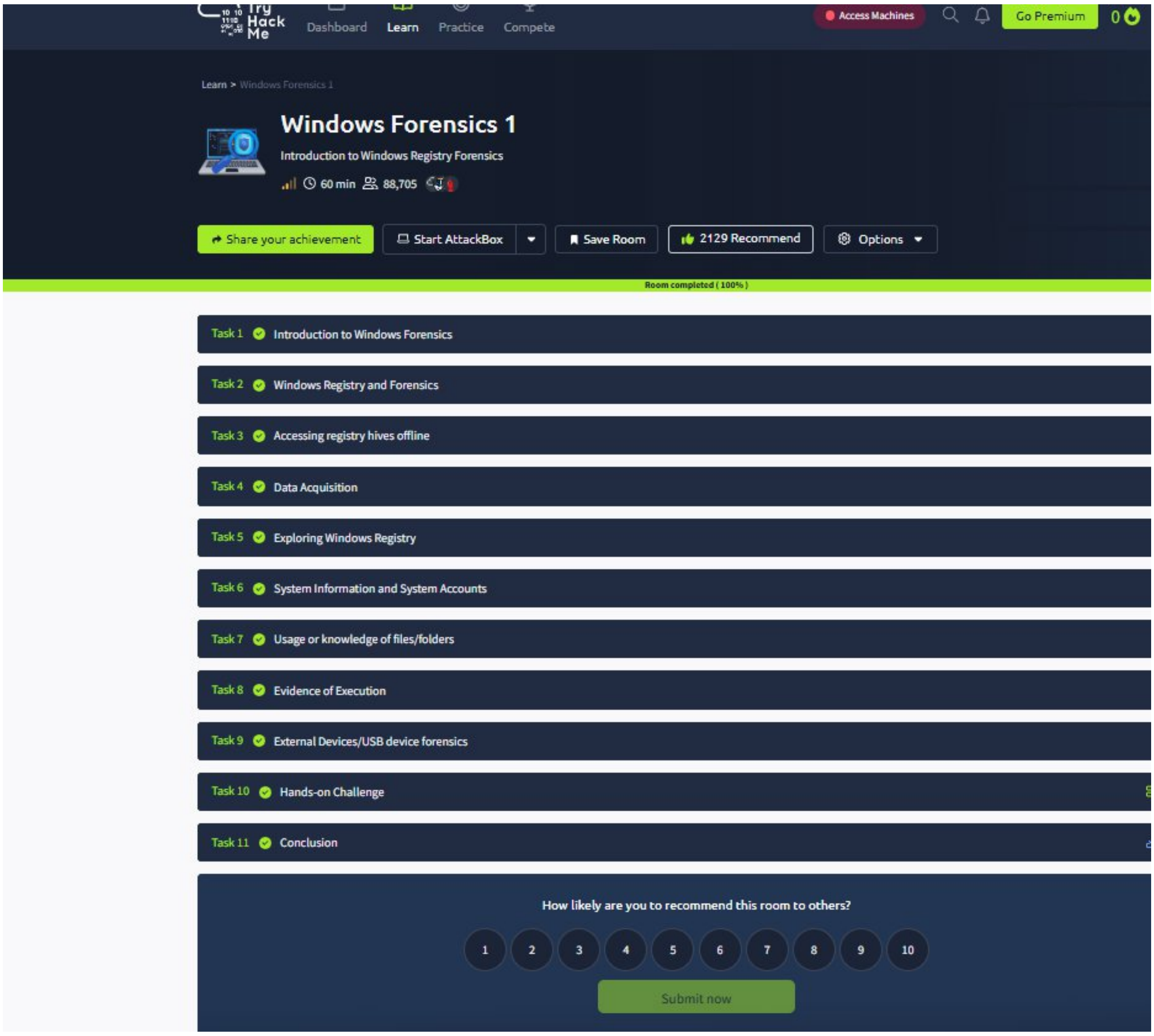
EXP:1 WINDOWS FORENSICS

AIM: To learn about the introduction to windows registry forensics.



Learn > Windows Forensics 1

Windows Forensics 1

Introduction to Windows Registry Forensics

60 min 88,705

Room completed (100%)

Task 1 Introduction to Windows Forensics

Task 2 Windows Registry and Forensics

Task 3 Accessing registry hives offline

Task 4 Data Acquisition

Task 5 Exploring Windows Registry

Task 6 System Information and System Accounts

Task 7 Usage or knowledge of files/folders

Task 8 Evidence of Execution

Task 9 External Devices/USB device forensics

Task 10 Hands-on Challenge

Task 11 Conclusion

How likely are you to recommend this room to others?

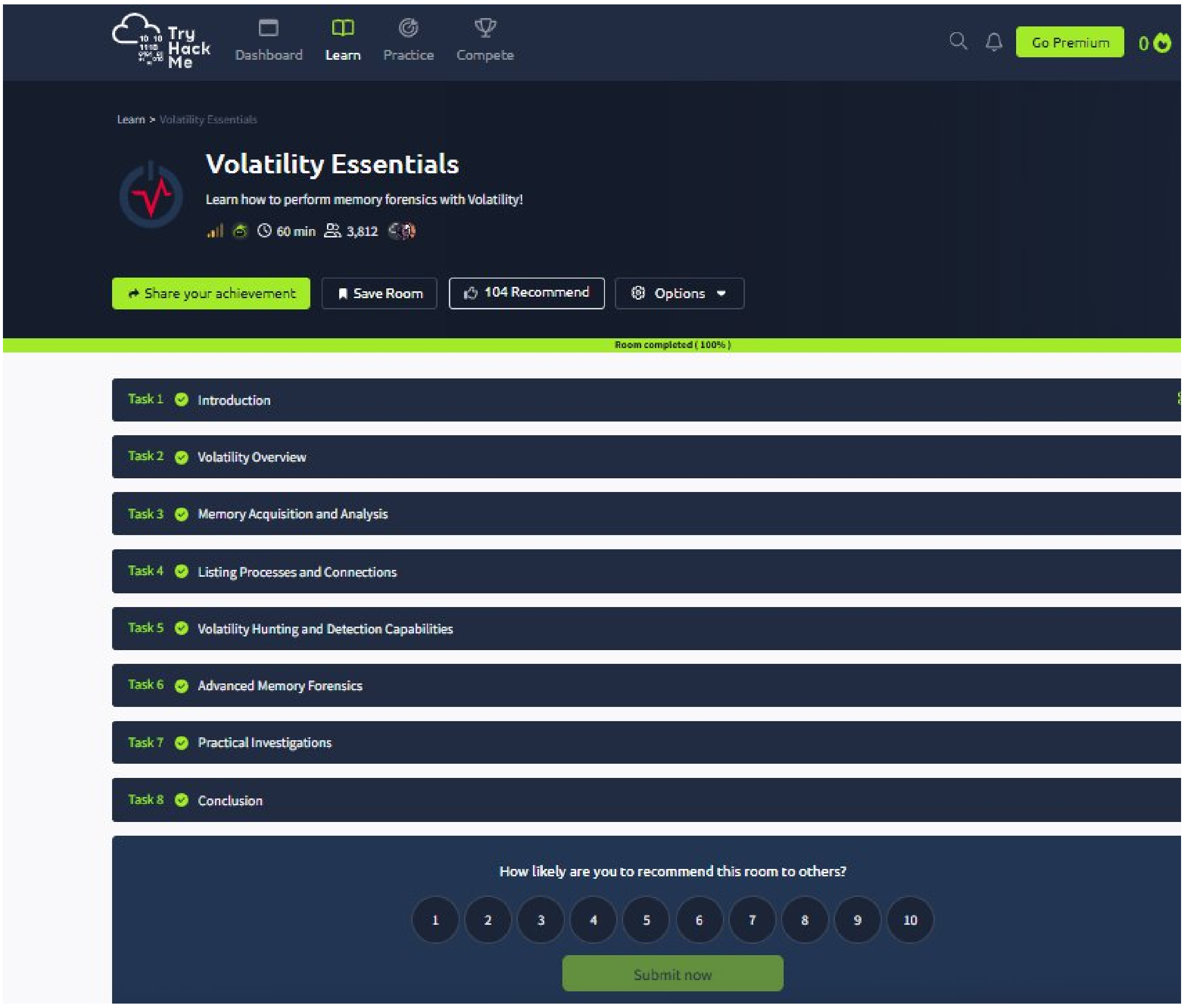
1 2 3 4 5 6 7 8 9 10

RESULT:

Thus about windows registry forensics has been successfully completed.

EXP :2 VOLATILITY ESSENTIALS

AIM: To learn how to perform memory forensics with volatility



Volatility Essentials

Learn how to perform memory forensics with Volatility!

Task 1 Introduction

Task 2 Volatility Overview

Task 3 Memory Acquisition and Analysis

Task 4 Listing Processes and Connections

Task 5 Volatility Hunting and Detection Capabilities

Task 6 Advanced Memory Forensics

Task 7 Practical Investigations

Task 8 Conclusion

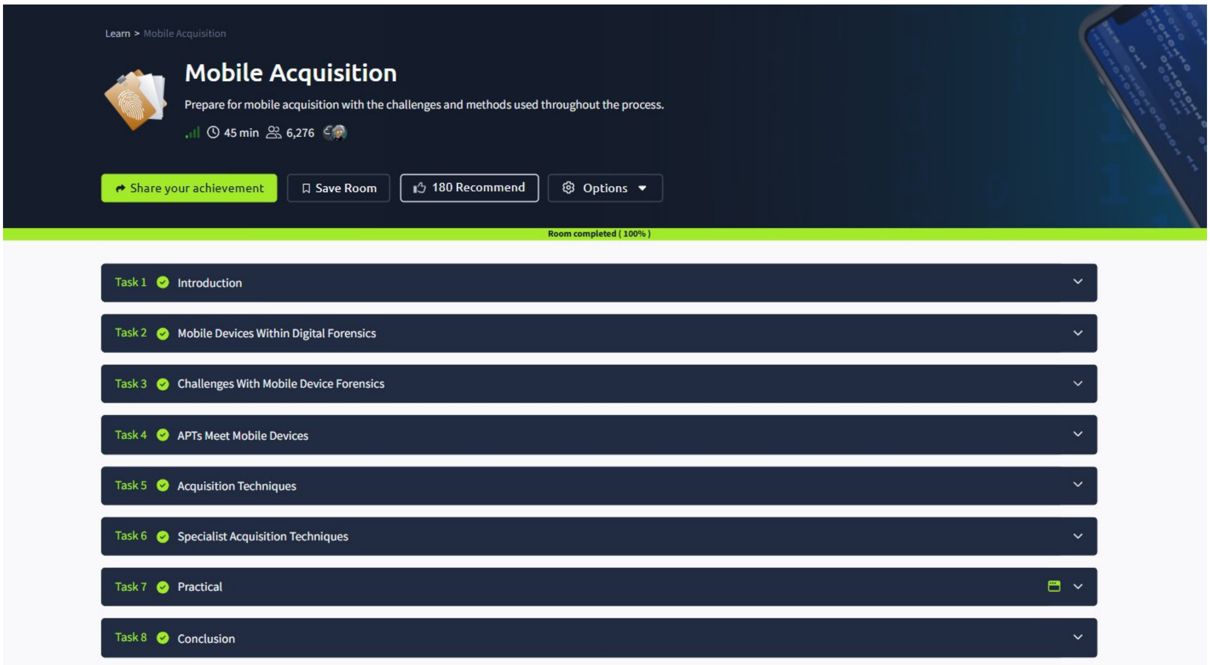
How likely are you to recommend this room to others?

RESULT:

Thus about memory forensics with volatility has been studied and executed.

EXP:3 MOBILE ACQUISITION

AIM: To prepare for mobile acquisition with the challenges and methods used throughout the process.



Mobile Acquisition

Prepare for mobile acquisition with the challenges and methods used throughout the process.

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Mobile Devices Within Digital Forensics

Task 3 ✓ Challenges With Mobile Device Forensics

Task 4 ✓ APTs Meet Mobile Devices

Task 5 ✓ Acquisition Techniques

Task 6 ✓ Specialist Acquisition Techniques

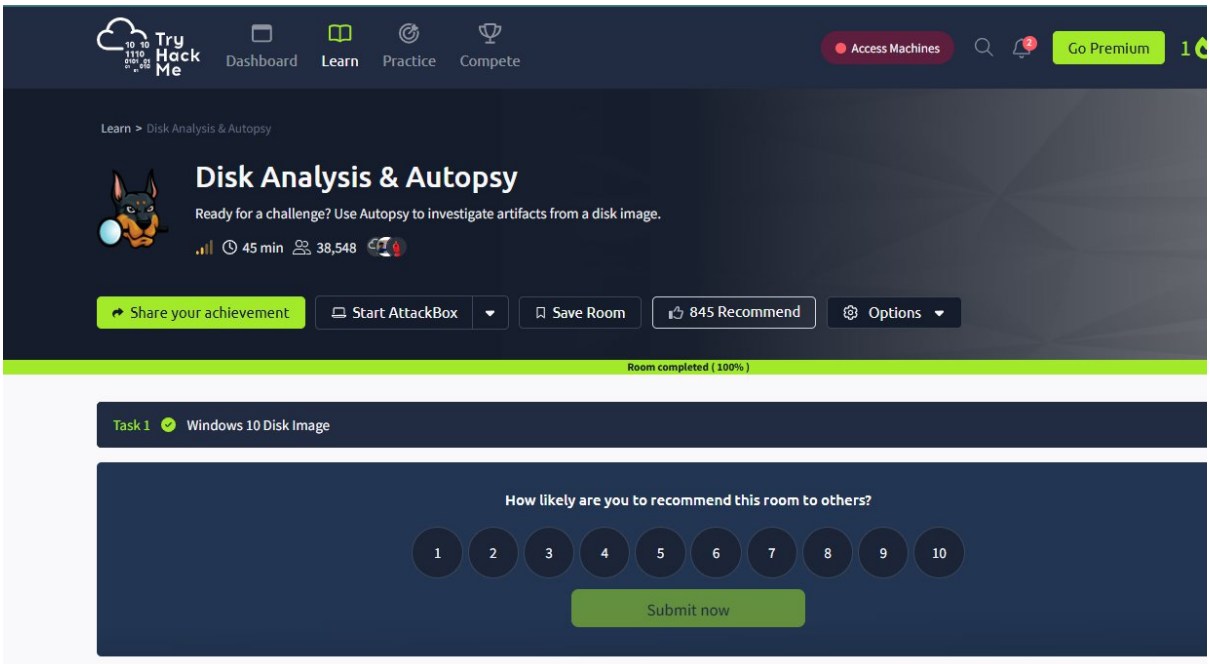
Task 7 ✓ Practical

Task 8 ✓ Conclusion

RESULT: Hence the mobile acquisition has been studied and successfully executed.

EXP:4 DISK ANALYSIS & AUTOPSY

AIM: To use autopsy to investigate artifacts from a disk image



Disk Analysis & Autopsy

Ready for a challenge? Use Autopsy to investigate artifacts from a disk image.

45 min 38,548

Task 1 Windows 10 Disk Image

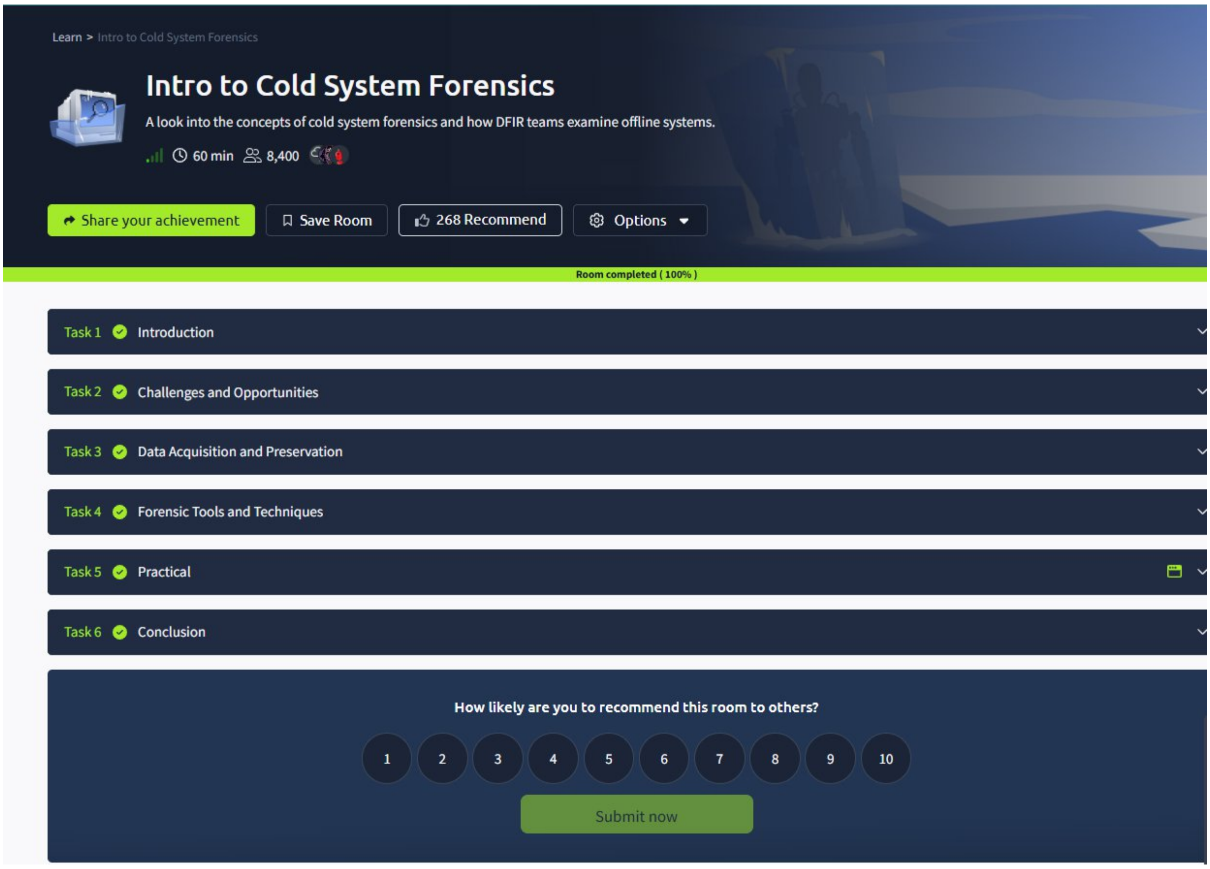
How likely are you to recommend this room to others?

RESULT:

Hence the disk analysis and forensics in tryhackme has been successfully studied.

EXP:5 INTRO TO COLD SYSTEM FORENSICS

AIM: To study about cold system forensics in tryhackme.



Learn > Intro to Cold System Forensics

Intro to Cold System Forensics

A look into the concepts of cold system forensics and how DFIR teams examine offline systems.

60 min 8,400

Task 1 ✓ Introduction

Task 2 ✓ Challenges and Opportunities

Task 3 ✓ Data Acquisition and Preservation

Task 4 ✓ Forensic Tools and Techniques

Task 5 ✓ Practical

Task 6 ✓ Conclusion

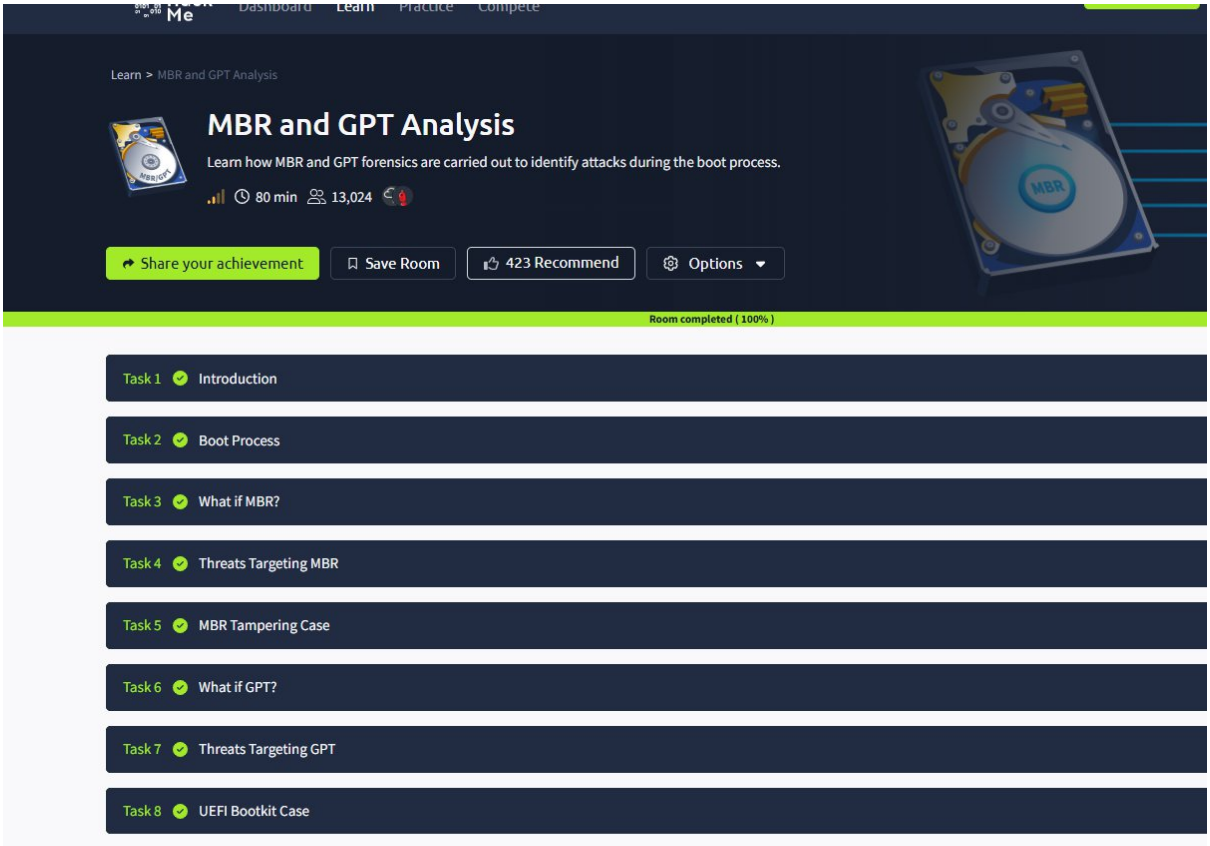
How likely are you to recommend this room to others?

RESULT:

Hence concept of cold system forensics were studied .

EXP:6 MBR AND GPT ANALYSIS

AIM: To learn how MBR and GPT forensics are carried out to identify attacks during the boot process.



Learn > MBR and GPT Analysis

MBR and GPT Analysis

Learn how MBR and GPT forensics are carried out to identify attacks during the boot process.

80 min 13,024

Room completed (100%)

Task 1 Introduction

Task 2 Boot Process

Task 3 What if MBR?

Task 4 Threats Targeting MBR

Task 5 MBR Tampering Case

Task 6 What if GPT?

Task 7 Threats Targeting GPT

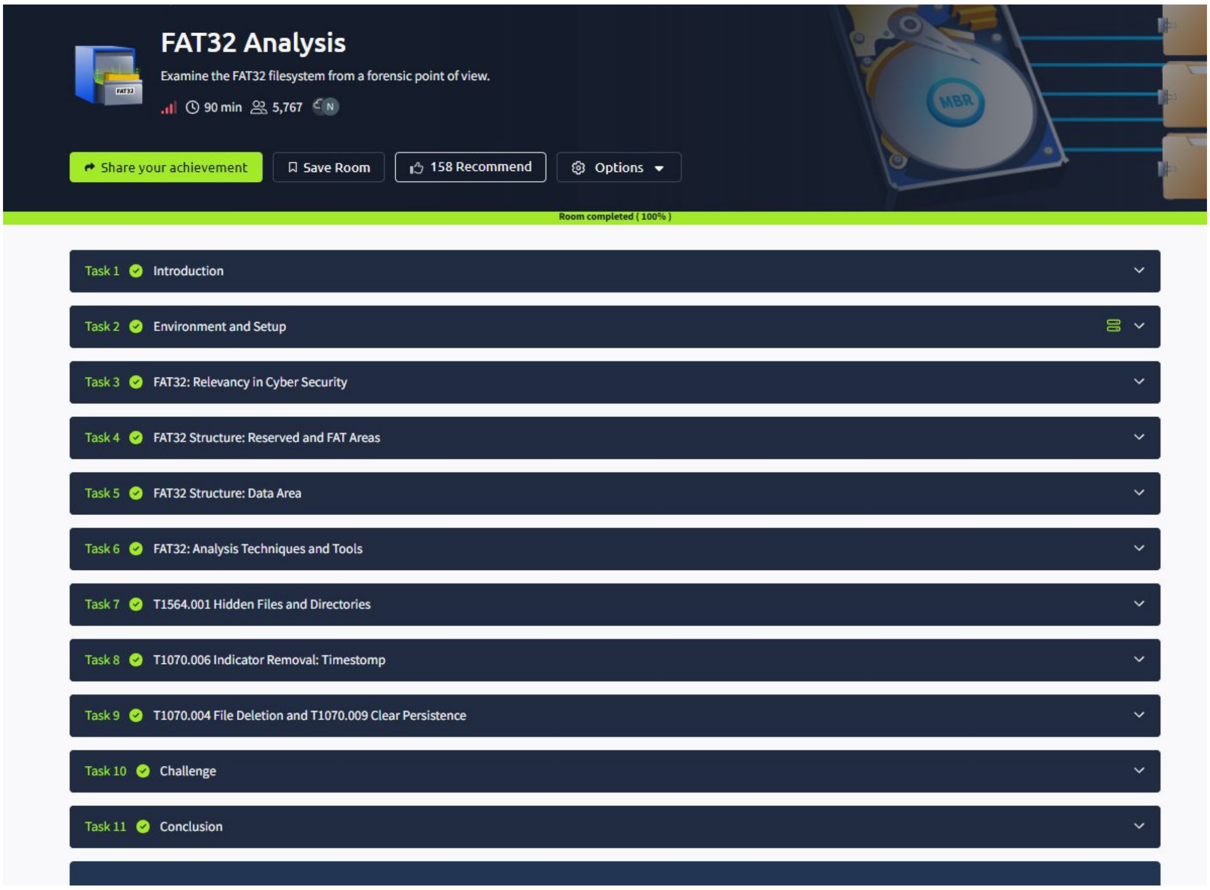
Task 8 UEFI Bootkit Case

RESULT:

Thus about MBR and GPT forensics have been successfully studied.

EXP :7 FAT32 ANALYSIS

AIM: To examine FAT32 filesystem from a forensic point of view.



FAT32 Analysis

Examine the FAT32 filesystem from a forensic point of view.

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Environment and Setup

Task 3 ✓ FAT32: Relevancy in Cyber Security

Task 4 ✓ FAT32 Structure: Reserved and FAT Areas

Task 5 ✓ FAT32 Structure: Data Area

Task 6 ✓ FAT32: Analysis Techniques and Tools

Task 7 ✓ T1564.001 Hidden Files and Directories

Task 8 ✓ T1070.006 Indicator Removal: Timestomp

Task 9 ✓ T1070.004 File Deletion and T1070.009 Clear Persistence

Task 10 ✓ Challenge

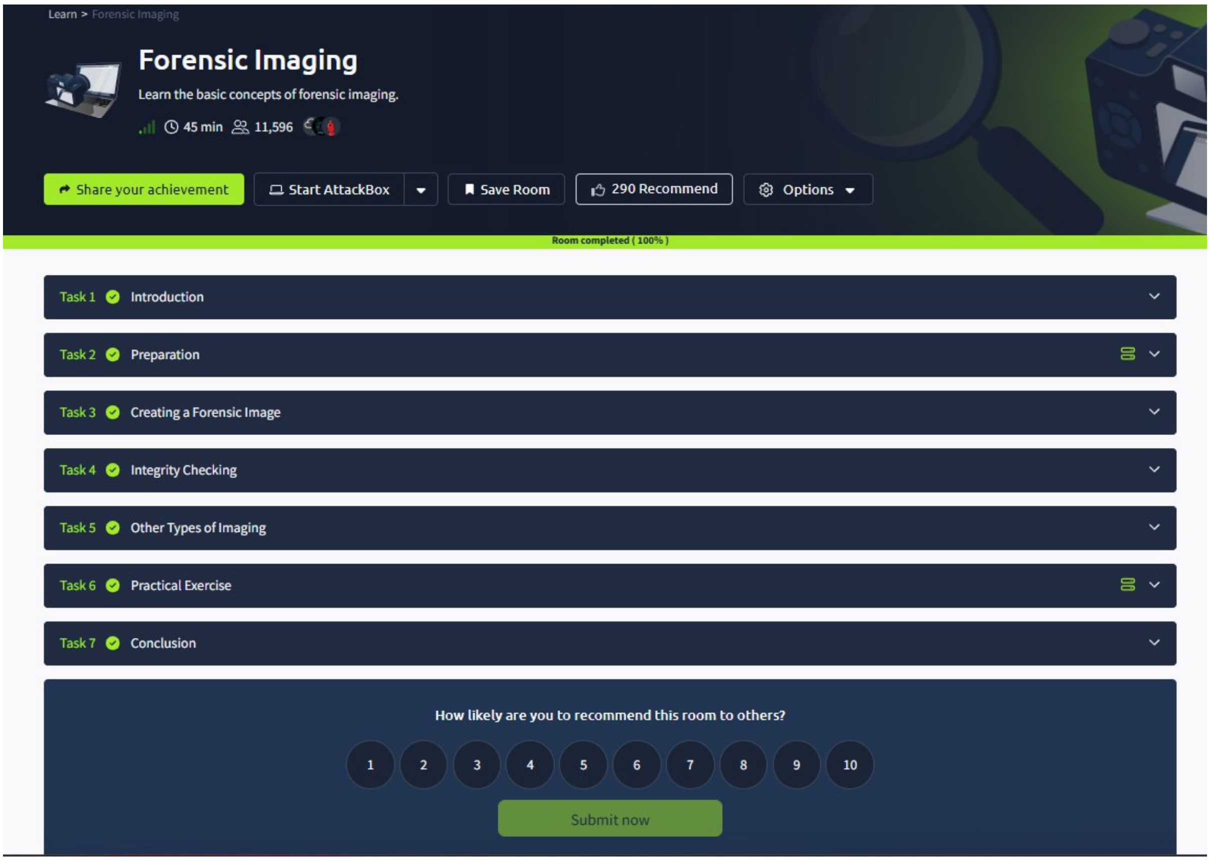
Task 11 ✓ Conclusion

RESULT:

Thus FAT32 Analysis in tryhackme has been successfully studied.

EXP: 8 FORENSIC IMAGING

AIM: To learn the basic concepts of forensic imaging



Learn > Forensic Imaging

Forensic Imaging

Learn the basic concepts of forensic imaging.

45 min 11,596

Room completed (100%)

Task 1 Introduction

Task 2 Preparation

Task 3 Creating a Forensic Image

Task 4 Integrity Checking

Task 5 Other Types of Imaging

Task 6 Practical Exercise

Task 7 Conclusion

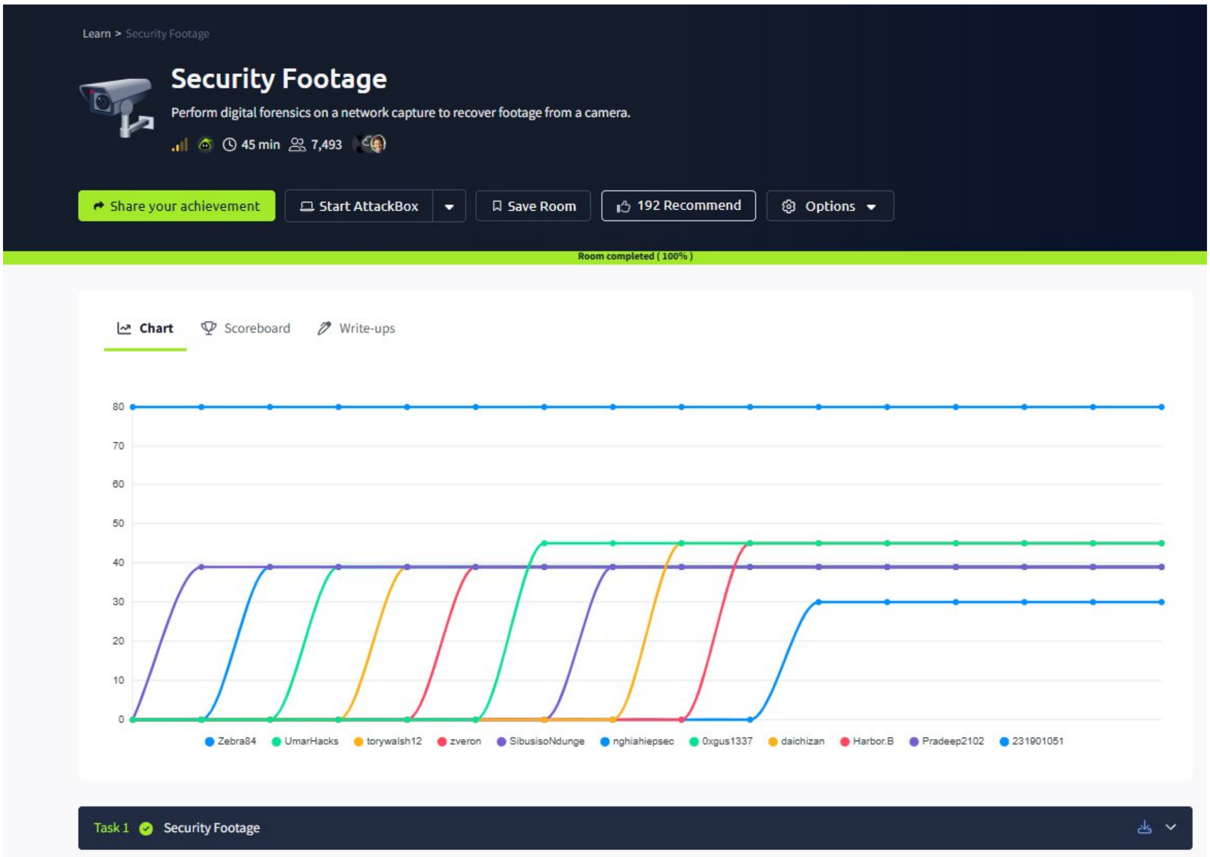
How likely are you to recommend this room to others?

RESULT:

Thus about forensic imaging in tryhackme has been successfully studied.

EXP:9 SECURITY FOOTAGE

AIM: To perform digital forensic on the network capture to recover footage .



Learn > Security Footage

Security Footage

Perform digital forensics on a network capture to recover footage from a camera.

45 min 7,493

Room completed (100%)

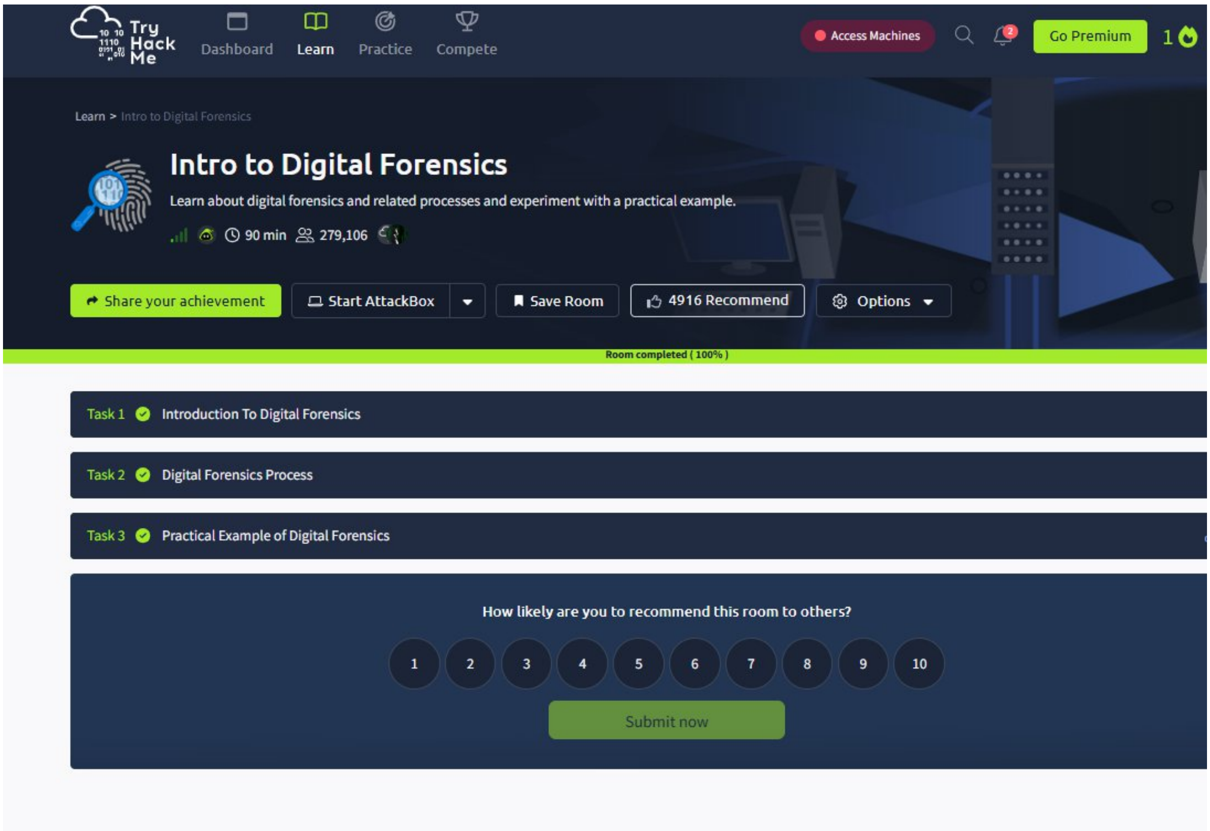
Task 1 Security Footage

RESULT:

Hence the security footage is studied and practised in tryhackme.

EXP:10 INTRO TO DIGITAL FORENSICS

AIM: To learn about digital forensics and its related processes.



Learn > Intro to Digital Forensics

Intro to Digital Forensics

Learn about digital forensics and related processes and experiment with a practical example.

90 min 279,106

Room completed (100%)

Task 1 Introduction To Digital Forensics

Task 2 Digital Forensics Process

Task 3 Practical Example of Digital Forensics

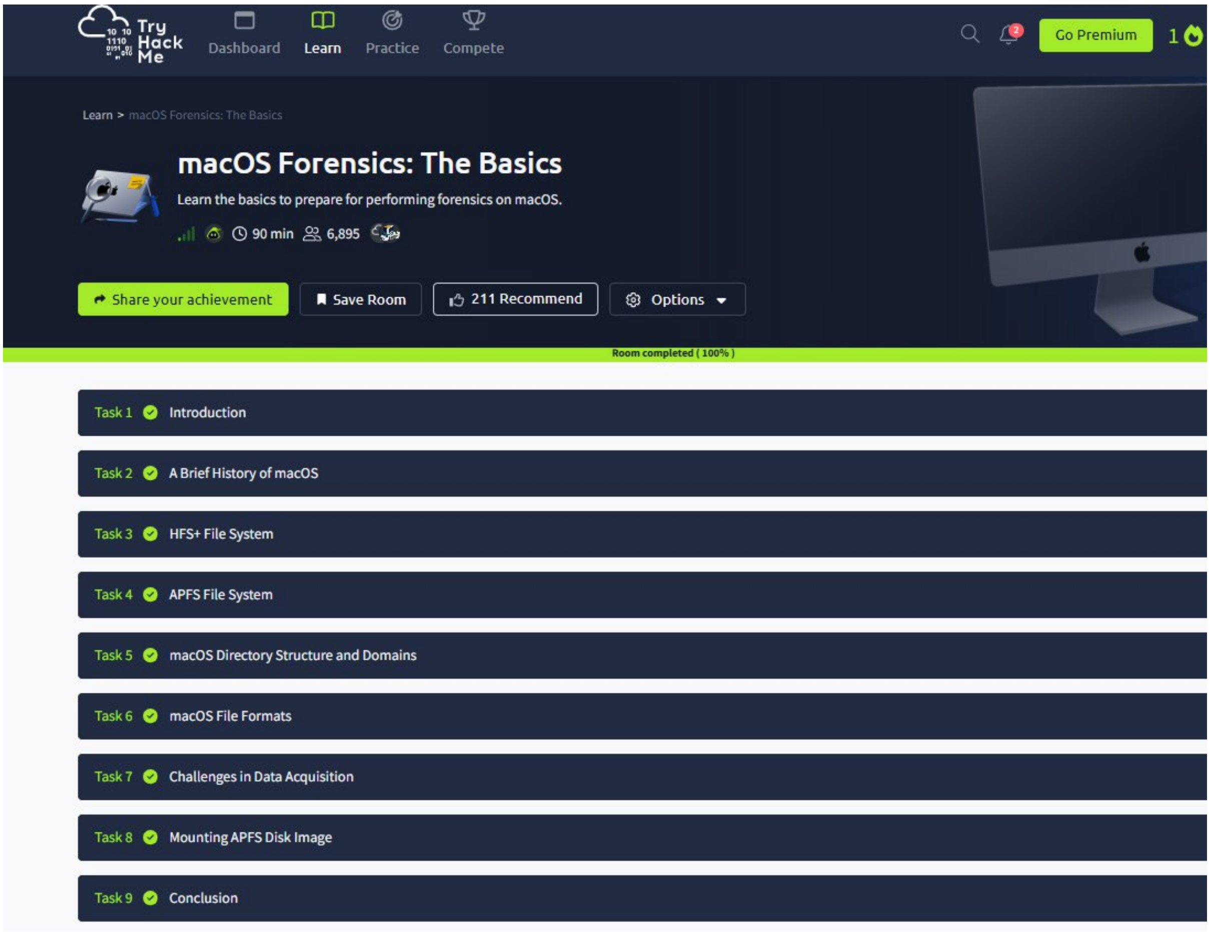
How likely are you to recommend this room to others?

RESULT:

The basic about digital forensics has been successfully completed.

EXP: 11 MACOS FORENSICS:THE BASICS

AIM: To learn the basics to prepare for performing forensics on macos.



macOS Forensics: The Basics

Learn the basics to prepare for performing forensics on macOS.

90 min 6,895

Task 1 ✓ Introduction

Task 2 ✓ A Brief History of macOS

Task 3 ✓ HFS+ File System

Task 4 ✓ APFS File System

Task 5 ✓ macOS Directory Structure and Domains

Task 6 ✓ macOS File Formats

Task 7 ✓ Challenges in Data Acquisition

Task 8 ✓ Mounting APFS Disk Image

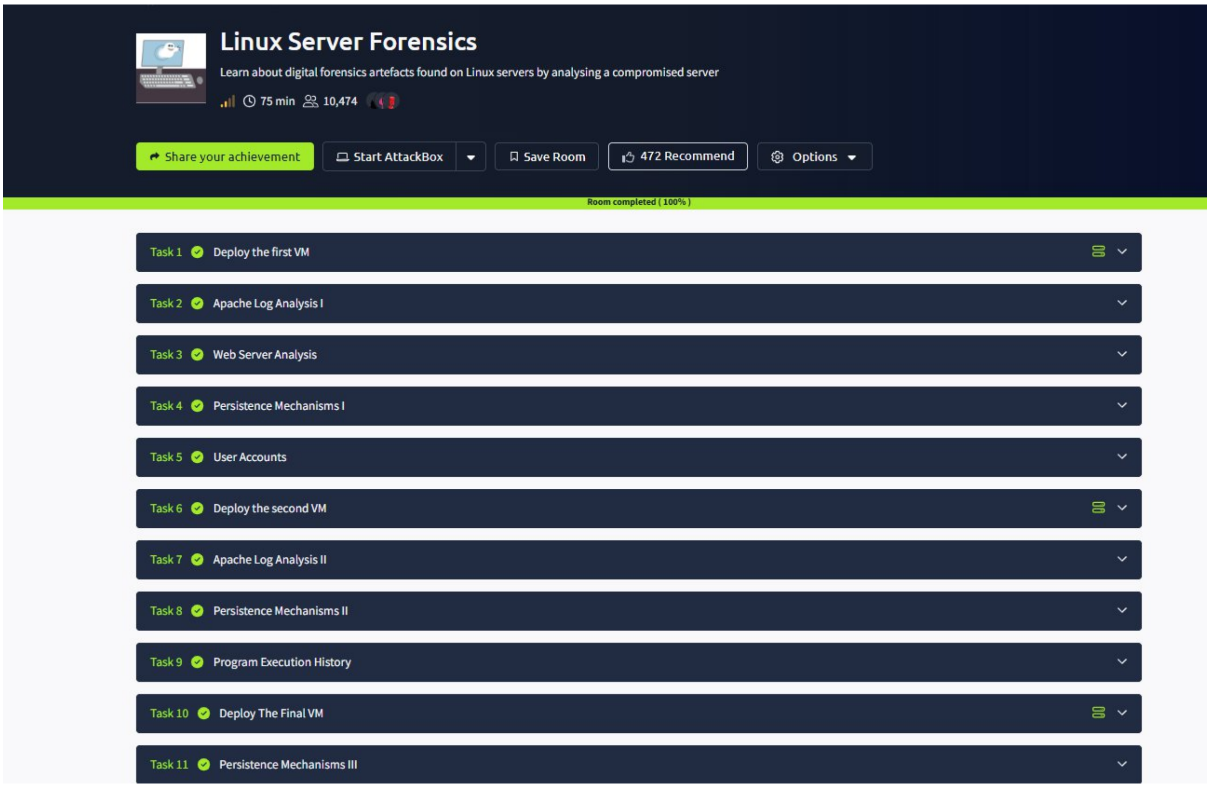
Task 9 ✓ Conclusion

RESULT:

Hence basics of macos forensic were successfully studied.

EXP: 12 LINUX SERVER FORENSICS

AIM: To learn about digital forensics artefacts found on linux servers by analysing a compromised server.



Linux Server Forensics

Learn about digital forensics artefacts found on Linux servers by analysing a compromised server

75 min 10,474

Share your achievement | Start AttackBox | Save Room | 472 Recommend | Options

Room completed (100%)

Task 1 ✓ Deploy the first VM

Task 2 ✓ Apache Log Analysis I

Task 3 ✓ Web Server Analysis

Task 4 ✓ Persistence Mechanisms I

Task 5 ✓ User Accounts

Task 6 ✓ Deploy the second VM

Task 7 ✓ Apache Log Analysis II

Task 8 ✓ Persistence Mechanisms II

Task 9 ✓ Program Execution History

Task 10 ✓ Deploy The Final VM

Task 11 ✓ Persistence Mechanisms III

RESULT:

Hence the linux server forensics is studied and successfully executed.