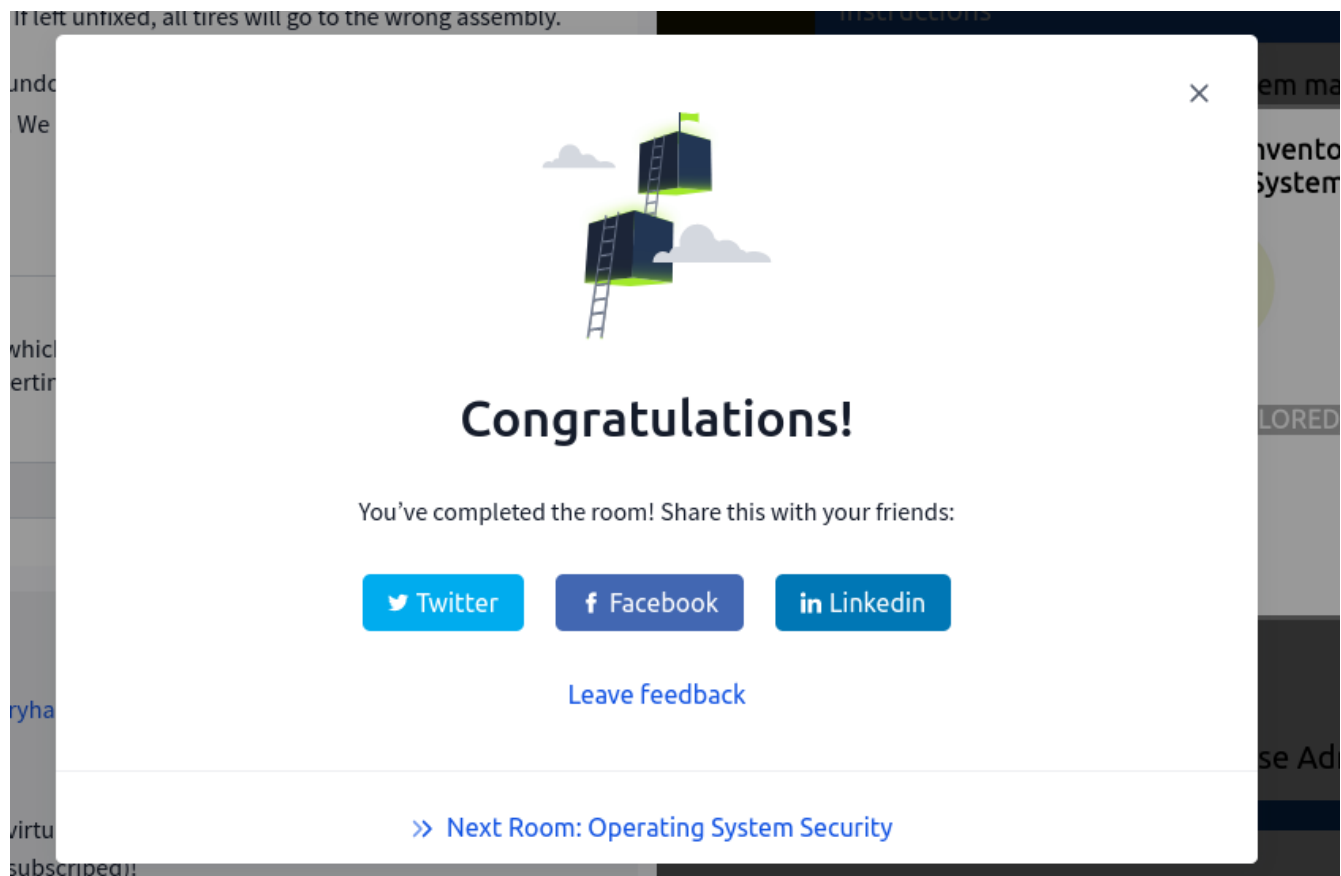
✓ Correct Answer

🔍 Hint

IDOR



occurs when an application exposes a reference to an internal object, such as a file, database record, or URL, and relies solely on user input to determine access to the object without verifying if the user is authorized to access it, of which it should not be the case.



INTRODUCTION TO DIGITAL FORENSICS

INTRODUCTION

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*.

Q & A

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

laptop

✓ Correct Answer

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

✓ Correct Answer

Using `pdftinfo`, find out the author of the attached PDF file, `ransom-letter.pdf`.

Ann Gree Shepherd

✓ Correct Answer

```
(root@kali)~[/home/mwabe/CyberShujaa/THM]
```

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

Canon EOS R6

✓ Correct Answer

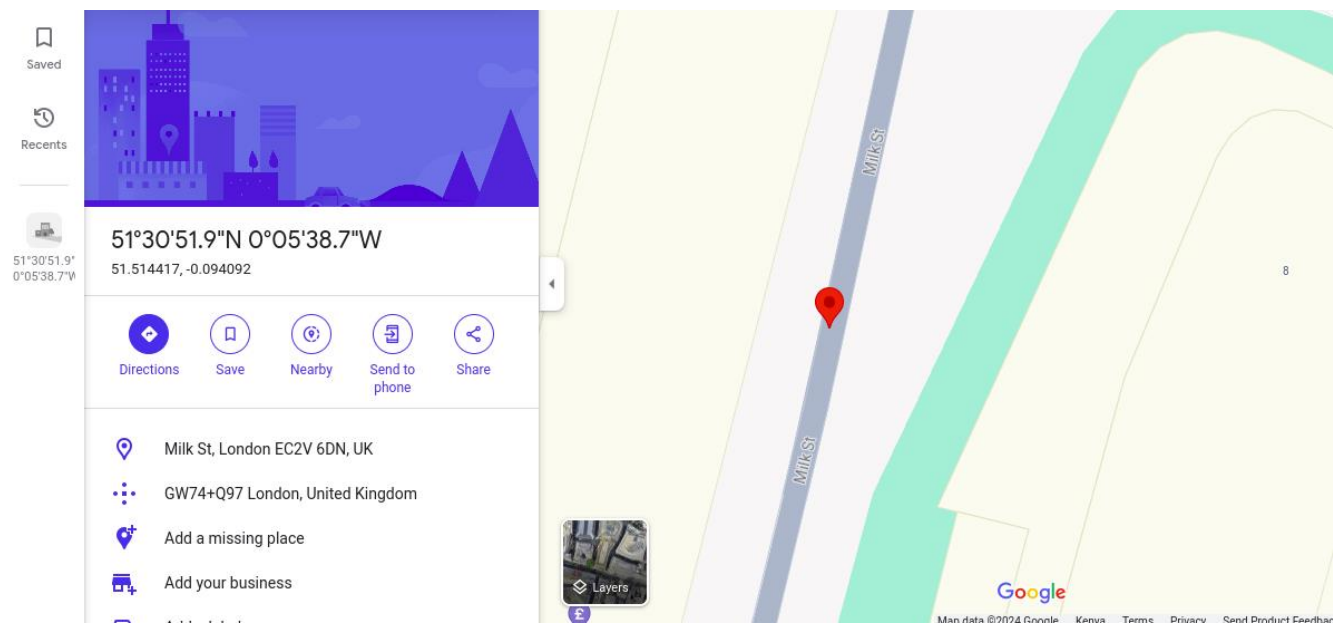
```
Author: Ann Gree Shepherd
Creator: Microsoft® Word 2016
```

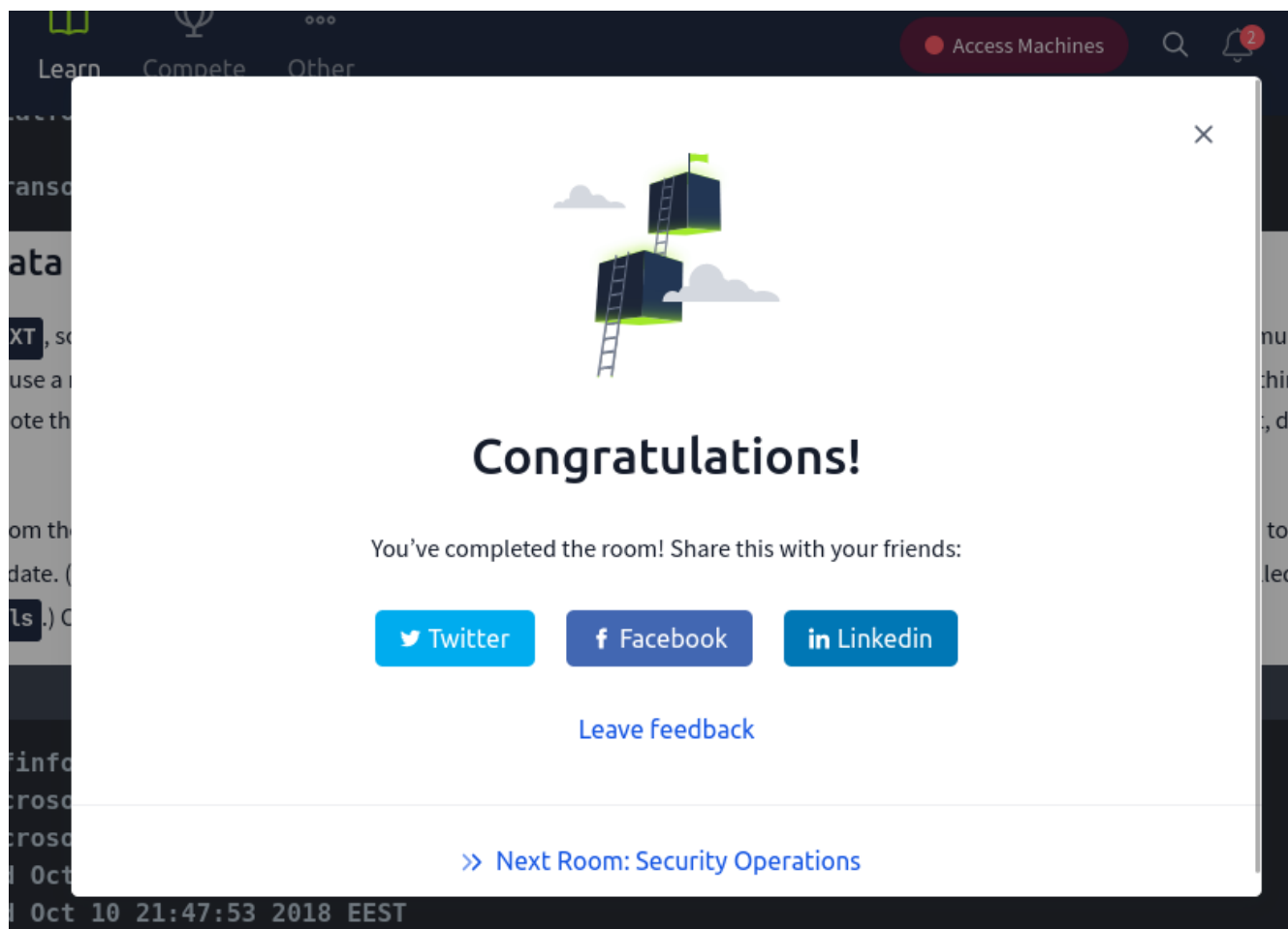
```
(root@kali)~[/home/mwabe/CyberShujaa/THM]
# exiftool letter-image.jpg
ExifTool Version Number      : 12.76
File Name                    : letter-image.jpg
Directory                    : .
File Size                    : 127 kB
File Modification Date/Time   : 2022:02:23 11:53:33+03:00
File Access Date/Time        : 2022:02:23 12:12:00+03:00
File Inode Change Date/Time   : 2024:05:16 07:48:48+03:00
File Permissions              : -rwxr-xr-x
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
```

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?

milk street

✓ Correct Answer





d

CONCLUSION

This room has given hands-on and general introduction to:

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