

## Introduction To Cybersecurity

### 1. Intro to offensive security

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

To beat a hacker, you need to behave like a hacker, finding vulnerabilities and recommending patches before a cybercriminal does, as you'll do in this room!

On the flip side, there is also defensive security, which is 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 a defensive cyber role, you could be investigating infected computers or devices to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.

The screenshot shows the TryHackMe website interface. The browser's address bar displays the URL `tryhackme.com/r/room/introtooffensesecurity`. The website's navigation bar includes links for Dashboard, Learn, Compete, and Other, along with a search icon, a 'Go Premium' button, and a user profile icon. The main content area contains the following text:

On the flip side, there is also defensive security, which is 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 a defensive cyber role, you could be investigating infected computers or devices to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.

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?

- Offensive Security
- Defensive Security

The 'Offensive Security' option is selected, and a green button labeled 'Correct Answer' is visible.

Below the quiz, there are two task cards:

- Task 2: Hacking your first machine
- Task 3: Careers in cyber security

At the bottom, a table provides room statistics:

| Created by    | Room Type   | Users In Room | Created      |
|---------------|---|---------------|--------------|
| ben tryhackme | Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 1,383,390     | 766 days ago |

Spotify - / x (57) What x Inbox (6 x Dashboard x CSA2-20 x How to In x TryHackMe x Word | M x onedrive x Halsey x +

tryhackme.com/r/room/introtooffensivesecurity

TryHackMe Dashboard Learn Compete Other

Go Premium 1

Stuck? See video

This page allows an attacker to steal money from any bank account, which is a critical risk for the bank. As an ethical hacker, you would (with permission) find vulnerabilities in their application and report them to the bank to fix before a hacker exploits them.

Transfer \$2000 from the bank account 2276, to your account (account number 8881).

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?

BANK-HACKED ✓ Correct Answer ? Hint

If you were a penetration tester or security consultant, this is an exercise you'd perform for companies to test for vulnerabilities in their web applications; find hidden pages to investigate for vulnerabilities.

No answer needed ✓ Correct Answer

Terminate the machine by clicking the red "Terminate" button at the top of the page.

No answer needed ✓ Correct Answer

Task 3 Careers in cyber security

Spotify - / x (57) What x Inbox (6 x Dashboard x CSA2-20 x How to In x TryHackMe x Word | M x onedrive x Halsey x +

tryhackme.com/r/room/introtooffensivesecurity

TryHackMe Dashboard Learn Compete Other

Go Premium 1

- Kassandra went from a music teacher to a security professional. [Read more.](#)
- Brandon used TryHackMe while at school to get his first job in cyber. [Read more.](#)

### What careers are there?

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

- Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

Answer the questions below

Read the above, and continue with the next room!

No answer needed ✓ Correct Answer

| Created by    | Room Type   | Users in Room | Created      |
|---------------|---|---------------|--------------|
| ben tryhackme | Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 1,383,390     | 766 days ago |

Copyright TryHackMe 2018-2024

Twitter LinkedIn Discord Facebook YouTube Instagram Pinterest

Shareable Link - <http://www.tryhackme.com/r/room/introtooffensivesecurity>

Conclusion

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

- Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
- Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
- Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

## **2. Web application security**

A web application is like a “program” that we can use without installation as long as we have a modern standard web browser, such as Firefox, Safari, or Chrome. Consequently, instead of installing every program you need, you only need to browse the related page. The following are some examples of web applications:

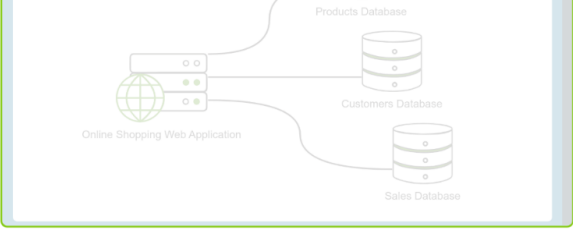
- Webmail such as Tutanota, Protonmail, Outlook, and Gmail
- Online office suites such as Microsoft Office 365 (Word, Excel, and PowerPoint), Google Drive (Docs, Sheets, and Slides), and Zoho Office (Writer, Sheet, and Show)
- Online shopping such as Amazon.com, AliExpress, and Etsy

Spot: x (57) x Inbo: x Dash: x CSA: x How: x TryH: x Wor: x Intro: x oned: x D: x New: x New: x +

tryhackme.com/r/room/introwebapplicationsecurity

TryHackMe Dashboard Learn Compete Other

Go Premium 1



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?

Browser

✓ Correct Answer

Task 2 Web Application Security Risks

Spot: x (57) x Inbo: x Dash: x CSA: x How: x TryH: x Wor: x Intro: x oned: x D: x New: x New: x +

tryhackme.com/r/room/introwebapplicationsecurity

TryHackMe Dashboard Learn Compete Other

Go Premium 1

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?

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

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 in the room (without being subscribed)! | 327,623       | 766 days ago |

Copyright TryHackMe 2018-2024

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?

THM{IDOR\_EXPLORED} ✓ Correct Answer 🔍 Hint

| Created by           | Room Type   | Users in Room | Created      |
|----------------------|---|---------------|--------------|
| tryhackme  strategos | Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 327,623       | 766 days ago |

Copyright TryHackMe 2018-2024

## Conclusion

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.

## 3. Intro 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*.

Think about the following scenario. The law enforcement agents arrive at a crime scene; however, part of this crime scene includes digital devices and media. Digital devices include desktop computers, laptops, digital cameras, music players, and

smartphones, to name a few. Digital media includes CDs, DVDs, USB flash memory drives, and external storage. A few questions arise:

- How should the police collect digital evidence, such as smartphones and laptops? What are the procedures to follow if the computer and smartphone are running?
- How to transfer the digital evidence? Are there certain best practices to follow when moving computers, for instance?
- How to analyze the collected digital evidence? Personal device storage ranges between tens of gigabytes to several terabytes; how can this be analyzed?

The screenshot shows a web browser window with the URL `tryhackme.com/r/room/introdigitalforensics`. The page features a dark blue header with navigation links: Dashboard, Learn, Compete, and Other. A red button labeled 'Access Machines' and a green 'Go Premium' button are also visible. Below the header, there is a large image of a desk with a smartphone, a camera, and SD cards. A text prompt 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 text input field contains the word 'laptop', and a green 'Correct Answer' button is visible. Below the input field, there are two task cards: 'Task 2: Digital Forensics Process' and 'Task 3: Practical Example of Digital Forensics'. At the bottom, a table provides room statistics:

| Created by           | Room Type   | Users in Room | Created      |
|----------------------|---|---------------|--------------|
| tryhackme  strategos | Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! | 220,344       | 806 days ago |

John\_Mbithi\_Mutave

**Shareable link - <https://t.co/tzfS5tMXwv>**

## Conclusion

Digital forensics is the application of computer science to investigate digital evidence for a legal purpose. Digital forensics is used in two types of investigations:

1. **Public-sector investigations** refer to the investigations carried out by government and law enforcement agencies. They would be part of a crime or civil investigation.
2. **Private-sector investigations** refer to the investigations carried out by corporate bodies by assigning a private investigator, whether in-house or outsourced. They are triggered by corporate policy violations.

Whether investigating a crime or a corporate policy violation, part of the evidence is related to digital devices and digital media. This is where digital forensics comes into play and tries to establish what has happened. Without trained digital forensics investigators, it won't be possible to process any digital evidence properly.