TryHackMe — Digital Forensics Fundamentals | Cyber Security 101 (THM)

Z3pH7 · Follow

12 min read · Nov 1, 2024

Listen Share More

Hey everyone! TryHackMe just announced the **NEW Cyber Security 101** learning path, and there are tons of giveaways this time! This article might help you out, but I've kept the summary short for easy understanding. Enjoy hacking!

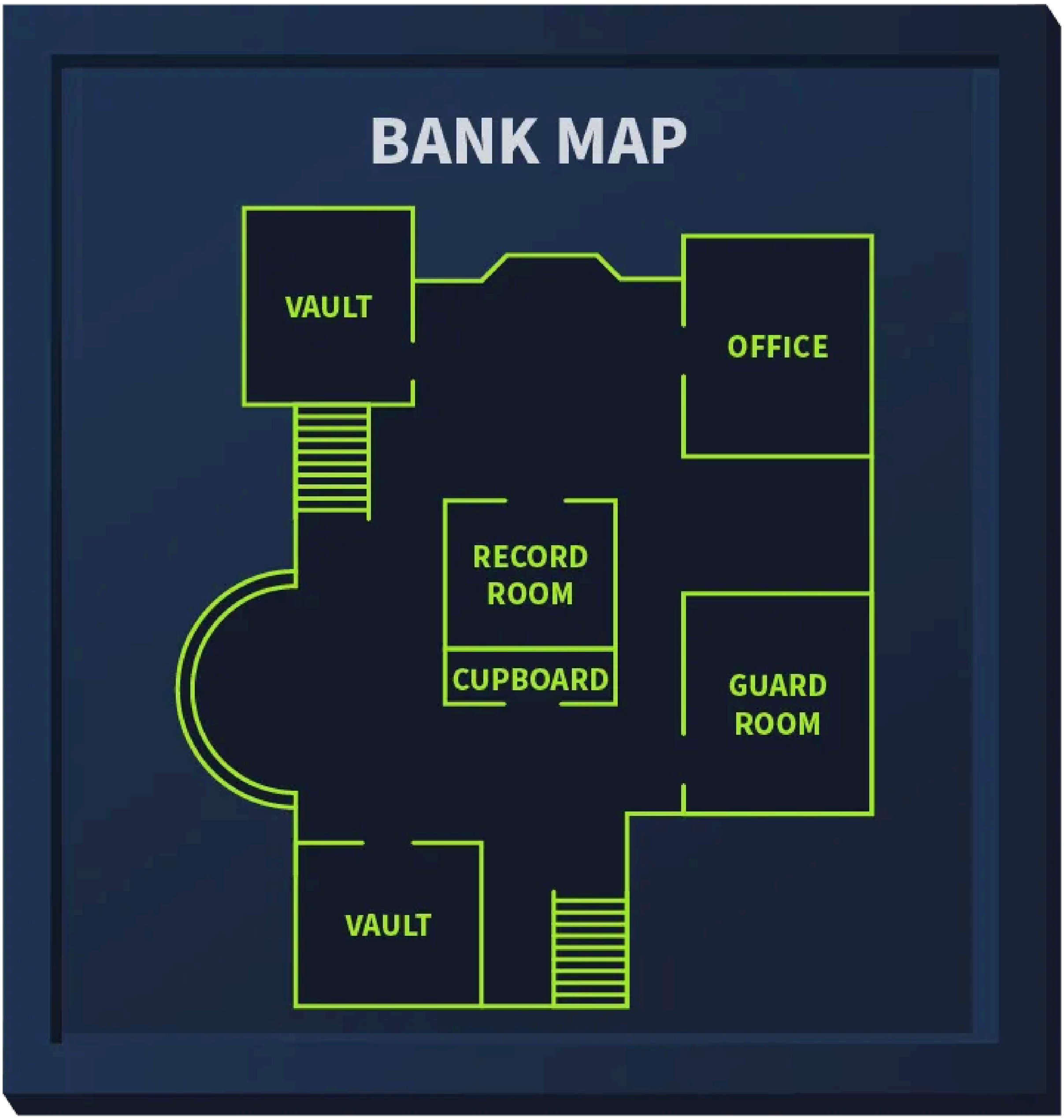
Introduction to Digital Forensics

Forensics is the application of methods and procedures to investigate and solve crimes. The branch of forensics that investigates cyber crimes is known as **digital forensics. Cyber crime** is any criminal activity conducted on or using a digital device. Several tools and techniques are used to investigate digital devices thoroughly after any crime to find and analyze evidence for necessary legal action.

Digital devices have solved many of our problems. Communication all around the globe is just a matter of a text or call. Due to the vast usage of digital devices, besides making life easier, an increase in digital crimes — cyber crimes has also been observed. A variety of crimes are committed using digital devices.

Consider an example where law enforcement agencies raid a bank robber's place with proper search warrants. Some digital devices, including a laptop, mobile phone, hard drive, and a USB, were found in the robber's home. The law enforcement agency handed over the case to the digital forensics team. The team collected evidence securely and conducted a thorough investigation inside their digital forensics lab equipped with forensics tools. The following evidence was found on the digital devices:

- A digital map of the bank was found on the suspect's laptop, which they kept for planning the robbery.
- A document with the bank's entrance and escape routes was found on the suspect's hard drive.
- A document on the hard drive that listed all the bank's physical security controls. The suspect devised plans to bypass the security measures.
- Some media files, including photos and videos of the suspect's previous robberies, were inside the suspect's laptop.
- After conducting a thorough investigation of the suspect's mobile phone, some illegal chat groups and call records related to the bank robbery were also found.



All this evidence helped law enforcement in the legal proceedings of the case. This scenario discusses a case from the start till the end. Some procedures are followed by the digital forensics team while collecting the evidence, storing it, analyzing it, and reporting it. This room will focus on covering the understanding of these procedures. The following are the learning objectives of this room:

Learning Objectives

- Phases of digital forensics
- Types of digital forensics
- Procedure of evidence acquisition
- Windows forensics

- Solving a forensics case

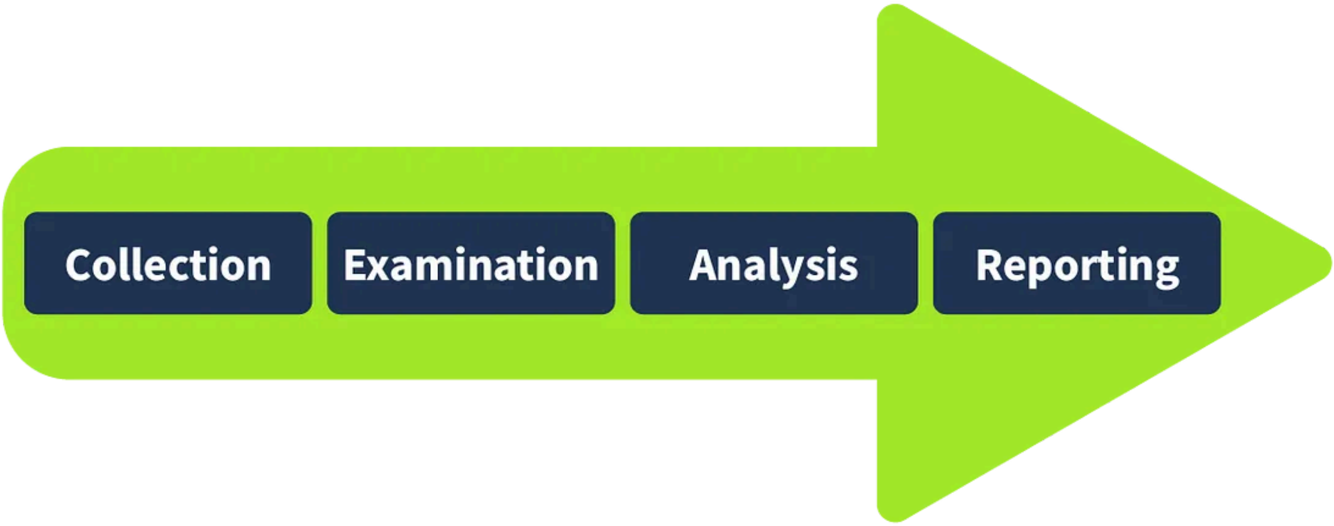
Answer the questions below

> *Which team was handed the case by law enforcement?*

Answer: digital forensics

Digital Forensics Methodology

The digital forensics team has various cases requiring different tools and techniques. However, the National Institute of Standards and Technology (NIST) defines a general process for every case. The NIST works on defining frameworks for different areas of technology, including cyber security, where they introduce the process of digital forensics in four phases.



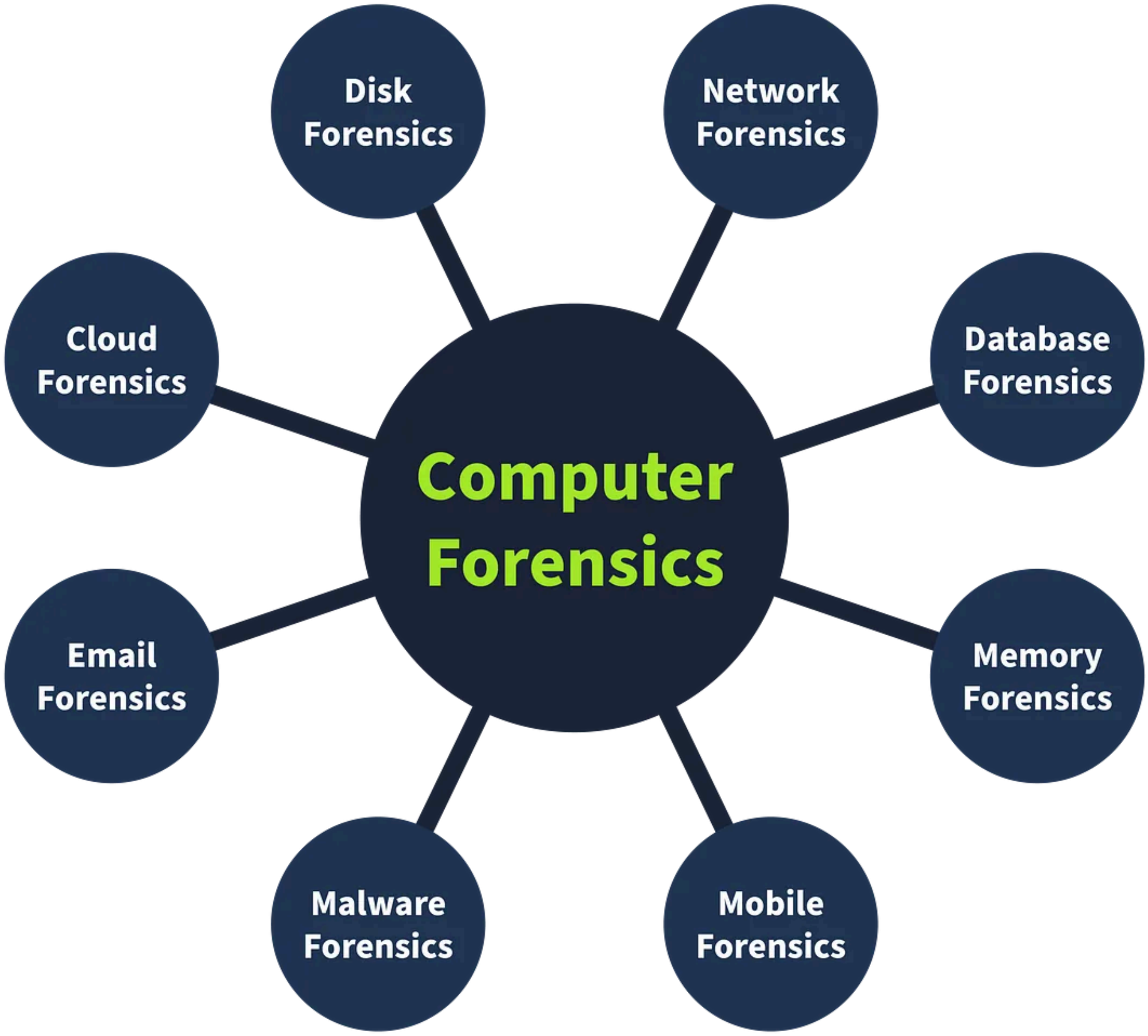
1. **Collection:** The first phase of digital forensics is data collection. Identifying all the devices from which the data can be collected is essential. Usually, an investigator can find personal computers, laptops, digital cameras, USBs, etc., on the crime scene. It is also necessary to ensure the original data is not tampered with while collecting the evidence and to maintain a proper document containing the collected items' details. We will also be discussing the evidence-acquisition procedures in the upcoming tasks.
2. **Examination:** The collected data may overwhelm investigators due to its size. This data usually needs to be filtered, and the data of interest needs to be extracted. For example, as an investigator, you collected all the media files from

a digital camera on the crime scene. You may only require some of the media as you are concerned with the media recorded on a specific date and time. So, in the examination phase, you would filter the media files of the required time and move them to the next phase. Similarly, you may only need the data of a specific user from a system containing numerous user accounts. The examination phase helps you filter this particular data for analysis.

3. **Analysis:** This is a critical phase. The investigators now have to analyze the data by correlating it with multiple pieces of evidence to draw conclusions. The analysis depends upon the case scenario and available data. The analysis aims to extract the activities relevant to the case chronologically.

4. **Reporting:** In the last phase of digital forensics, a detailed report is prepared. This report contains the investigation's methodology and detailed findings from the collected evidence. It may also contain recommendations. This report is presented to law enforcement and executive management. It is important to include executive summaries as part of the report, considering the level of understanding of all the receiving parties.

As part of the collection phase, we saw that various pieces of evidence can be found at the crime scene. Analyzing these multiple categories of evidence requires various tools and techniques. There are different types of digital forensics, all with their own collection and analysis methodologies. Some of the most common types are listed below.



- **Computer forensics:** The most common type of digital forensics is computer forensics, which concerns investigating computers, the devices most commonly used in crimes.
- **Mobile forensics:** Mobile forensics involves investigating mobile devices and extracting evidence such as call records, text messages, GPS locations, and more.
- **Network forensics:** This area of forensics covers investigation beyond individual devices. It includes the whole network. The majority of the evidence found in networks is the network traffic logs.
- **Database forensics:** Many critical data is stored in dedicated databases. Database forensics investigates any intrusion into these databases that results in data modification or exfiltration.

- **Cloud forensics:** Cloud forensics is the type of forensics that involves investigating data stored on cloud infrastructure. This type of forensics sometimes gets tricky for the investigators as there is little evidence on cloud infrastructures.
- **Email forensics:** Email, the most common communication method between professionals, has become an important part of digital forensics. Emails are investigated to determine whether they are part of phishing or fraudulent campaigns.

Answer the questions below

> *Which phase of digital forensics is concerned with correlating the collected data to draw any conclusions from it?*

Answer: Analysis

> *Which phase of digital forensics is concerned with extracting the data of interest from the collected evidence?*

Answer: Examination

Evidence Acquisition

Acquiring evidence is a critical job. The forensics team must collect all the evidence securely without tampering with the original data. Evidence acquisition methods for digital devices depend on the type of digital device. However, some general practices must be followed while the evidence is acquired. Let's discuss some of the important ones.

Proper Authorization

The forensics team should obtain authorization from the relevant authorities before collecting any data. Evidence collected without prior approval may be deemed inadmissible in court. Forensic evidence contains private and sensitive data of an organization or individual. Proper authorization before collecting this data is essential for investigating according to the limits of the law.

Chain of Custody

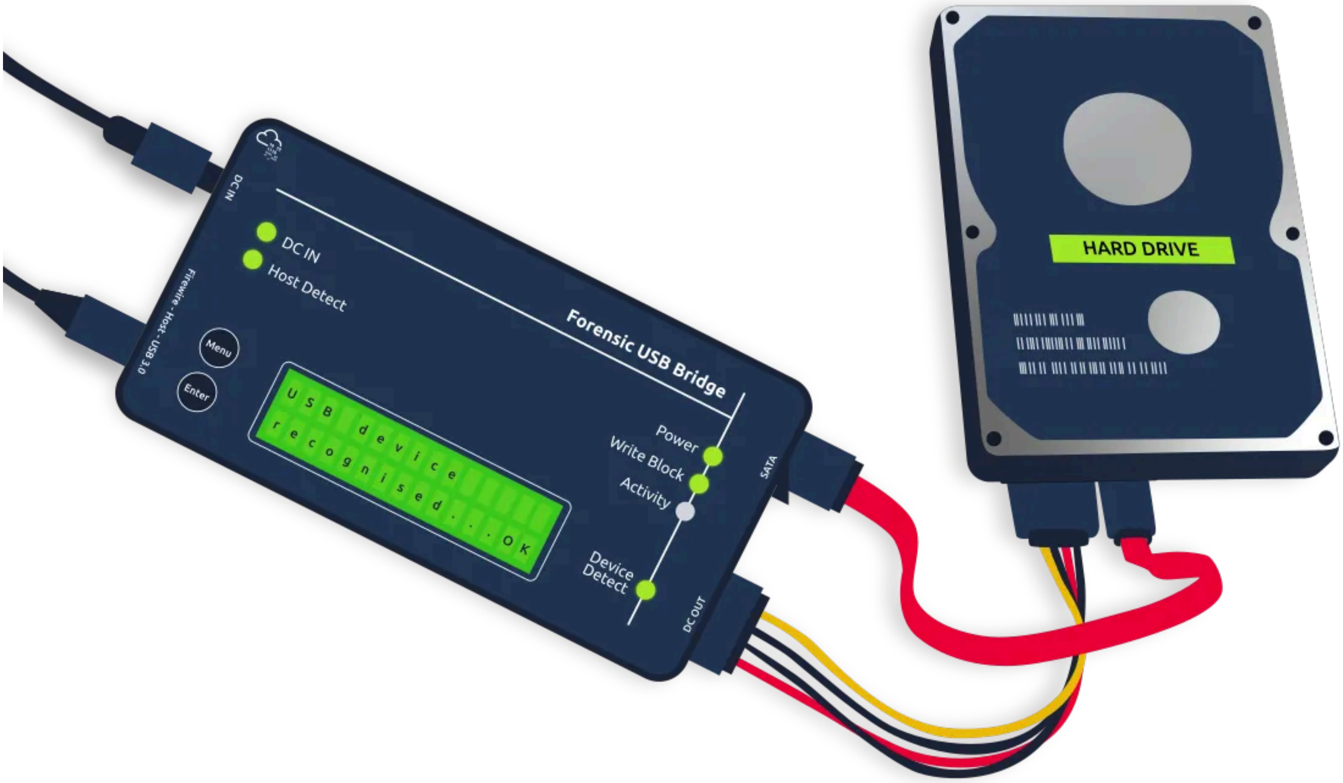
Imagine that a team of investigators collects all the evidence from the crime scene, and some of the evidence goes missing after a few days, or there is any change in the evidence. No individual can be held accountable in this scenario because there is no proper process for documenting the evidence owners. This problem can be solved by maintaining a chain of custody document. A chain of custody is a formal document containing all the details of the evidence. Some of the key details are listed below:

- Description of the evidence (name, type).
- Name of individuals who collected the evidence.
- Date and time of evidence collection.
- Storage location of each piece of evidence.
- Access times and the individual record who accessed the evidence.

This creates a proper trail of evidence and helps preserve it. The chain of custody document can be used to prove the integrity and reliability of the evidence admitted in court. A sample chain of custody can be downloaded from **here**.

Use of Write Blockers

Write blockers are an essential part of the digital forensics team's toolbox. Suppose you are collecting evidence from a suspect's hard drive and attaching the hard drive to the forensic workstation. While the collection occurs, some background tasks in the forensic workstation may alter the timestamps of the files on the hard drive. This can cause hindrances during the analysis, ultimately producing incorrect results. Suppose the data was collected from the hard drive using a write blocker instead in the same scenario. This time, the suspect's hard drive would remain in its original state as the write blocker can block any evidence alteration actions.



Answer the questions below

> *Which tool is used to ensure data integrity during the collection?*

Answer: write blocker

> *What is the name of the document that has all the details of the collected digital evidence?*

Answer: chain of custody

Windows Forensics

The most common types of evidence collected from crime scenes are desktop computers and laptops, as most criminal activity involves a personal system. These devices have different operating systems running on them. In this task, we will discuss the evidence acquisition and analysis of the Windows operating system, which is a very common operating system that has been investigated in several cases.

As part of the data collection phase, forensic images of the Windows operating system are taken. These forensic images are bit-by-bit copies of the whole operating system. Two different categories of forensic images are taken from a Windows operating system.

- **Disk image:** The disk image contains all the data present on the storage device of the system (HDD, SSD, etc.). This data is non-volatile, meaning that the disk data would survive even after a restart of the operating system. For example, all the files like media, documents, internet browsing history, and more.
- **Memory image:** The memory image contains the data inside the operating system's RAM. This memory is volatile, meaning the data will get lost after the system is powered off or restarted. For example, to capture open files, running processes, current network connections, etc., the memory image should be prioritized and taken first from the suspect's operating system; otherwise, any restart or shutdown of the system would result in all the volatile data getting deleted. While carrying out digital forensics on a Windows operating system, disk and memory images are very important to collect.

Let's discuss some popular tools used for disk and memory image acquisition and analysis of the Windows operating system.

FTK Imager: FTK Imager is a widely used tool for taking disk images of Windows operating systems. It offers a user-friendly graphical interface for creating the image in various formats. This tool can also analyze the contents of a disk image. It can be used for both acquisition and analysis purposes.

Autopsy: Autopsy is a popular open-source digital forensics platform. An investigator can import an acquired disk image into this tool, and the tool will conduct an extensive analysis of the image. It offers various features during image analysis, including keyword search, deleted file recovery, file metadata, extension mismatch detection, and many more.

DumpIt: DumpIt offers the utility of taking a memory image from a Windows operating system. This tool creates memory images using a command-line interface and a few commands. The memory image can also be taken in different formats.

Volatility: Volatility is a powerful open-source tool for analyzing memory images. It offers some extremely useful plugins. Each artifact can be analyzed using a specific plugin. This tool supports various operating systems, including Windows, Linux, macOS, and Android.

Note: Various other tools are also used to acquire and analyze disk and memory images of the Windows operating system.

Answer the questions below

> *Which type of forensic image is taken to collect the volatile data from the operating system?*

Answer: Memory Image

Practical Example of Digital Forensics

Everything we do on our digital devices, from smartphones to computers, leaves traces. Let’s see how we can use this in the subsequent investigation.

Our cat, Gado, has been kidnapped. The kidnapper has sent us a document with their requests in MS Word Document format. We have converted the document to PDF format and extracted the image from the MS Word file for your convenience.

You can download the attached file below to your local machine for inspection.

However, for your convenience we have added the files to the AttackBox. To follow along, press the **Start AttackBox** button on top of the page. The AttackBox will open in split view. In case it is not showing up, you can press the **Show Split View** button on top of the page. Once started, open a new terminal and navigate to the `/root/Rooms/introdigitalforensics` directory as shown below. In the following terminal output, we changed to the directory containing the case files.

```
root@tryhackme:~# cd /root/Rooms/introdigitalforensics
```

When you create a text file, `TXT` , some metadata gets saved by the operating system, such as file creation date and last modification date. However, much information gets kept within the file's metadata when you use a more advanced editor, such as MS Word. There are various ways to read the file metadata; you might open them within their official viewer/editor or use a suitable forensic tool. Note that exporting the file to other formats, such as `PDF` , would maintain most of the metadata of the original document, depending on the PDF writer used.

Let's see what we can learn from the PDF file. We can try to read the metadata using the program `pdfinfo` . Pdfinfo displays various metadata related to a PDF file, such as title, subject, author, creator, and creation date. (The AttackBox already has `pdfinfo` installed; however, if you are using Kali Linux and don't have `pdfinfo` installed, you can install it using `sudo apt install poppler-utils` .) Consider the following example of using `pdfinfo DOCUMENT.pdf:`

```
root@tryhackme:~# pdfinfo DOCUMENT.pdf
Creator:        Microsoft® Word for Office 365
Producer:       Microsoft® Word for Office 365
CreationDate:   Wed Oct 10 21:47:53 2018 EEST
ModDate:        Wed Oct 10 21:47:53 2018 EEST
Tagged:         yes
```

```
    UserProperties: no
    Suspects:       no
    Form:           none
    JavaScript:     no
    Pages:          20
    Encrypted:      no
    Page size:      595.32 x 841.92 pts (A4)
    Page rot:       0
    File size:      560362 bytes
    Optimized:      no
    PDF version:    1.7
```

The PDF metadata clearly shows that it was created using MS Word for Office 365 on October 10, 2018.

Photo EXIF Data

EXIF stands for Exchangeable Image File Format; it is a standard for saving metadata to image files. Whenever you take a photo with your smartphone or with your digital camera, plenty of information gets embedded in the image. The following are examples of metadata that can be found in the original digital images:

- Camera model / Smartphone model
- Date and time of image capture
- Photo settings such as focal length, aperture, shutter speed, and ISO settings

Because smartphones are equipped with a GPS sensor, finding GPS coordinates embedded in the image is highly probable. The GPS coordinates, i.e., latitude and longitude, would generally show the place where the photo was taken.

There are many online and offline tools to read the EXIF data from images. One command-line tool is `exiftool` . ExifTool is used to read and write metadata in various file types, such as JPEG images. The AttackBox already has `exiftool` installed; however, if you are using Kali Linux and don't have `exiftool` installed, you can install it using `sudo apt install libimage-exiftool-perl` . In the following terminal window, we executed `exiftool IMAGE.jpg` to read all the EXIF data embedded in this image.

```
root@tryhackme:~# exiftool IMAGE.jpg
[...]
```

```
GPS Position : 51 deg 31' 4.00" N, 0 deg 5' 48.30" W
[...]
```

If you take the above coordinates and search one of the online maps, you will learn more about this location. Searching Microsoft Bing Maps or Google Maps for `51 deg 30' 51.90" N, 0 deg 5' 38.73" W` reveals the street where the photo was taken. Note that for the search to work, we had to replace `deg` with `°` and remove the extra white space. In other words, we typed `51°30'51.9"N 0°05'38.7"W` in the map search bar.

Answer the questions below

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

Answer: Ann Gree Shepherd

```
pdfinfo ransom-letter.pdf
```

> *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?*

Answer: Milk Street

```
exiftool letter-image.jpg | grep GPS
```

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

Answer: Canon EOS R6

```
exiftool letter-image.jpg | grep Camera
```

Thank You!

Tryhackme Tryhackme Walkthrough Cyber Security 101 Digital Forensics

Follow

Written by Z3pH7

234 Followers · 7 Following

Cybersecurity | Pentester | Student

Responses (1)

What are your thoughts?

Respond

Samar
2 months ago

thank you

Reply

More from Z3pH7

Z3pH7

How to Install and Uninstall OpenVAS completely — Kali linux

OpenVAS, an application used to scan endpoints and web applications to identify and detect vulnerabilities. It is commonly used by...

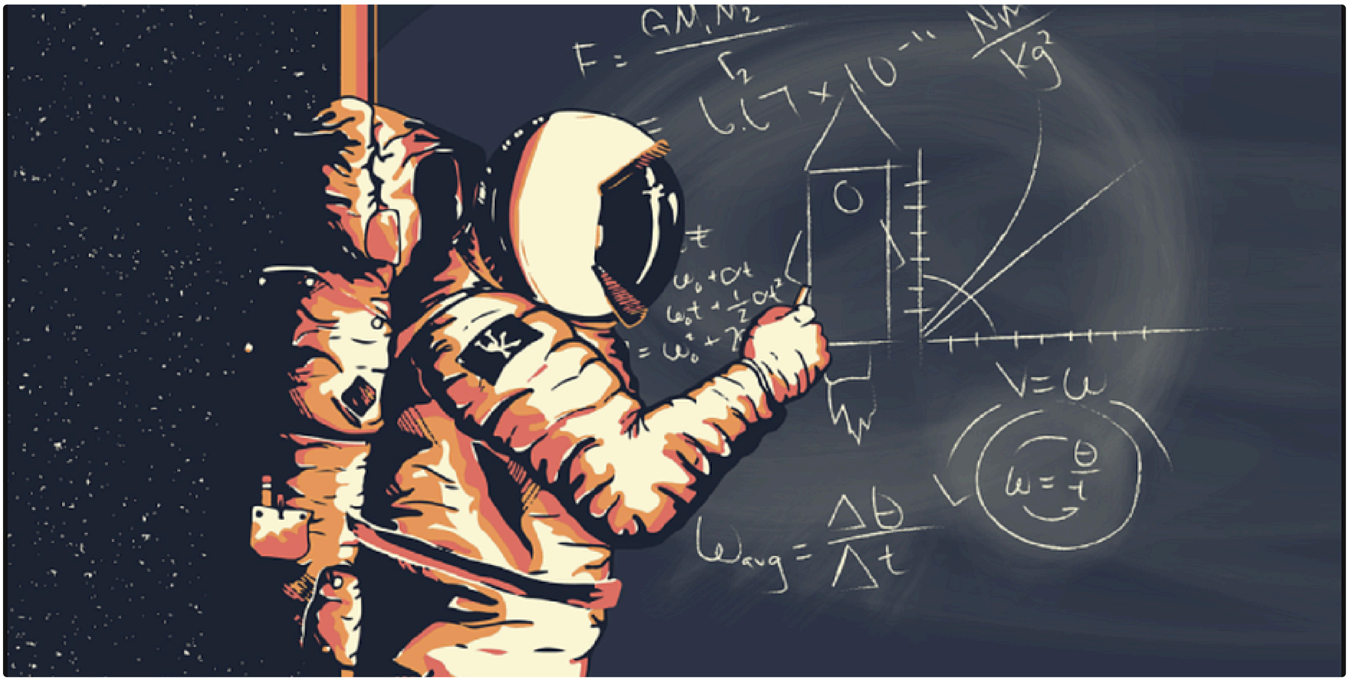
Sep 19, 2024 3

Z3pH7

TryHackMe — Basic Pentesting | Write-up (THM)

Hello, everyone! This CTF is an entry-level path toward becoming a penetration tester, taking your first step. This challenge is very easy...

Aug 26, 2024

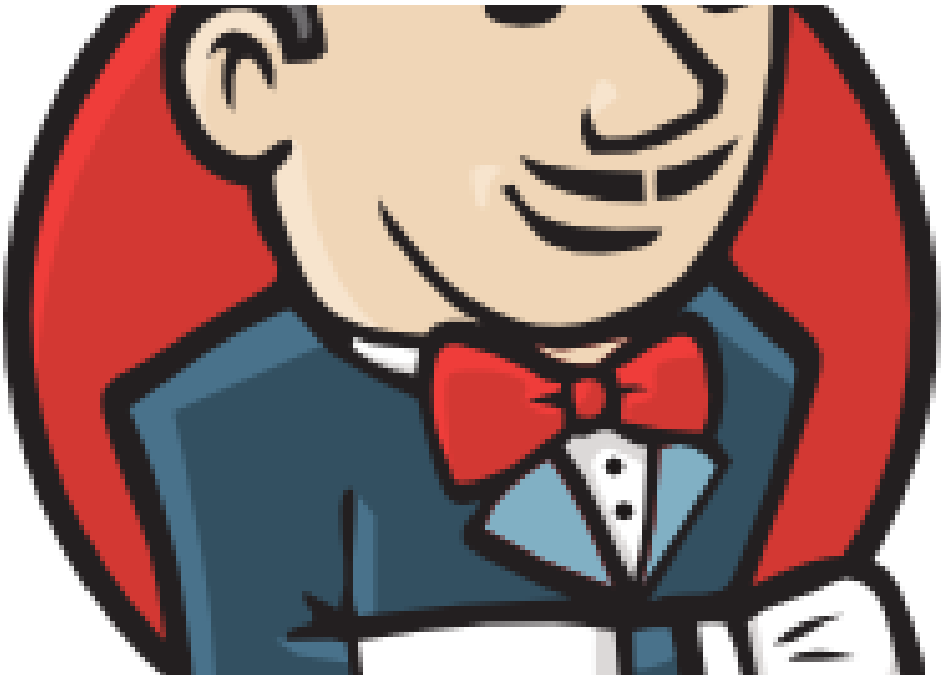


Z3pH7

TryHackMe — Vulnversity | Write-up (THM)

Hi everyone! Today, we're going to practice enumeration, reconnaissance, exploitation, and privilege escalation. TryHackMe will guide us...

Sep 1, 2024



Z3pH7

TryHackMe — Alfred | Walkthrough (THM)

This is a Windows application, we'll be using Nishang to gain initial access. The repository contains a useful set of scripts for initial...

Sep 9, 2024 1

See all from Z3pH7

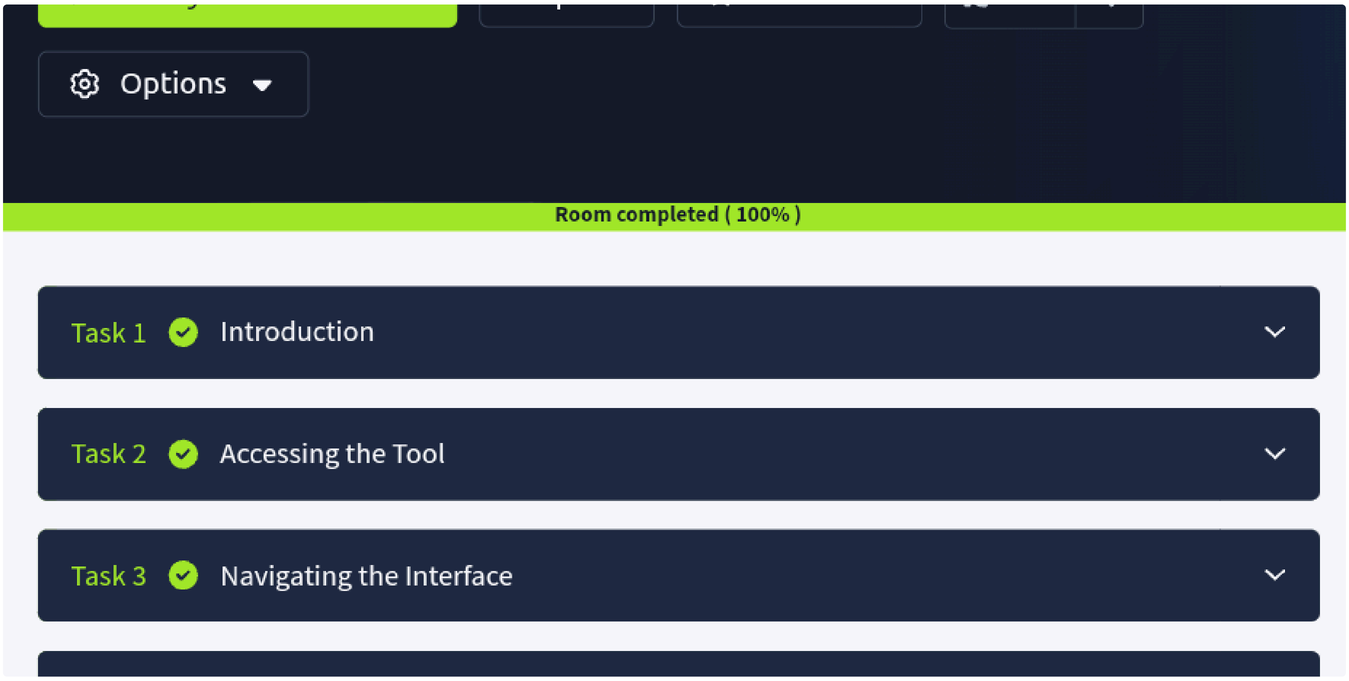
Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



Options

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Accessing the Tool

Task 3 ✓ Navigating the Interface

Jawstar

CyberChef: The Basics Tryhackme Write up

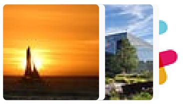
Tryhackme

Nov 7, 2024 8

Lists

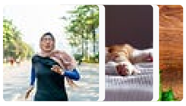
Staff picks

791 stories · 1544 saves



Stories to Help You Level-Up at Work

19 stories · 908 saves



Self-Improvement 101

20 stories · 3177 saves

Productivity 101

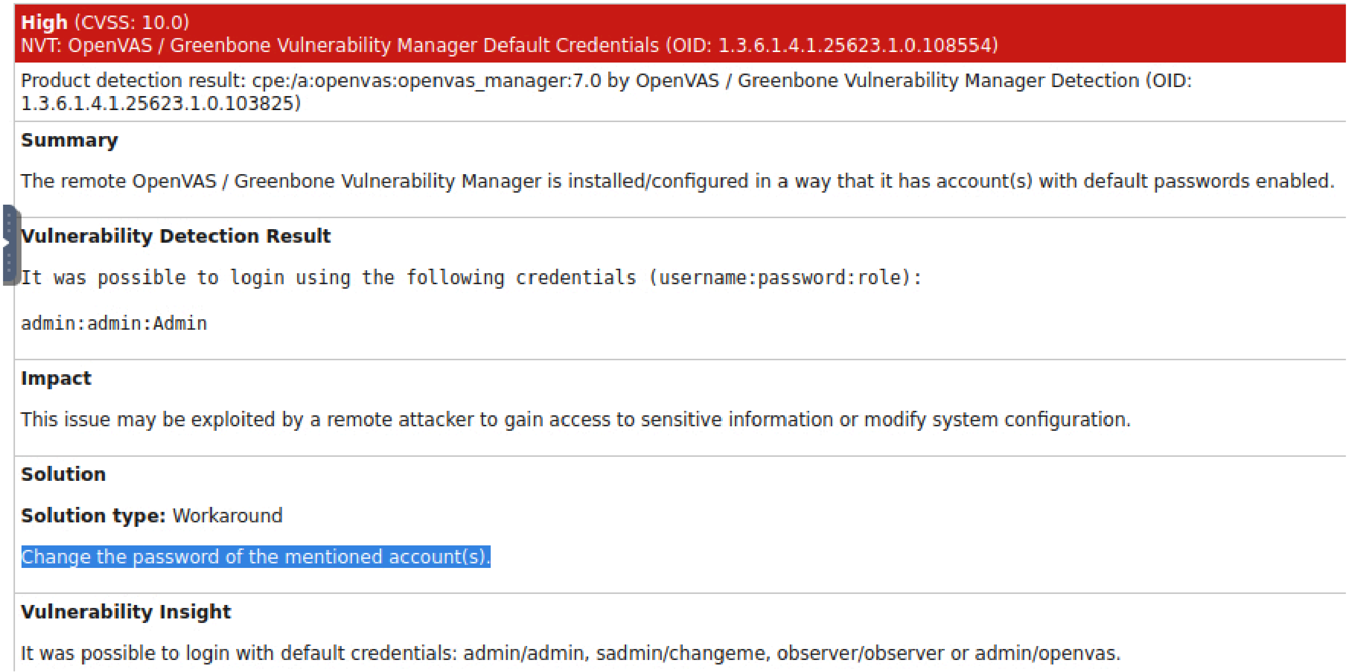
20 stories · 2693 saves

rutbar

TryHackMe — CAPA: The Basics | Cyber Security 101 (THM)

Tool Overview: How CAPA Works

Oct 23, 2024 13



High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)

Product detection result: cpe:/a:openvas:openvas_manager:7.0 by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)

Summary

The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result

```
It was possible to login using the following credentials (username:password:role):

admin:admin:Admin
```

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution

Solution type: Workaround

Change the password of the mentioned account(s).

Vulnerability Insight

It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

embossdotar

TryHackMe — Vulnerability Scanner Overview — Writeup

Key points: Vulnerability scanners | Vulnerability scanning | CVE | CVSS | OpenVAS. Vulnerability Scanner Overview by awesome TryHackMe! 🎉

Oct 22, 2024 65 1

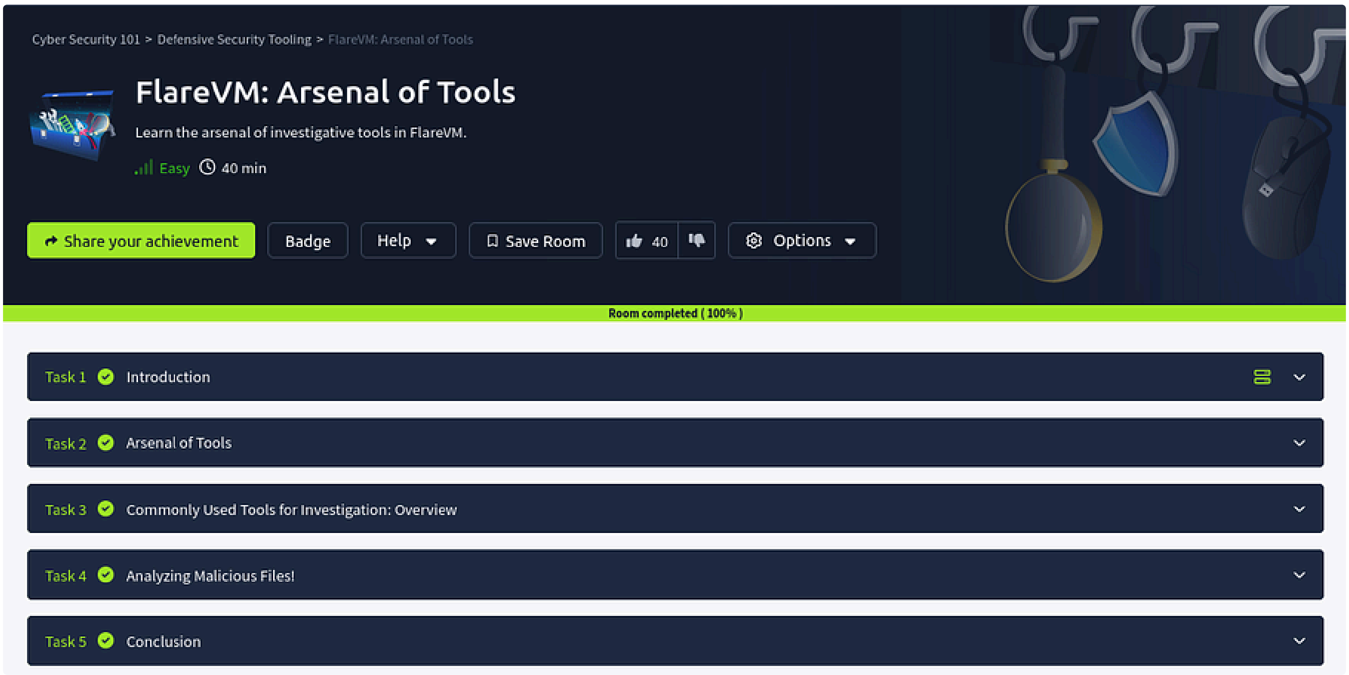
Advent of Cyber 2024
Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!
I'm all atomic inside!
Day 4
Answers
cyberw1ng.medium.com

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

Dec 4, 2024 882 1



Cyber Security 101 > Defensive Security Tooling > FlareVM: Arsenal of Tools

FlareVM: Arsenal of Tools

Learn the arsenal of investigative tools in FlareVM.

Easy 40 min

Room completed (100%)

Task 1 Introduction

Task 2 Arsenal of Tools

Task 3 Commonly Used Tools for Investigation: Overview

Task 4 Analyzing Malicious Files!

Task 5 Conclusion

Jawstar

FlareVM: Arsenal of Tools

CYBER SECURITY 101 Tryhackme Write up

✦ Oct 29, 2024 37 1

See more recommendations

Open in app ↗

Medium Search