**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.

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

Step 1) Open a terminal

A terminal, also known as the command-line, allows us to interact with a computer without using a graphical user interface. On the machine, open the terminal using the Terminal icon: 

Stuck? See video

Step 2) Find hidden website pages

Most companies will have an admin portal page, giving their staff access to basic admin controls for day-to-day operations. For a bank, an employee might need to transfer money to and from client accounts. Often these pages are not made private, allowing attackers to find hidden pages that show, or give access to, admin controls or sensitive data.

Type the following command into the terminal to find potentially hidden pages on FakeBank's website using GoBuster (a command-line security application).

gobuster -u http://fakebank.com -w wordlist.txt dir

The command will run and show you an output similar to this:

GoBuster command to brute-force website pages

**ubuntu@tryhackme:~/Desktop$ gobuster -u http://fakebank.com -w wordlist.txt dir**

**=====================================================**

**Gobuster v2.0.1**

**=====================================================**

**[+] Mode : dir**

**[+] Url/Domain : http://fakebank.com/**

**[+] Threads : 10**

**[+] Wordlist : wordlist.txt**

**[+] Status codes : 200,204,301,302,307,403**

**[+] Timeout : 10s**

**=====================================================**

**2022/04/11 18:23:28 Starting gobuster**

**=====================================================**

**/images (Status: 301)**

**/DIRECTORY\_NAME\_OUTPUT (Status: 200)**

**=====================================================**

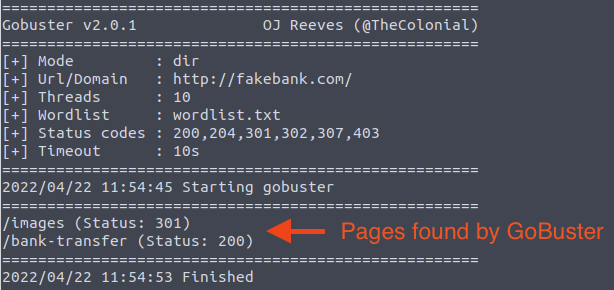
**2022/04/11 18:23:38 Finished**

**=====================================================**

*Don't worry if you have not used a terminal before - TryHackMe walks you through everything!*

In the command above, **-u** is used to state the website we're scanning, **-w** takes a list of words to iterate through to find hidden pages.

You will see that GoBuster scans the website with each word in the list, finding pages that exist on the site. GoBuster will have told you the pages it found in the list of page/directory names (indicated by Status: 200).



Step 3) Hack the bank

You should have found a secret bank transfer page that allows you to transfer money between accounts at the bank (/bank-transfer). Type the hidden page into the FakeBank website on the machine.

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?

http://fakebank.com/bank-transfer

BANK-HACKED

How can I start learning?

People often wonder how others become hackers (security consultants) or defenders (security analysts fighting cybercrime), and the answer is simple. Break it down, learn an area of cyber security you're interested in, and regularly practice using hands-on exercises. Build a habit of learning a little bit each day on TryHackMe, and you'll acquire the knowledge to get your first job in the industry.

Trust us; you can do it! Just take a look at some people who have used TryHackMe to get their first security job:

* Paul went from a construction worker to a security engineer. [Read more](https://tryhackme.com/resources/blog/construction-worker-to-security-engineer-how-paul-used-tryhackme-to-land-his-first-job-in-security).
* Kassandra went from a music teacher to a security professional. [Read more](https://tryhackme.com/resources/blog/the-teacher-becomes-the-student).
* Brandon used TryHackMe while at school to get his first job in cyber. [Read more](https://tryhackme.com/resources/blog/brandons-success-story).

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.

**2-Intro to Defensive Security**

Offensive security focuses on one thing: breaking into systems. Breaking into systems might be achieved through exploiting bugs, abusing insecure setups, and taking advantage of unenforced access control policies, among other things. Red teams and penetration testers specialize in offensive security.

Defensive security is somewhat the opposite of offensive security, as it is concerned with two main tasks:

1. Preventing intrusions from occurring
2. Detecting intrusions when they occur and responding properly

Blue teams are part of the defensive security landscape.

Some of the tasks that are related to defensive security include:

* User cyber security awareness: Training users about cyber security helps protect against various attacks that target their systems.
* Documenting and managing assets: We need to know the types of systems and devices that we have to manage and protect properly.
* Updating and patching systems: Ensuring that computers, servers, and network devices are correctly updated and patched against any known vulnerability (weakness).
* Setting up preventative security devices: firewall and intrusion prevention systems (IPS) are critical components of preventative security. Firewalls control what network traffic can go inside and what can leave the system or network. IPS blocks any network traffic that matches present rules and attack signatures.
* Setting up logging and monitoring devices: Without proper logging and monitoring of the network, it won’t be possible to detect malicious activities and intrusions. If a new unauthorized device appears on our network, we should be able to know.

There is much more to defensive security, and the list above only covers a few common topics.

In this room, we cover:

* Security Operations Center (SOC)
* Threat Intelligence
* Digital Forensics and Incident Response (DFIR)
* Malware Analysis

Answer the questions below

Which team focuses on defensive security?

Top of Form

Blue Team

In this task, we will cover two main topics related to defensive security:

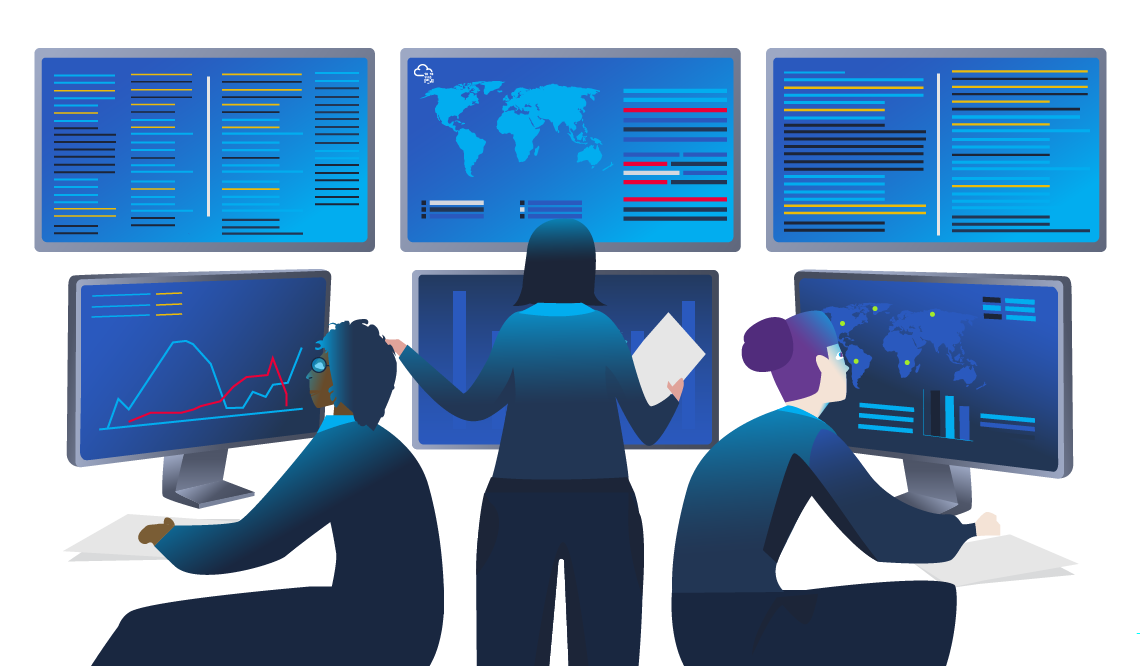
* Security Operations Center (SOC), where we cover Threat Intelligence
* Digital Forensics and Incident Response (DFIR), where we also cover Malware Analysis

### **Security Operations Center (SOC)**

A Security Operations Center (SOC) is a team of cyber security professionals that monitors the network and its systems to detect malicious cyber security events. Some of the main areas of interest for a SOC are:

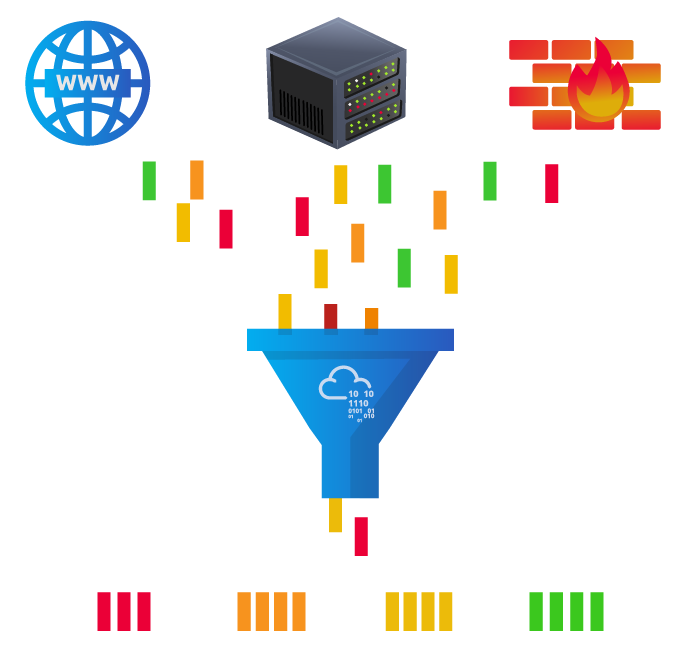
* Vulnerabilities: Whenever a system vulnerability (weakness) is discovered, it is essential to fix it by installing a proper update or patch. When a fix is not available, the necessary measures should be taken to prevent an attacker from exploiting it. Although remediating vulnerabilities is of vital interest to a SOC, it is not necessarily assigned to them.
* Policy violations: We can think of a security policy as a set of rules required for the protection of the network and systems. For example, it might be a policy violation if users start uploading confidential company data to an online storage service.
* Unauthorized activity: Consider the case where a user’s login name and password are stolen, and the attacker uses them to log into the network. A SOC needs to detect such an event and block it as soon as possible before further damage is done.
* Network intrusions: No matter how good your security is, there is always a chance for an intrusion. An intrusion can occur when a user clicks on a malicious link or when an attacker exploits a public server. Either way, when an intrusion occurs, we must detect it as soon as possible to prevent further damage.

Security operations cover various tasks to ensure protection; one such task is threat intelligence.



#### **Threat Intelligence**

In this context, intelligence refers to information you gather about actual and potential enemies. A threat is any action that can disrupt or adversely affect a system. Threat intelligence aims to gather information to help the company better prepare against potential adversaries. The purpose would be to achieve a threat-informed defense. Different companies have different adversaries. Some adversaries might seek to steal customer data from a mobile operator; however, other adversaries are interested in halting the production in a petroleum refinery. Example adversaries include a nation-state cyber army working for political reasons and a ransomware group acting for financial purposes. Based on the company (target), we can expect adversaries.



Intelligence needs data. Data has to be collected, processed, and analyzed. Data collection is done from local sources such as network logs and public sources such as forums. Processing of data aims to arrange them into a format suitable for analysis. The analysis phase seeks to find more information about the attackers and their motives; moreover, it aims to create a list of recommendations and actionable steps.

Learning about your adversaries allows you to know their tactics, techniques, and procedures. As a result of threat intelligence, we identify the threat actor (adversary), predict their activity, and consequently, we will be able to mitigate their attacks and prepare a response strategy.

### **Digital Forensics and Incident Response (DFIR)**

This section is about Digital Forensics and Incident Response (DFIR), and we will cover:

* Digital Forensics
* Incident Response
* Malware Analysis

#### **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.

In defensive security, the focus of digital forensics shifts to analyzing evidence of an attack and its perpetrators and other areas such as intellectual property theft, cyber espionage, and possession of unauthorized content. Consequently, digital forensics will focus on different areas such as:

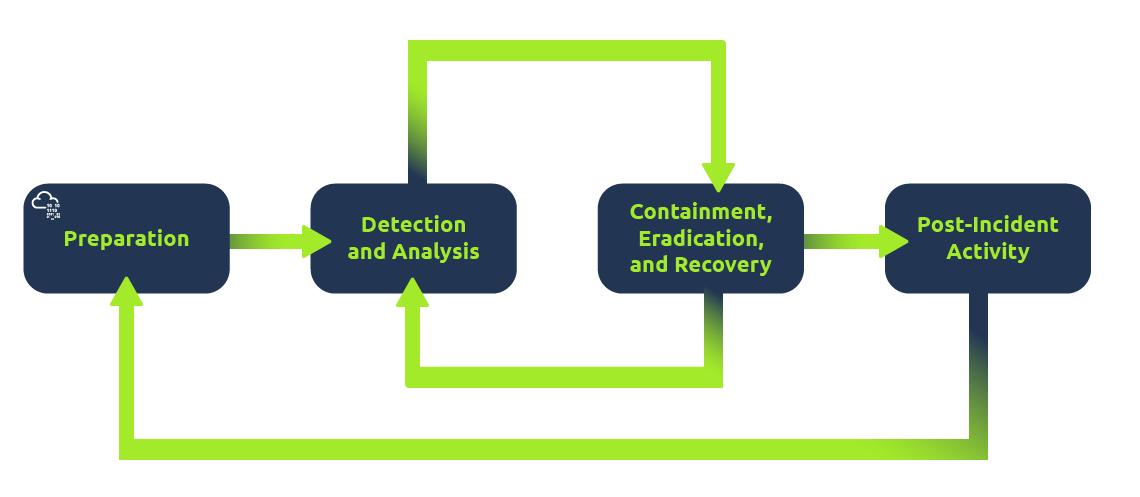
* File System: Analyzing a digital forensics image (low-level copy) of a system’s storage reveals much information, such as installed programs, created files, partially overwritten files, and deleted files.
* System memory: If the attacker is running their malicious program in memory without saving it to the disk, taking a forensic image (low-level copy) of the system memory is the best way to analyze its contents and learn about the attack.
* System logs: Each client and server computer maintains different log files about what is happening. Log files provide plenty of information about what happened on a system. Some traces will be left even if the attacker tries to clear their traces.
* Network logs: Logs of the network packets that have traversed a network would help answer more questions about whether an attack is occurring and what it entails.

#### **Incident Response**

An incident usually refers to a data breach or cyber attack; however, in some cases, it can be something less critical, such as a misconfiguration, an intrusion attempt, or a policy violation. Examples of a cyber attack include an attacker making our network or systems inaccessible, defacing (changing) the public website, and data breach (stealing company data). How would you respond to a cyber attack? Incident response specifies the methodology that should be followed to handle such a case. The aim is to reduce damage and recover in the shortest time possible. Ideally, you would develop a plan ready for incident response.

The four major phases of the incident response process are:

1. Preparation: This requires a team trained and ready to handle incidents. Ideally, various measures are put in place to prevent incidents from happening in the first place.
2. Detection and Analysis: The team has the necessary resources to detect any incident; moreover, it is essential to further analyze any detected incident to learn about its severity.
3. Containment, Eradication, and Recovery: Once an incident is detected, it is crucial to stop it from affecting other systems, eliminate it, and recover the affected systems. For instance, when we notice that a system is infected with a computer virus, we would like to stop (contain) the virus from spreading to other systems, clean (eradicate) the virus, and ensure proper system recovery.
4. Post-Incident Activity: After successful recovery, a report is produced, and the learned lesson is shared to prevent similar future incidents.



#### **Malware Analysis**

Malware stands for malicious software. Software refers to programs, documents, and files that you can save on a disk or send over the network. Malware includes many types, such as:

* Virus is a piece of code (part of a program) that attaches itself to a program. It is designed to spread from one computer to another; moreover, it works by altering, overwriting, and deleting files once it infects a computer. The result ranges from the computer becoming slow to unusable.
* Trojan Horse is a program that shows one desirable function but hides a malicious function underneath. For example, a victim might download a video player from a shady website that gives the attacker complete control over their system.
* Ransomware is a malicious program that encrypts the user’s files. Encryption makes the files unreadable without knowing the encryption password. The attacker offers the user the encryption password if the user is willing to pay a “ransom.”



Malware analysis aims to learn about such malicious programs using various means:

1. Static analysis works by inspecting the malicious program without running it. Usually, this requires solid knowledge of assembly language (processor’s instruction set, i.e., computer’s fundamental instructions).
2. Dynamic analysis works by running the malware in a controlled environment and monitoring its activities. It lets you observe how the malware behaves when running.

Answer the questions below

What would you call a team of cyber security professionals that monitors a network and its systems for malicious events?

**Security Operations Center**

Bottom of Form

What does DFIR stand for?

Top of Form

### **Digital Forensics and Incident Response**

Bottom of Form

Which kind of malware requires the user to pay money to regain access to their files?

**ransomware**

Top of Form

What would be a typical task that you will be doing as a security analyst? Click on “View Site” to follow along until you get the flag. (If this is your first time obtaining flags, a flag can be seen as a string of text you receive once you accomplish a task. An example flag is **FLAG{WORDS\_AND\_MORE}**.)

View Site



You are part of a *Security Operations Center* (SOC) responsible for protecting a bank. This bank’s SOC uses a *Security Information and Event Management* (SIEM) system. A SIEM gathers security-related information and events from various sources and presents them via one system. For instance, you would be notified if there is a failed login attempt or a login attempt from an unexpected geographic location. Moreover, with the advent of machine learning, a SIEM might detect unusual behavior, such as a user logging in at 3 AM when he usually logs in only during work hours.

In this exercise, we will interact with a SIEM to monitor the different events on our network and systems in real-time. Some of the events are typical and harmless; others might require further intervention from us. Find the event flagged in red, take note of it, and click on it for further inspection.

Next, we want to learn more about the suspicious activity or event. The suspicious event might have been triggered by an event, such as a local user, a local computer, or a remote IP address. To send and receive postal mail, you need a physical address; similarly, you need an IP address to send and receive data over the Internet. An IP address is a logical address that allows you to communicate over the Internet. We inspect the cause of the trigger to confirm whether the event is indeed malicious. If it is malicious, we need to take due action, such as reporting to someone else in the SOC and blocking the IP address.

Answer the questions below

What is the flag that you obtained by following along?

Top of Form

THM{THREAT-BLOCKED}

**3 -Careers in Cyber**

Cyber security careers are becoming more in demand and offer [high salaries](https://tryhackme.com/resources/blog/cyber-security-salary-career-options). There are many different jobs within the security industry, from offensive pentesting (hacking machines and reporting on vulnerabilities) to defensive security (defending against and investigating cyberattacks).

Why get a career in cyber:

* High Pay - jobs in security have high starting salaries
* Exciting - work can include legally hacking systems or defending against cyber attacks
* Be in demand - there are over 3.5 million unfilled cyber positions

This room helps you break into cyber security by providing information about various cyber security roles; it also links to different learning paths that you can use to start building your cyber skills.

**1-Security Analyst**

Security analysts are integral to constructing security measures across organisations to protect the company from attacks. Analysts explore and evaluate company networks to uncover actionable data and recommendations for engineers to develop preventative measures. This job role requires working with various stakeholders to gain an understanding of security requirements and the security landscape.

Responsibilities

* Working with various stakeholders to analyse the cyber security throughout the company
* Compile ongoing reports about the safety of networks, documenting security issues and measures taken in response
* Develop security plans, incorporating research on new attack tools and trends, and measures needed across teams to maintain data security.

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Security Analyst.

* [Introduction to Cyber Security](https://tryhackme.com/path/outline/introtocyber)
* [Pre Security](https://tryhackme.com/path/outline/presecurity/)
* [SOC Level 1](https://tryhackme.com/path/outline/soclevel1)

**2-Security Engineer**

*Design, monitor and maintain security controls, networks, and systems to help prevent cyberattacks*

Security engineers develop and implement security solutions using threats and vulnerability data - often sourced from members of the security workforce. Security engineers work across circumventing a breadth of attacks, including web application attacks, network threats, and evolving trends and tactics. The ultimate goal is to retain and adopt security measures to mitigate the risk of attack and data loss.

Responsibilities

* Testing and screening security measures across software
* Monitor networks and reports to update systems and mitigate vulnerabilities
* Identify and implement systems needed for optimal security

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Security Engineer.

* [SOC Level 1](https://tryhackme.com/path/outline/soclevel1)
* [JR Penetration Tester](https://tryhackme.com/path/outline/jrpenetrationtester)
* [Offensive Pentesting](https://tryhackme.com/path/outline/pentesting)

**3-Incident Responder**

*Identifies and mitigates attacks whilst an attackers operations are still unfolding*

Incident responders respond productively and efficiently to security breaches. Responsibilities include creating plans, policies, and protocols for organisations to enact during and following incidents. This is often a highly pressurised position with assessments and responses required in real-time, as attacks are unfolding. Incident response metrics include MTTD, MTTA, and MTTR - the meantime to detect, acknowledge, and recover (from attacks.) The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber attacks.

Responsibilities

* Developing and adopting a thorough, actionable incident response plan
* Maintaining strong security best practices and supporting incident response measures
* Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Incident Responder.

* [SOC Level 1](https://tryhackme.com/path/outline/soclevel1)

**4-Digital Forensic Examiner**

*Responsible for using digital forensics to investigate incidents and crimes*

If you like to play detective, this might be the perfect job. If you are working as part of a law-enforcement department, you would be focused on collecting and analysing evidence to help solve crimes: charging the guilty and exonerating the innocent. On the other hand, if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.

Responsibilities

* Collect digital evidence while observing legal procedures
* Analyse digital evidence to find answers related to the case
* Document your findings and report on the case

**5-Malware Analyst**

*Analyses all types of malware to learn more about how they work and what they do*

A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. A malware analyst is sometimes called a reverse-engineer as their core task revolves around converting compiled programs from machine language to readable code, usually in a low-level language. This work requires the malware analyst to have a strong programming background, especially in low-level languages such as assembly language and C language. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.

Responsibilities

* Carry out static analysis of malicious programs, which entails reverse-engineering
* Conduct dynamic analysis of malware samples by observing their activities in a controlled environment
* Document and report all the findings

**6-Penetration Tester**

*Responsible for testing technology products for security loopholes*

You may see penetration testing referred to as pentesting and ethical hacking. A penetration tester's job role is to test the security of the systems and software within a company - this is achieved through attempts to uncover flaws and vulnerabilities through systemised hacking. Penetration testers exploit these vulnerabilities to evaluate the risk in each instance. The company can then take these insights to rectify issues to prevent a real-world cyberattack.

Responsibilities

* Conduct tests on computer systems, networks, and web-based applications
* Perform security assessments, audits, and analyse policies
* Evaluate and report on insights, recommending actions for attack prevention

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Penetration Tester.

* [JR Penetration Tester](https://tryhackme.com/path/outline/jrpenetrationtester)
* [Offensive Pentesting](https://tryhackme.com/path/outline/pentesting)

**7-Red Teamer**

*Plays the role of an adversary, attacking an organisation and providing feedback from an enemies perspective*

Red teamers share similarities to penetration testers, with a more targeted job role. Penetration testers look to uncover many vulnerabilities across systems to keep cyber-defence in good standing, whilst red teamers are enacted to test the company's detection and response capabilities. This job role requires imitating cyber criminals' actions, emulating malicious attacks, retaining access, and avoiding detection. Red team assessments can run for up to a month, typically by a team external to the company. They are often best suited to organisations with mature security programs in place.

Responsibilities

* Emulate the role of a threat actor to uncover exploitable vulnerabilities, maintain access and avoid detection
* Assess organisations' security controls, threat intelligence, and incident response procedures
* Evaluate and report on insights, with actionable data for companies to avoid real-world instances

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Red Teamer.

* [JR Penetration Tester](https://tryhackme.com/path/outline/jrpenetrationtester)
* [Offensive Pentesting](https://tryhackme.com/path/outline/pentesting)
* [Red Teamer](https://tryhackme.com/path/outline/redteaming)