Exp No : 1 A WINDOWS FUNDAMENTALS 1

Date :

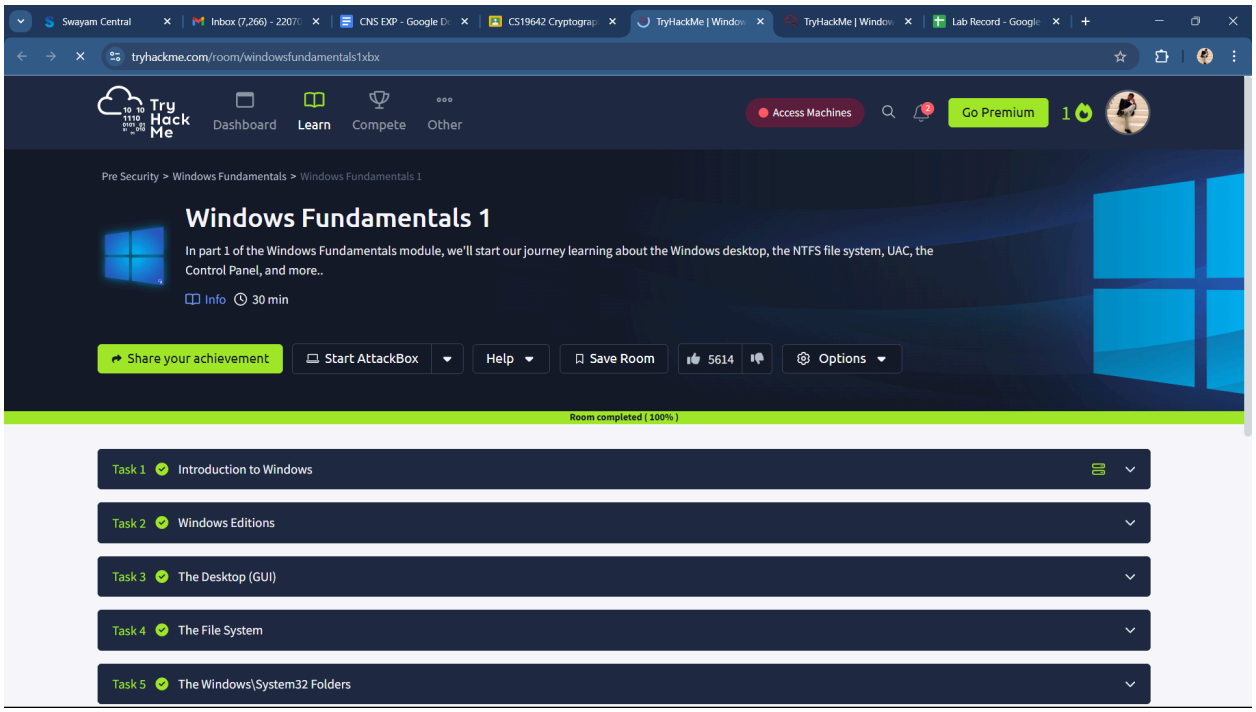
Aim:

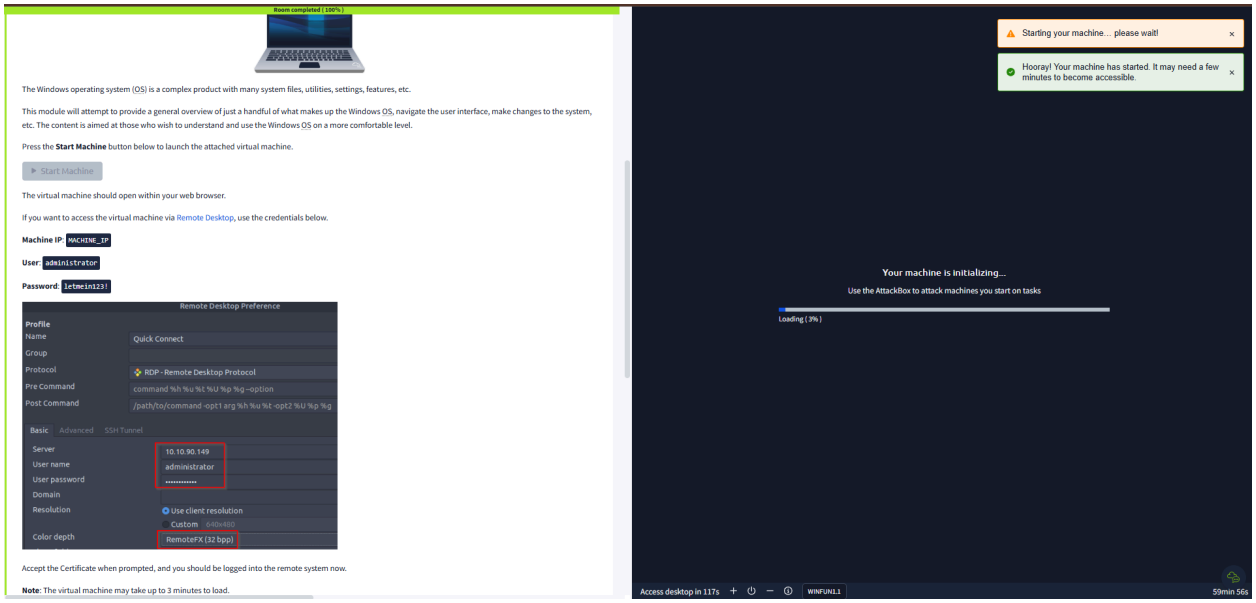
To understand and explore the fundamentals of the Windows operating system, including key components such as the file system, command prompt (CMD), task manager,and registry, to build a strong foundation for cybersecurity and system administration in TryHackMe platform.

Algorithm:

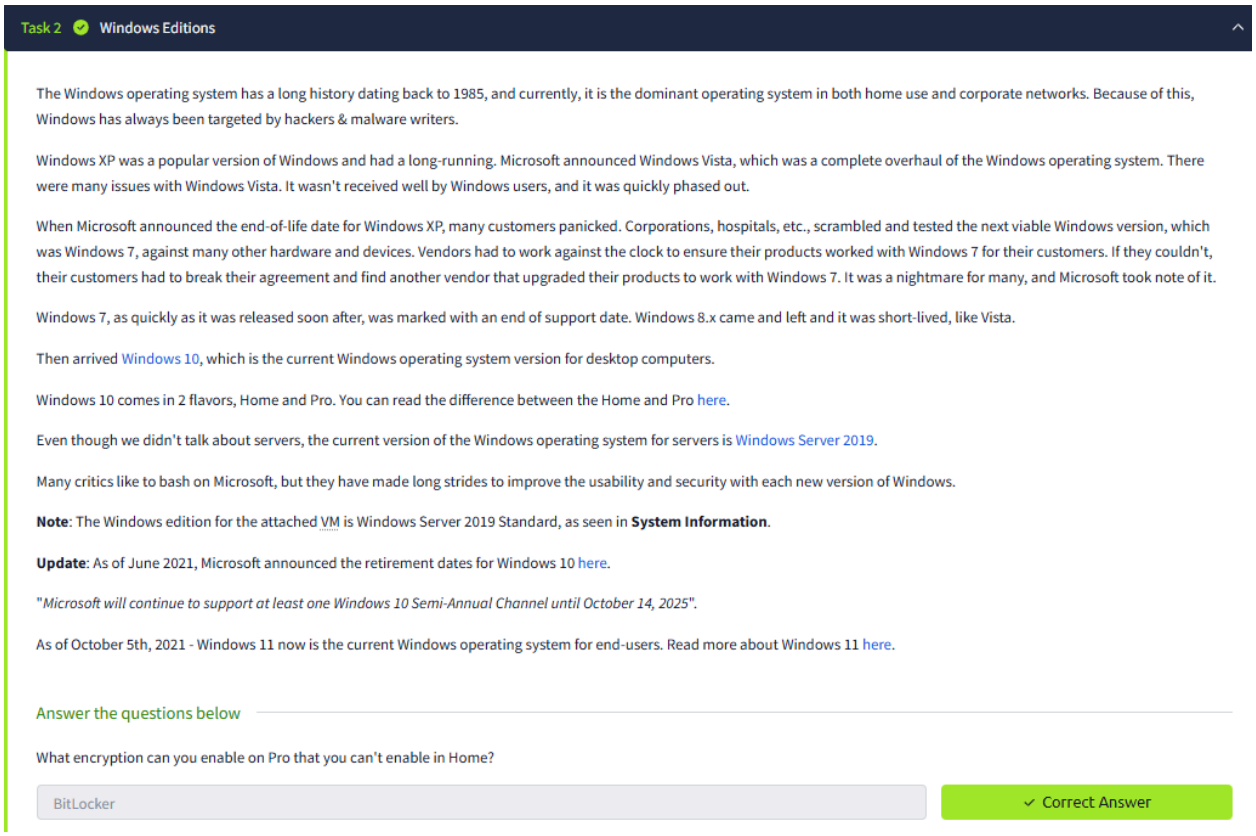
1. Access the lab in TryHackMe platform using the link below-
2. https://tryhackme.com/r/room/windowsfundamentals1xbx
3. Click Start a Machine and AttackBox to run the instance of Kali Windows
4. distribution.
5. Solve the task questions start with Windows OS edition and Desktop GUI.
6. Understand the 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:

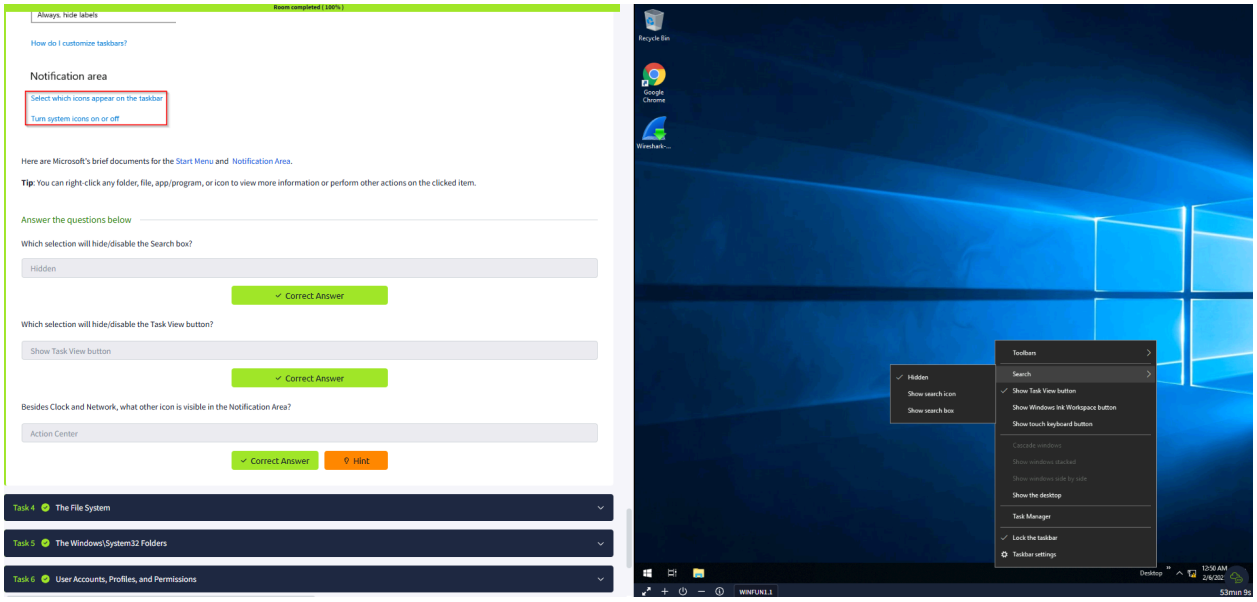




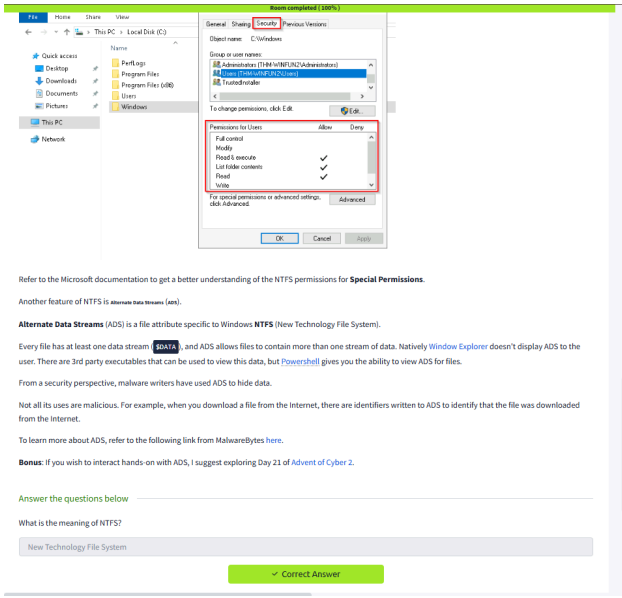
Task 2:

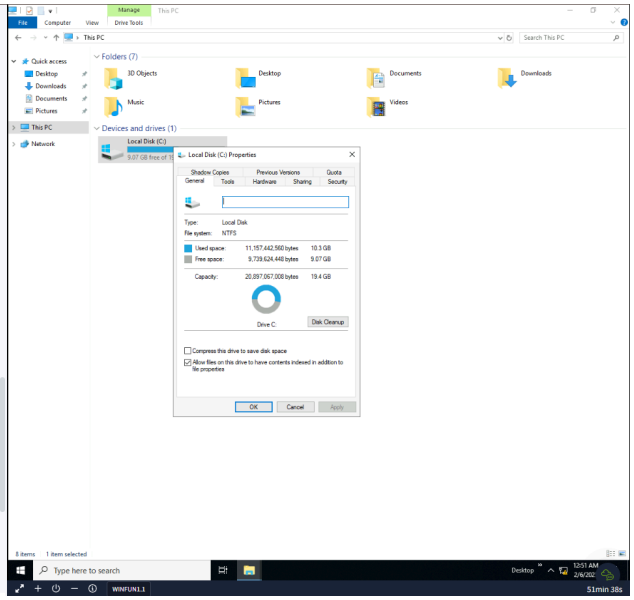

Task 2 Windows Editions
The Windows operating system has a long history dating back to 1985, and currently, it is the dominant operating system in both home use and corporate networks. Because of this, Windows has always been targeted by hackers & malware writers.
Windows XP was a popular version of 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:

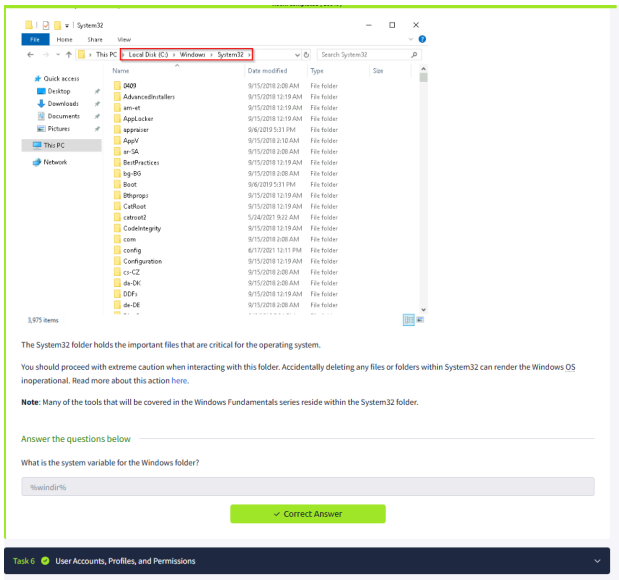

Always, hide labels
How do I customize taskbars?
Notification area
Select which icons appear on the taskbar
Turn system icons on or off
Here are Microsoft's brief documents for the Start Menu and Notification Area.
Tip: You can right-click any folder, file, app/program, or icon to view more information or perform other actions on the clicked item.
Answer the questions below
Which selection will hide/disable the Search box?
Hidden
Correct Answer
Which selection will hide/disable the Task View button?
Show Task View button
Correct Answer
Besides Clock and Network, what other icon is visible in the Notification Area?
Action Center
Correct Answer
Hint
Task 4 The File System
Task 5 The Windows\System32 Folders
Task 6 User Accounts, Profiles, and Permissions
Recycle Bin
Google Chrome
Toolbars
Search
Show Task View button
Show Windows Ink Workspace button
Show touch keyboard button
Show the desktop
Task Manager
Lock the taskbar
Taskbar settings
Hidden
Show search icon
Show search box

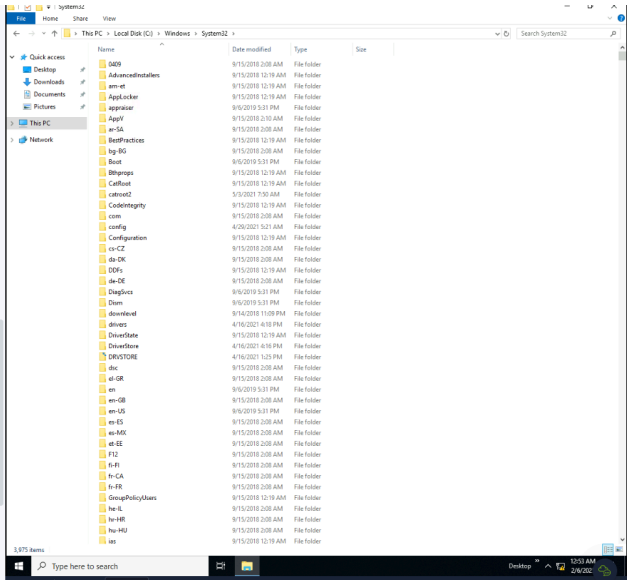
Task 4:


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

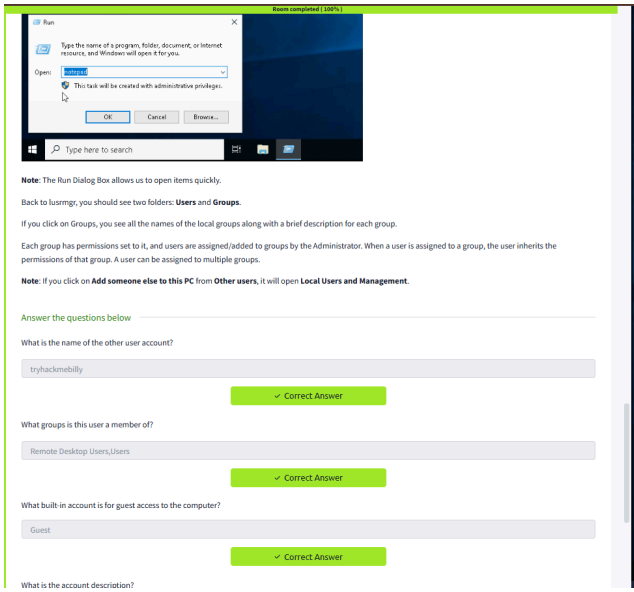


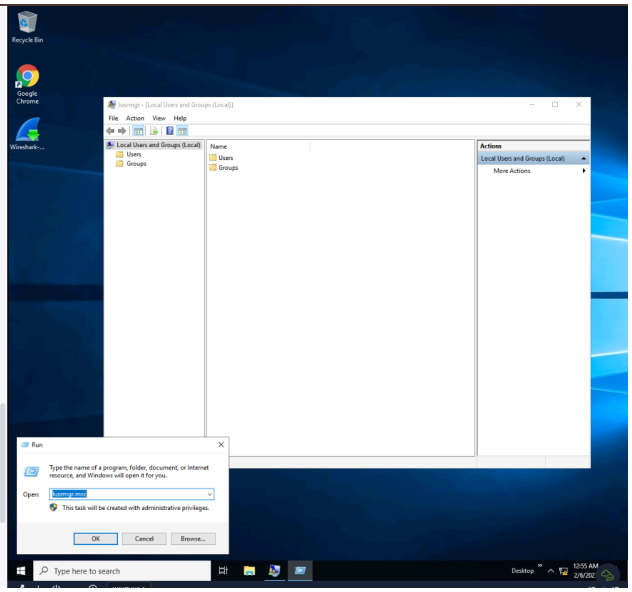
Task 5:


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

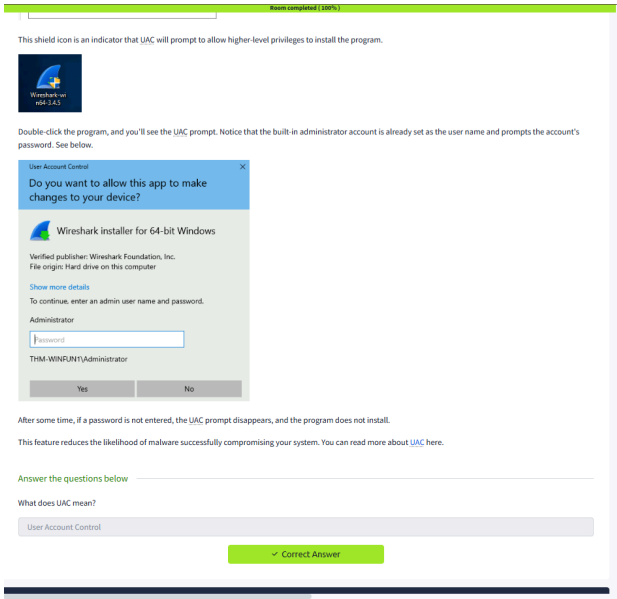
What built-in account is for guest access to the computer?

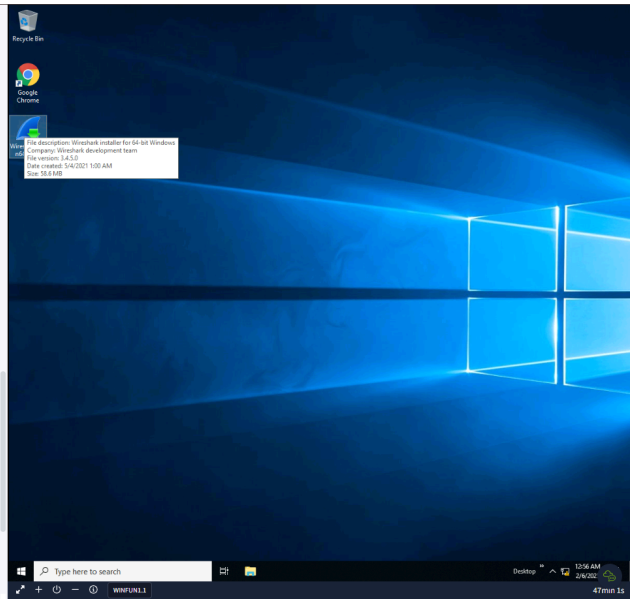
Guest

✓ Correct Answer

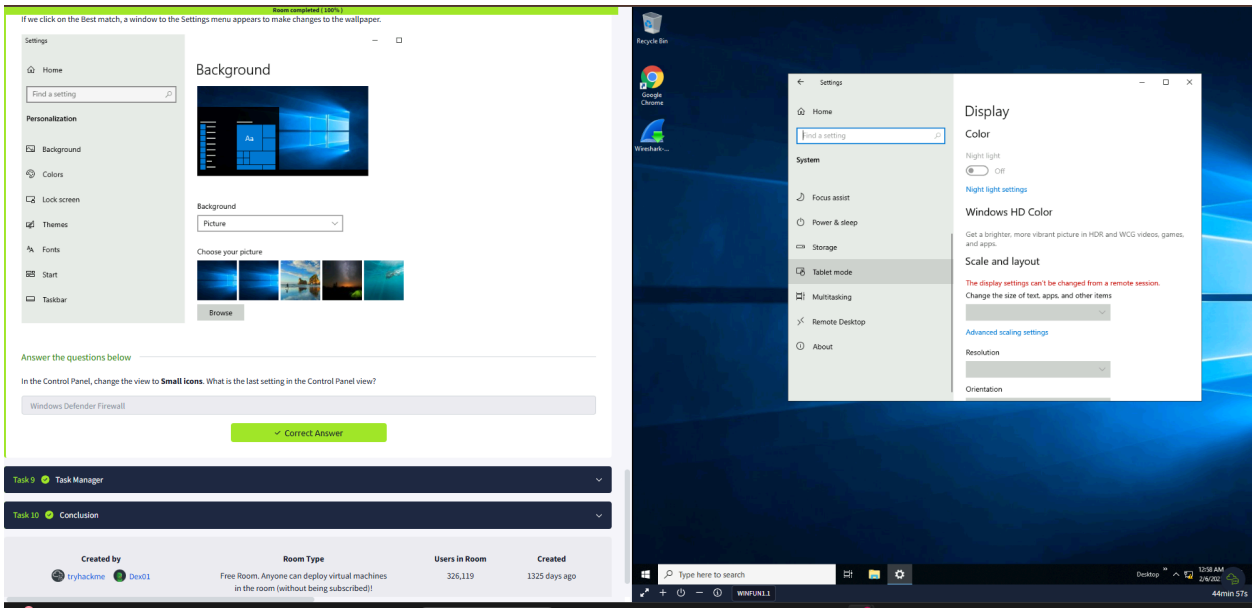
What is the account description?

Task 7:

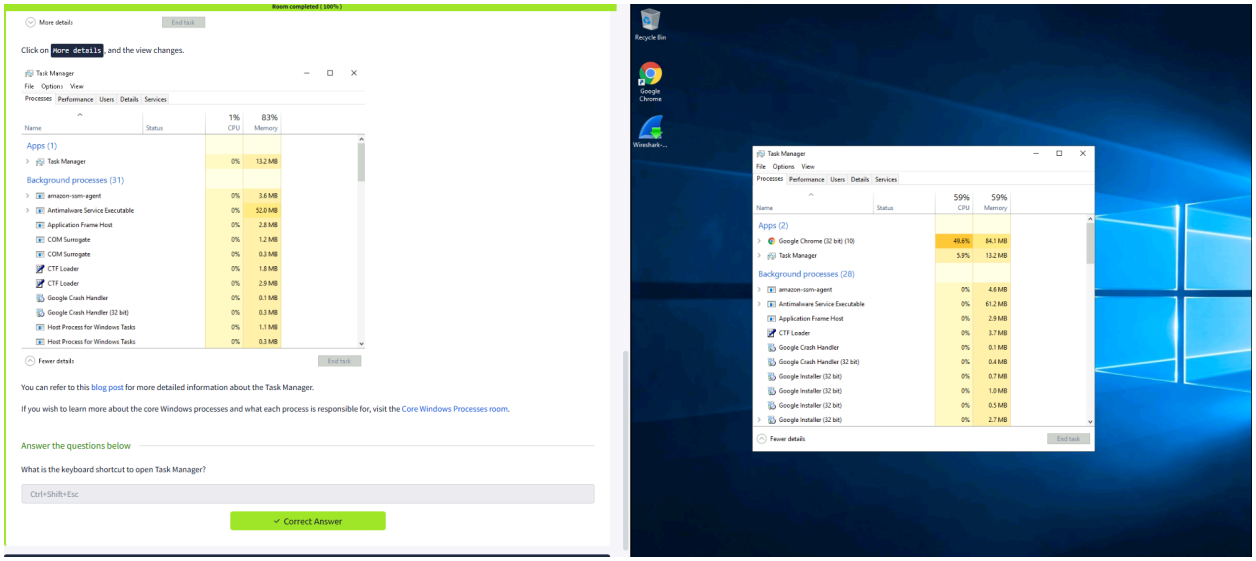




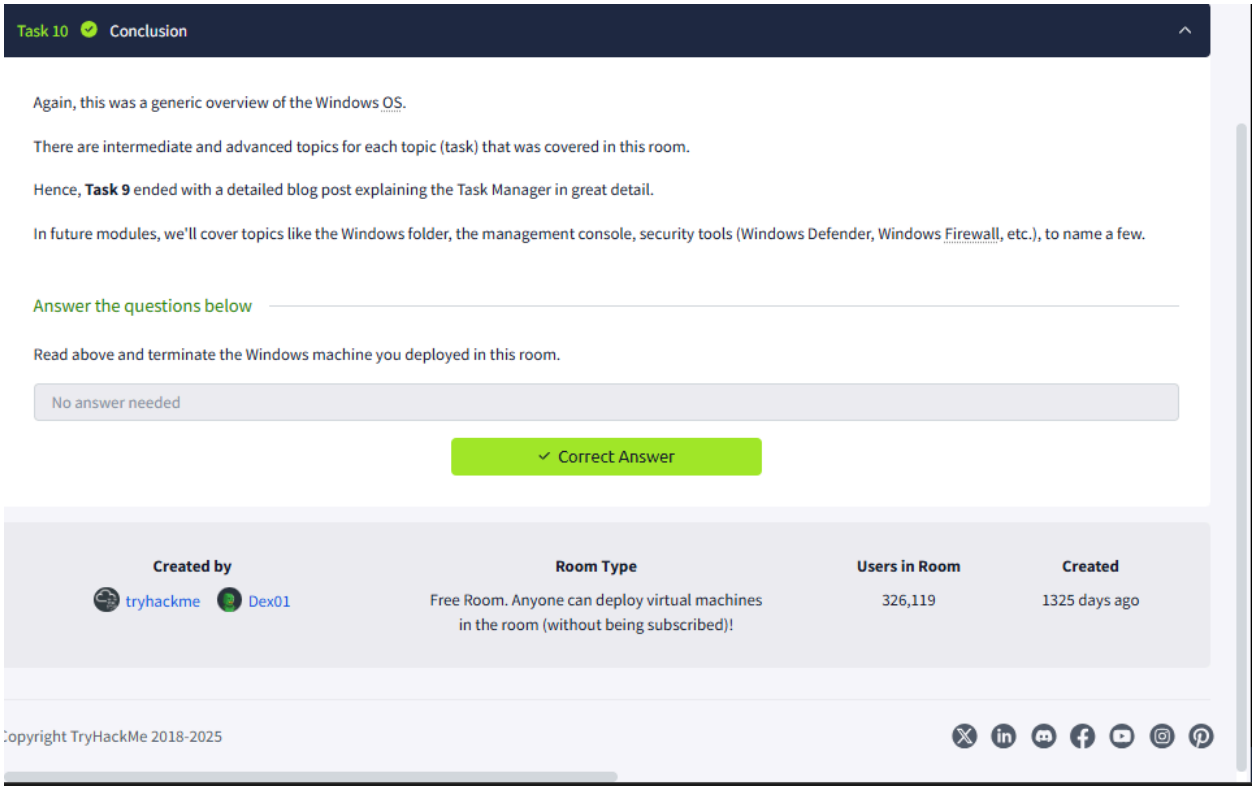
Task 8:



Task 9:



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.

EXP No : 1 B WINDOWS FUNDAMENTALS 2

DATE :

Aim:

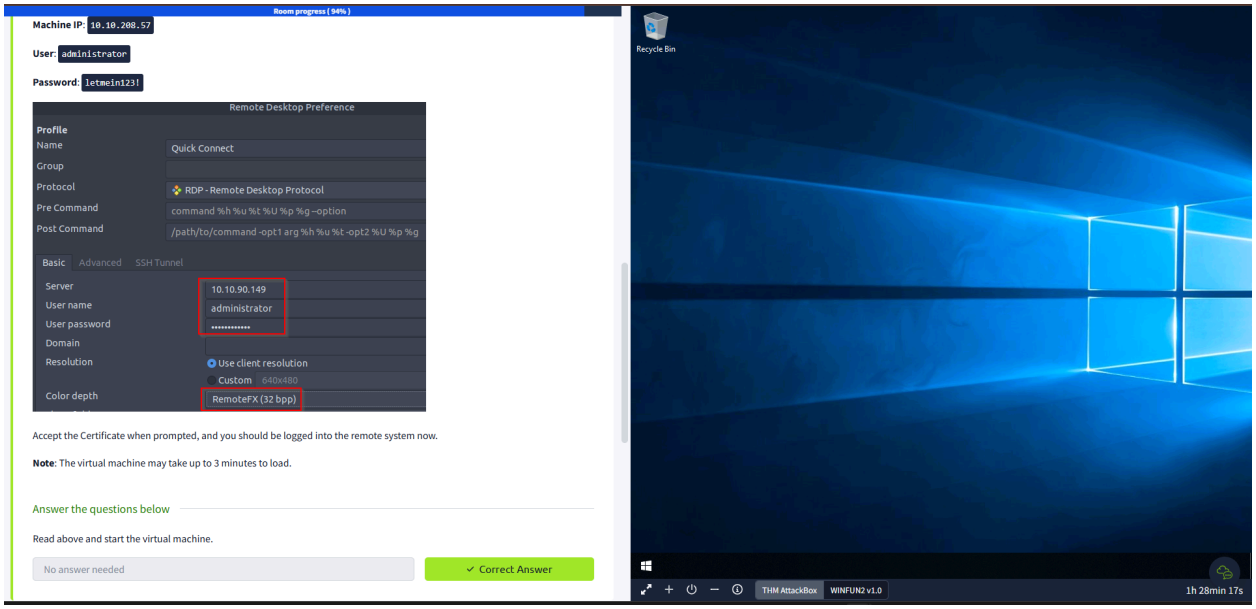
To understand and explore the fundamentals of the Windows operating system, including key components such as System Configuration UAC settings , Windows fundamental modules and Windows registry, to build a strong foundation for cybersecurity and system administration in TryHackMe platform.

Algorithm:

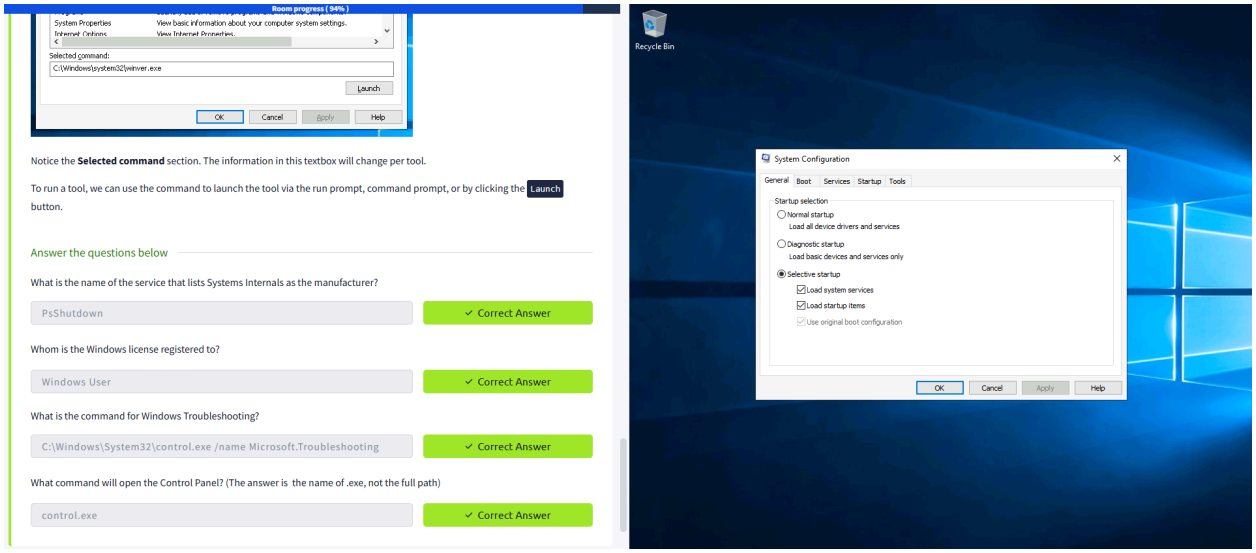
1. Access the lab in TryHackMe platform using the link below-
2. https://tryhackme.com/r/room/windowsfundamentals1xbx
3. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.
4. Solve the task questions starting with Windows OS edition and Desktop GUI.
5. Understand the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

Output:

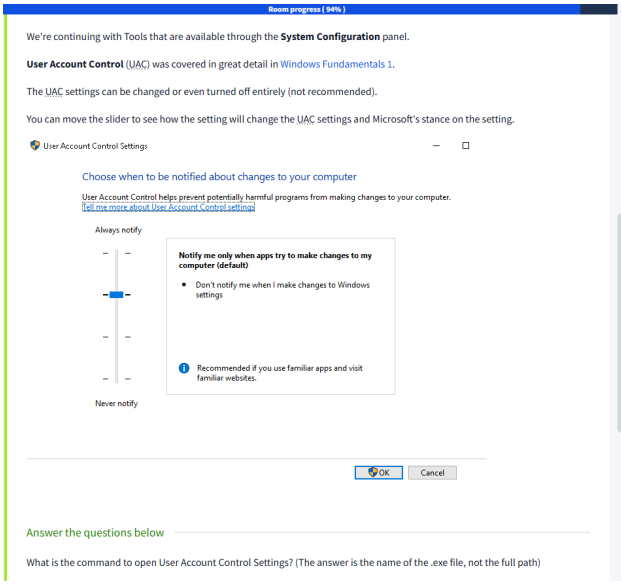
Task 1:

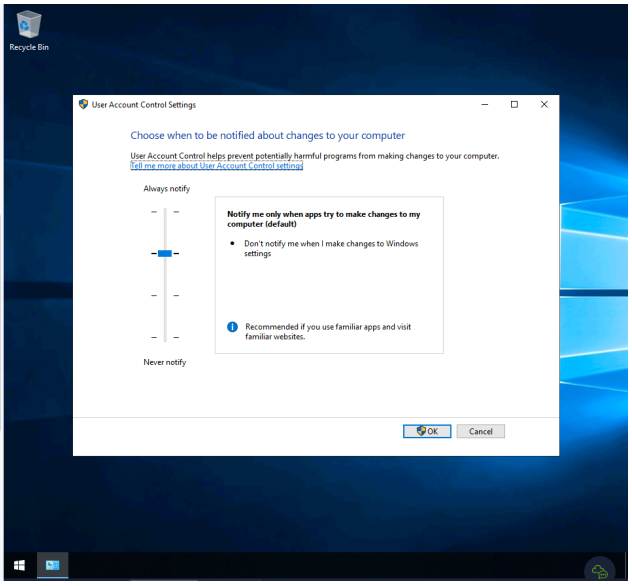


Task 2:

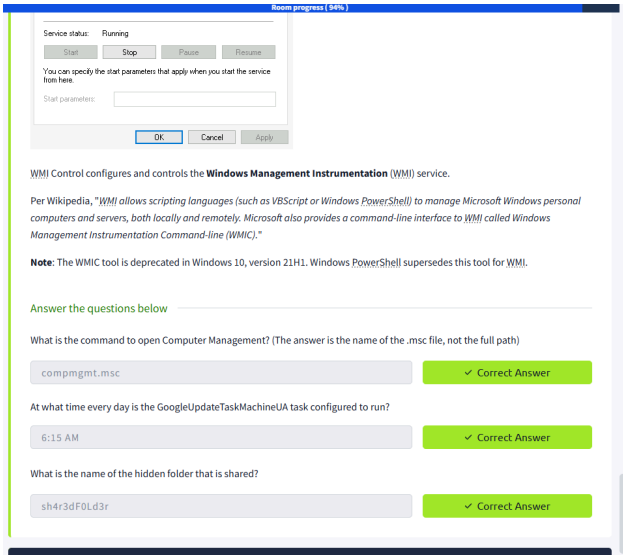


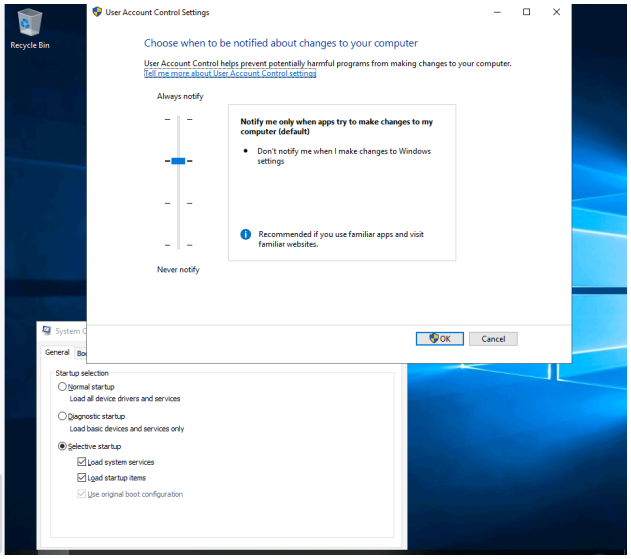
Task 3:


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)

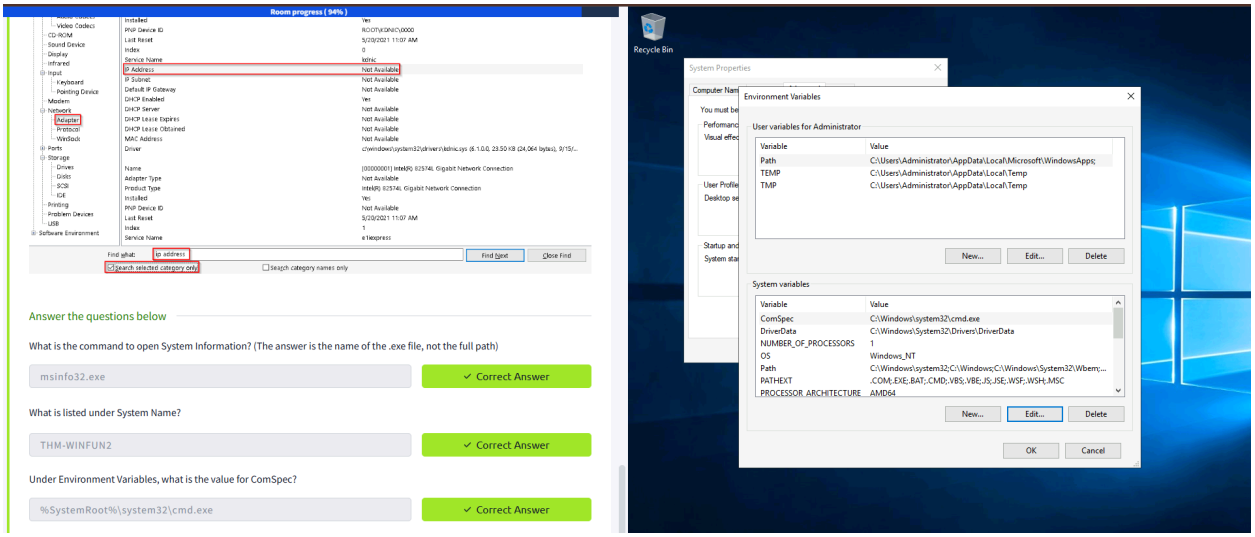

Recycle Bin
User Account Control Settings
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when apps try to make 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:

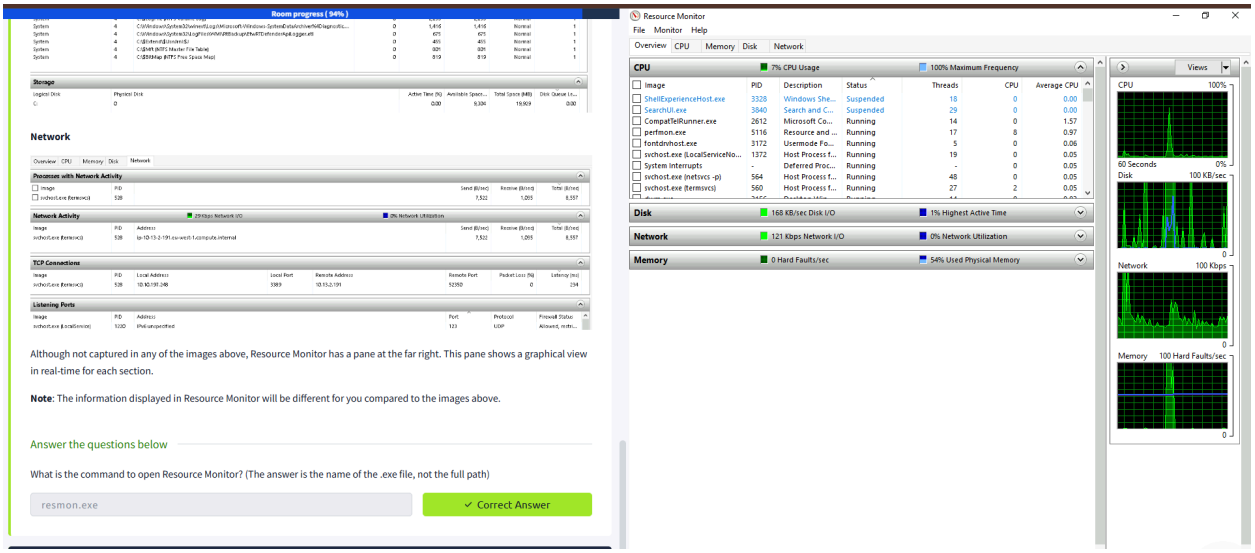

Room progress (94%)
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
WMI Control configures and controls the Windows Management Instrumentation (WMI) service.
Per Wikipedia, "WMI allows 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

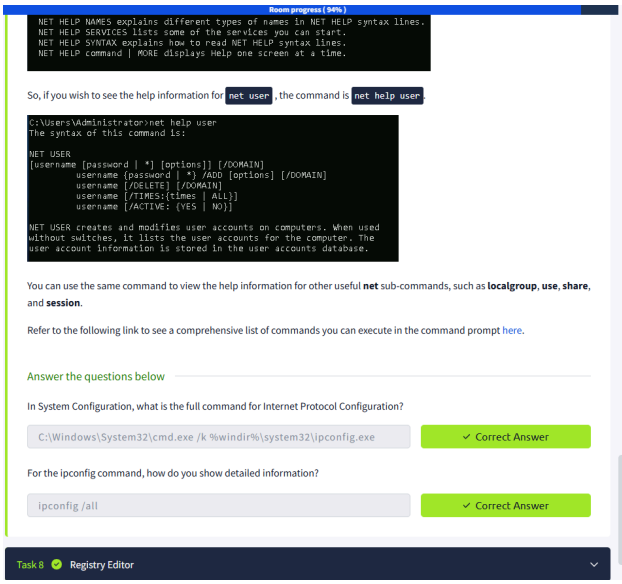
Task 5:

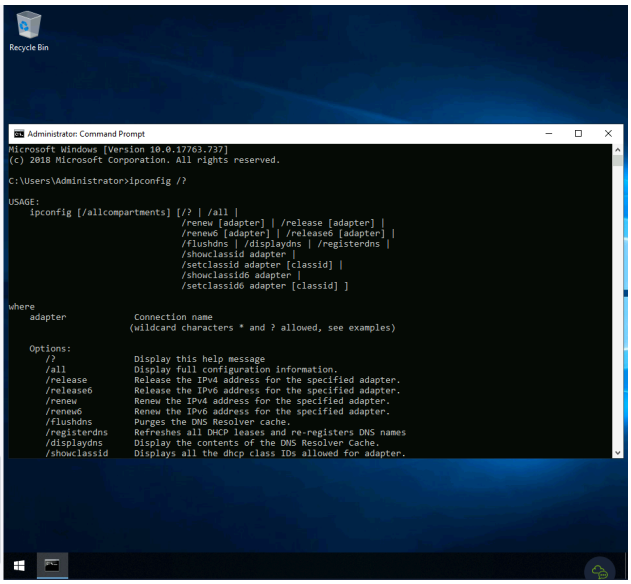

Room progress (94%)
Answer the questions below
What is the command to open System Information? (The answer is the name of the .exe file, not the full path)
msinfo32.exe
✓ Correct Answer
What is listed under System Name?
THM-WINFUN2
✓ Correct Answer
Under Environment Variables, what is the value for ComSpec?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

Task 6:

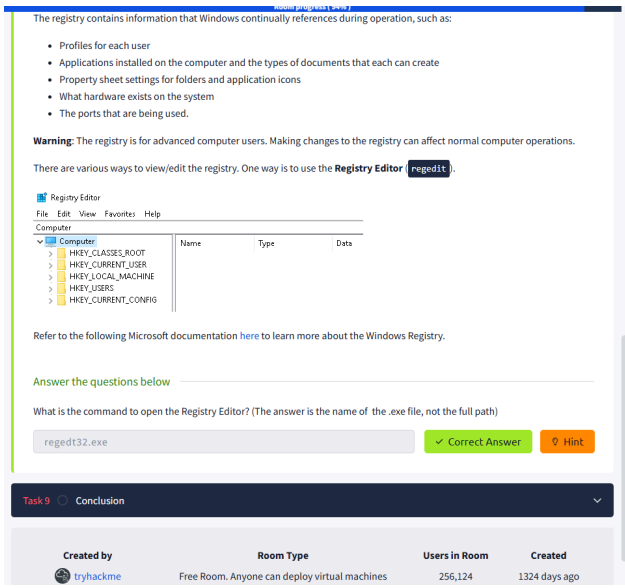

Room progress (94%)
Network
Although not captured in any of the images above, Resource Monitor has a pane at the far right. This pane shows a graphical view in real-time for each section.
Note: The information displayed in Resource Monitor will be different for you compared to the images above.
Answer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

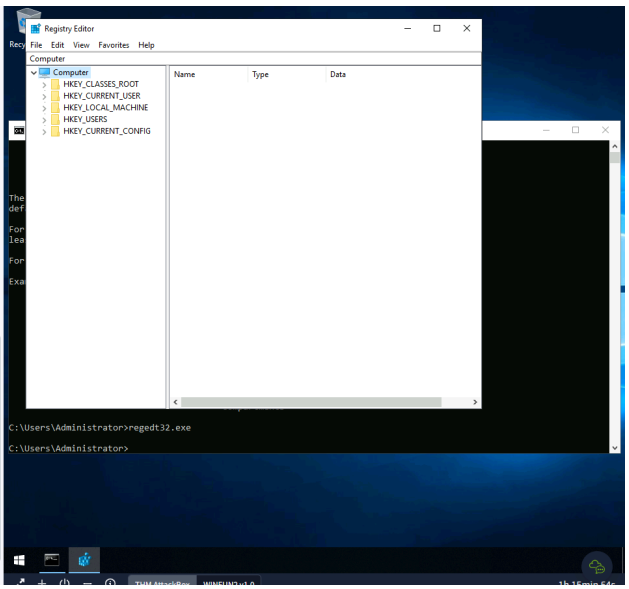
Task 7:


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

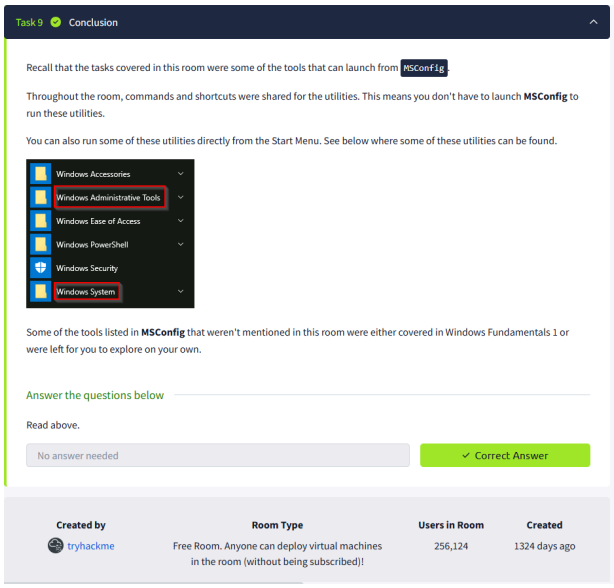

Recycle Bin
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ipconfig /?
USAGE:
ipconfig [/allcompartments] [/? | /all |
/renew [adapter] | /release [adapter] |
/renew6 [adapter] | /release6 [adapter] |
/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.

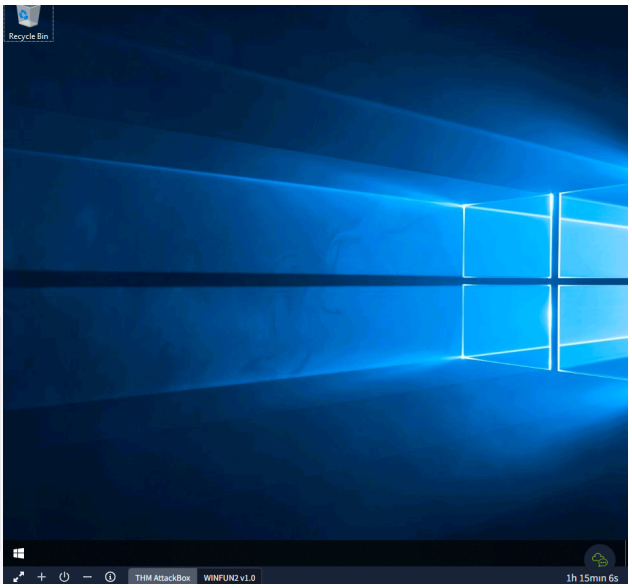
Task 8:


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:

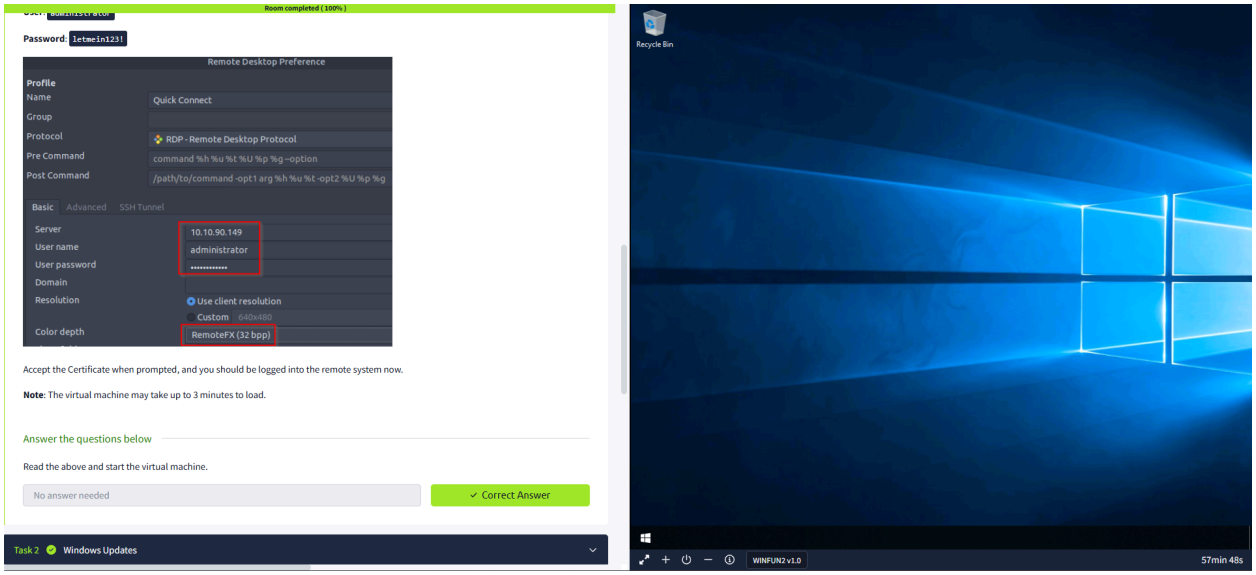
To understand and explore the fundamentals of the Windows built-in tools, including key components such as the device secure system, Windows Security, Bit locker in TryHackMe platform.

Algorithm:

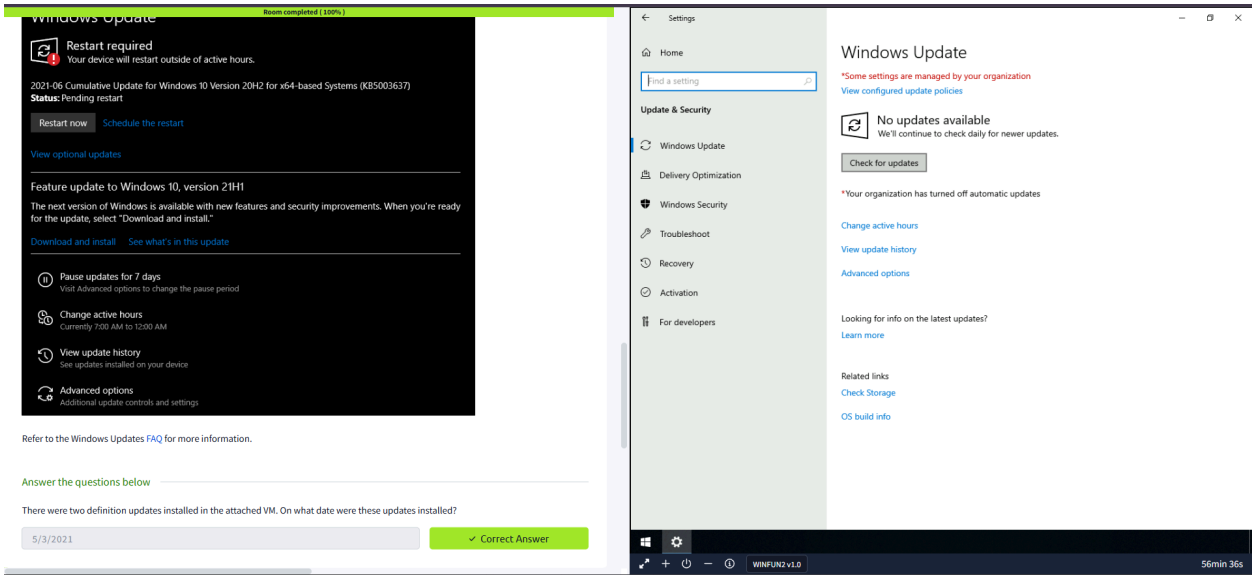
1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/r/room/windowsfundamentals1xbx
2. Click Start a Machine and AttackBox to run the instance of Windows
3. distribution.
4. Solve the task questions start with Windows built-in tools.
5. Understand the importants of Device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

Output:

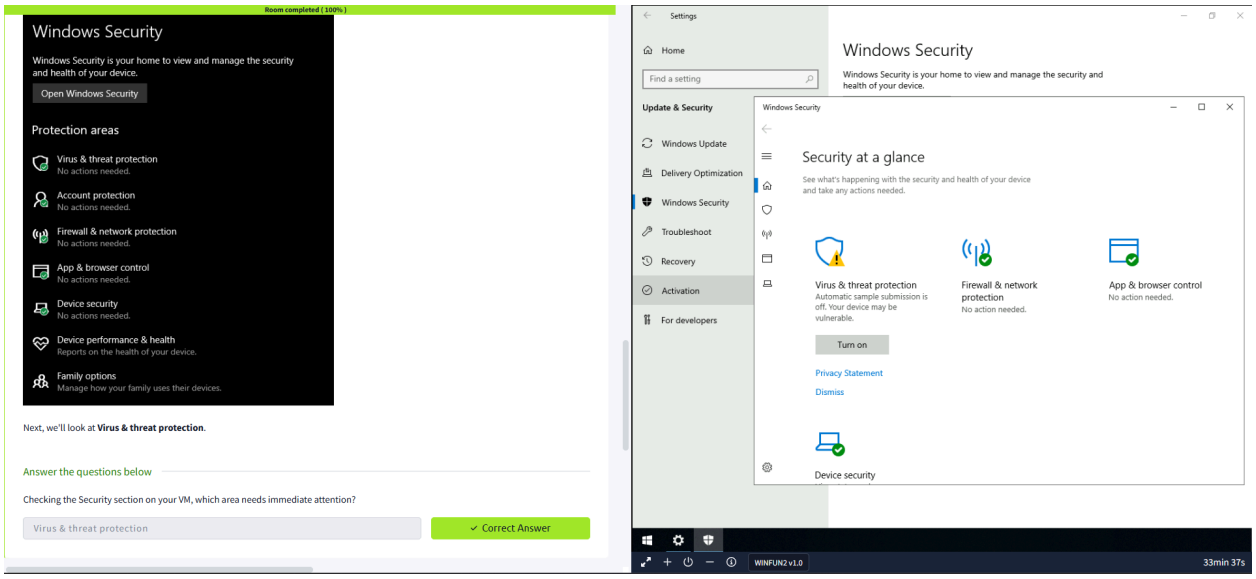
Task 1:



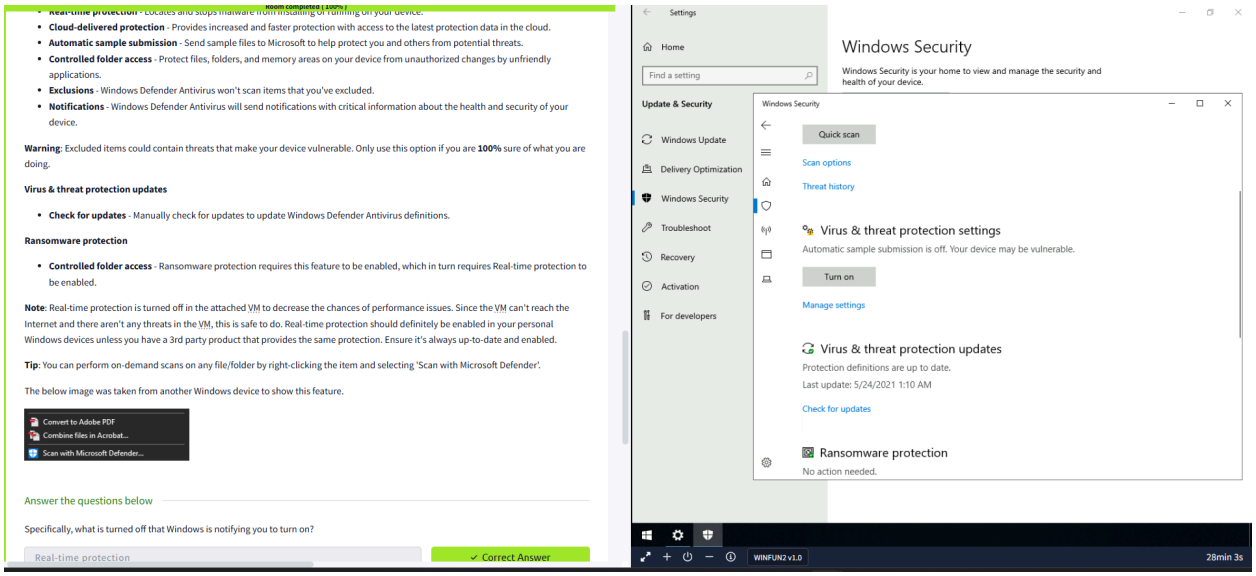
Task 2:



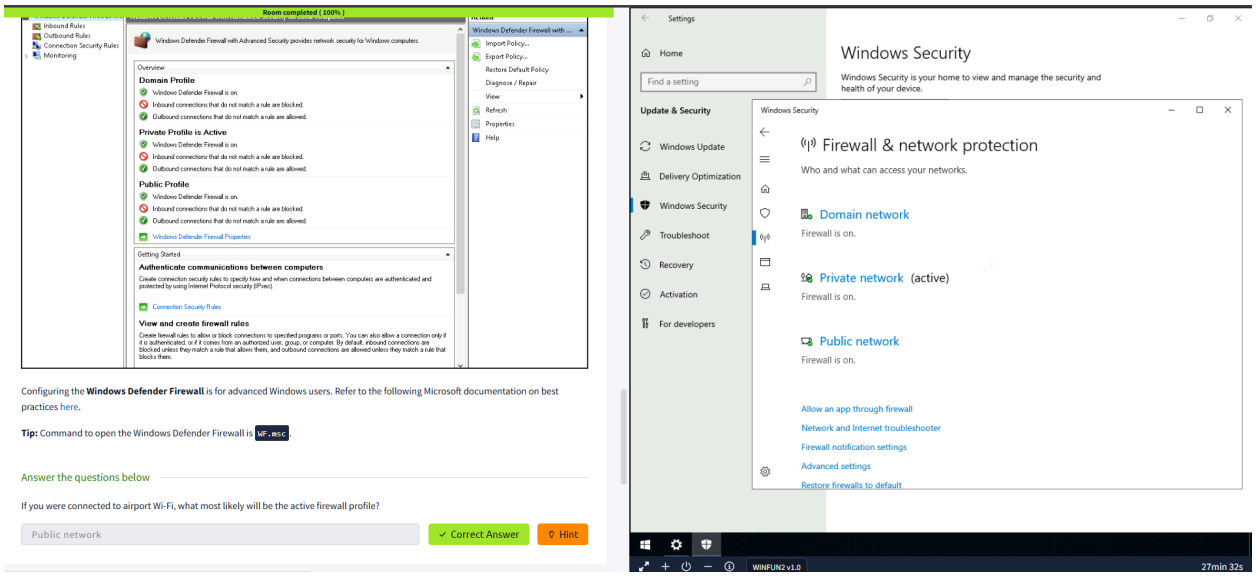
Task 3:


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

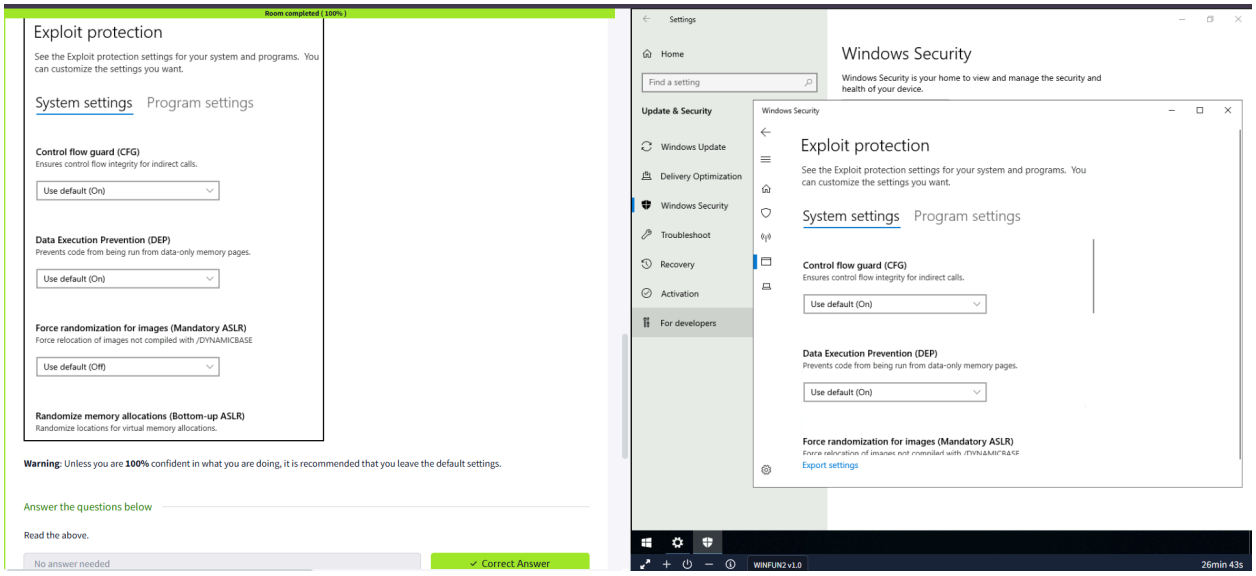
Task 4:


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

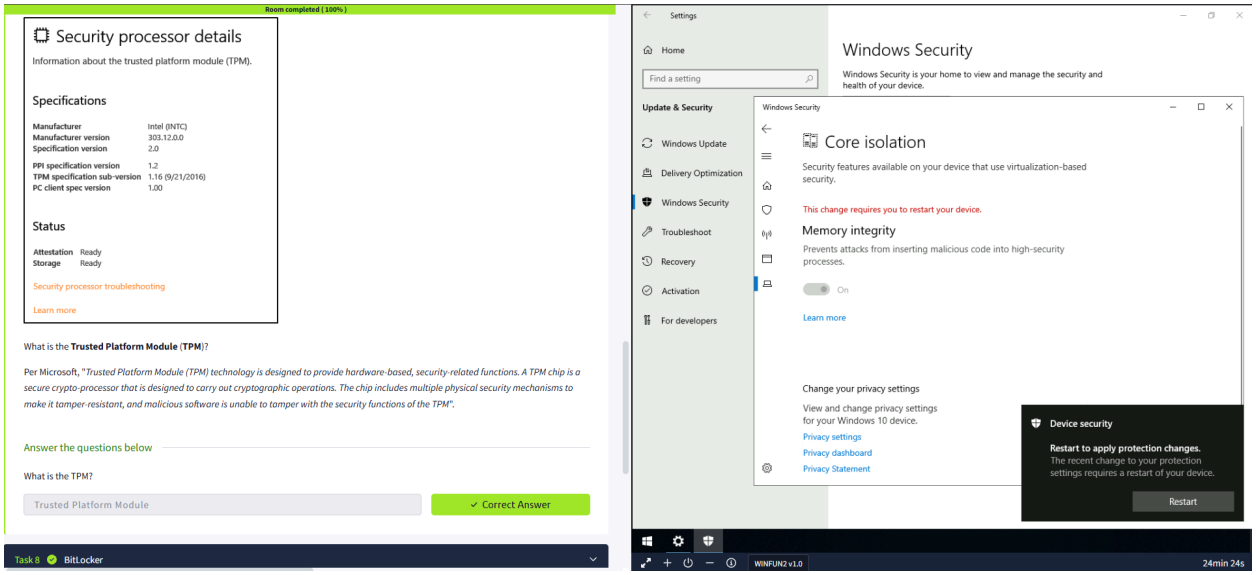
Task 5:


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
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.
Public 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.
Windows Defender Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
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
Windows Security is your home to view and manage the security and health of your device.
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)
Firewall is on.
Public network
Firewall is on.
Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default
WINFUN2 v1.0
27min 32s

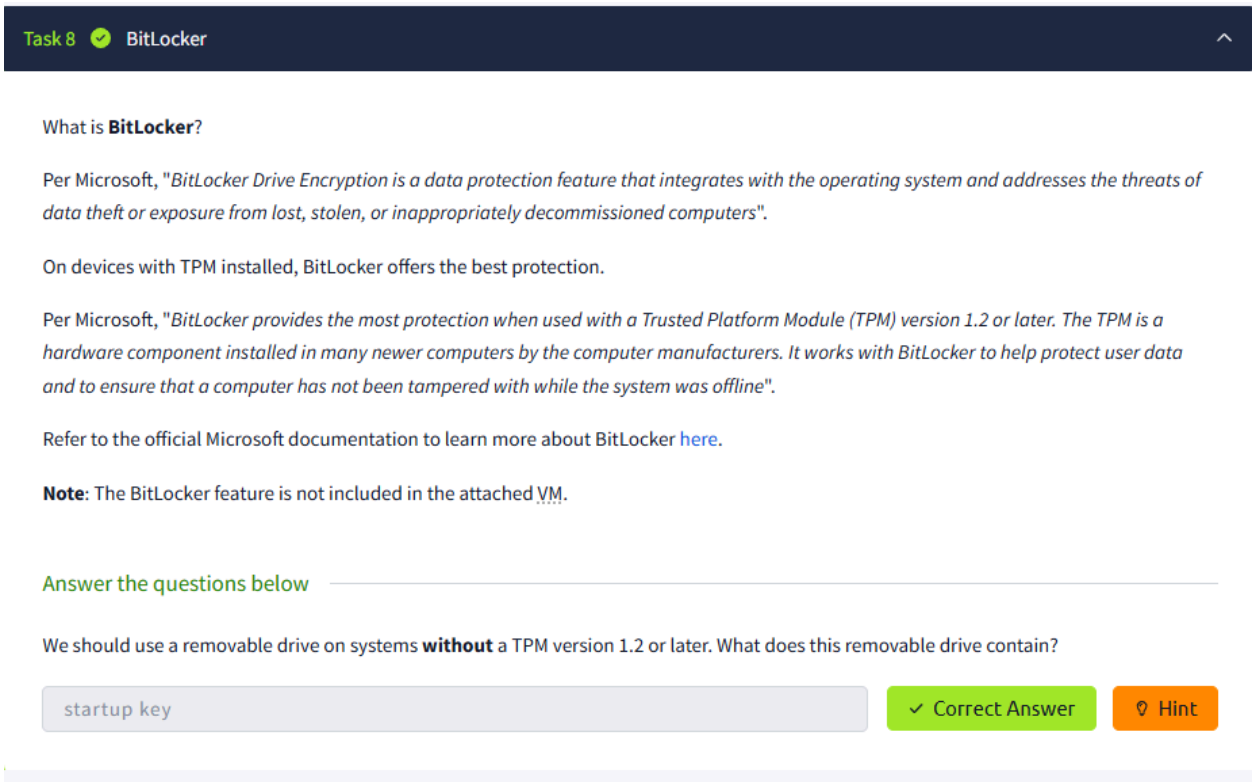
Task 6:


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
Windows Security is your home to view and manage the security and health of your device.
Update & Security
Windows Update
Delivery Optimization
Windows Security
Troubleshoot
Recovery
Activation
For developers
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)
Export settings
WINFUN2 v1.0
26min 43s

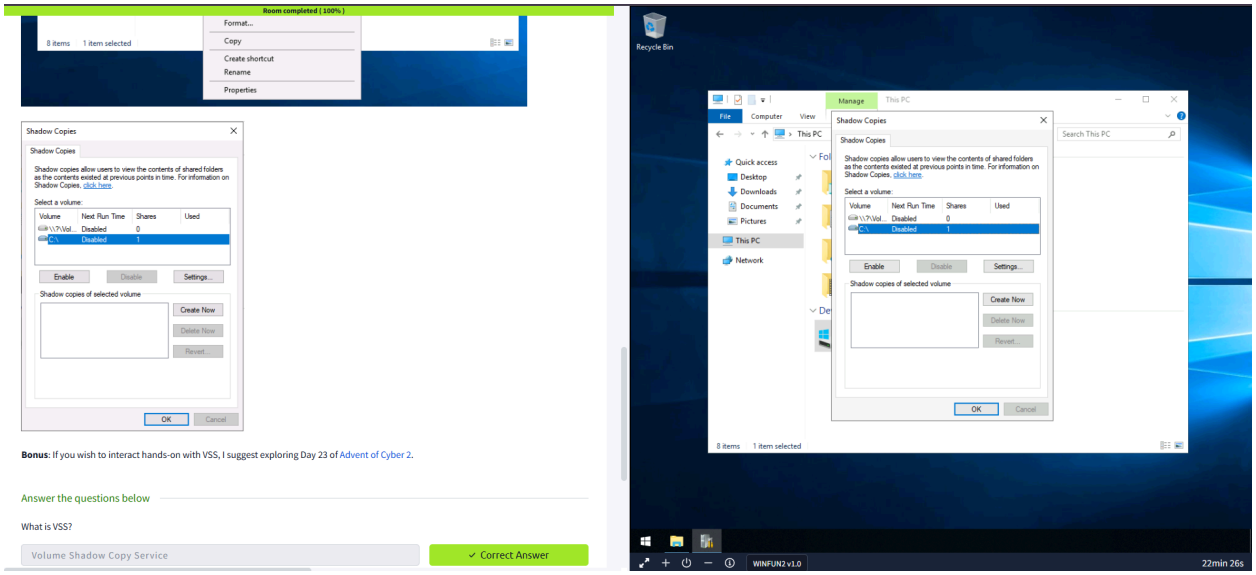
Task 7:


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

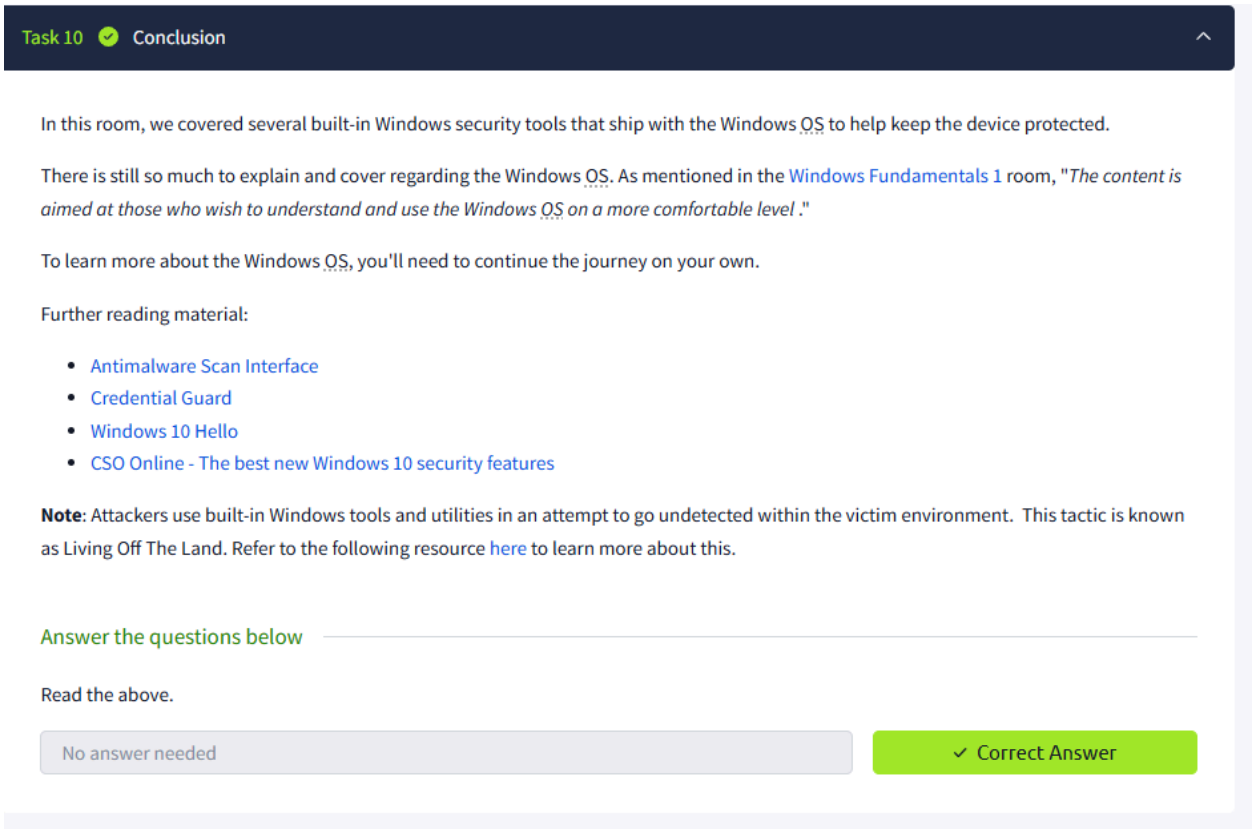
Task 8:


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!

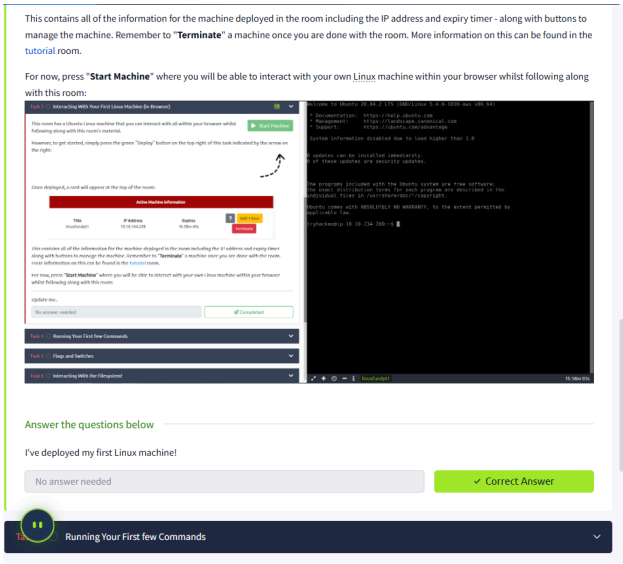
Similar to how you have different versions Windows (7, 8 and 10), there are many different versions/distributions of Linux.

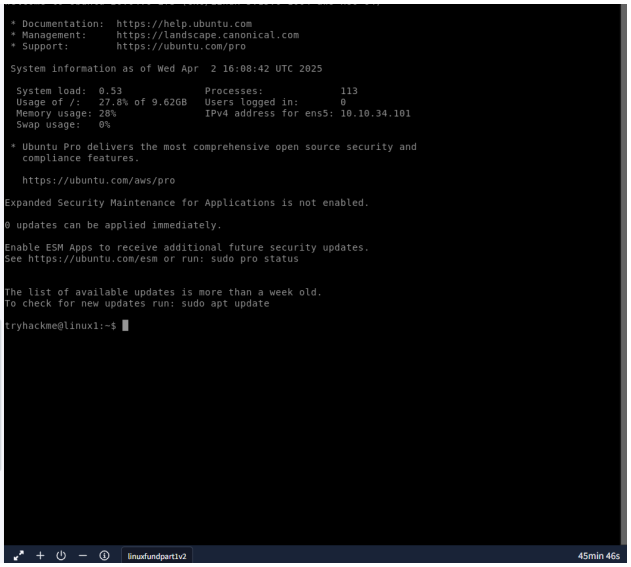
Answer the questions below

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

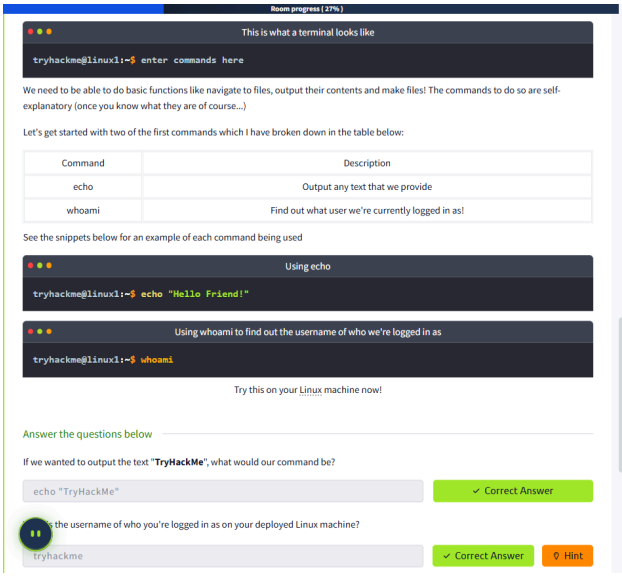
- 1980
- 1985
- 1989
- 1991 ✓ Correct Answer

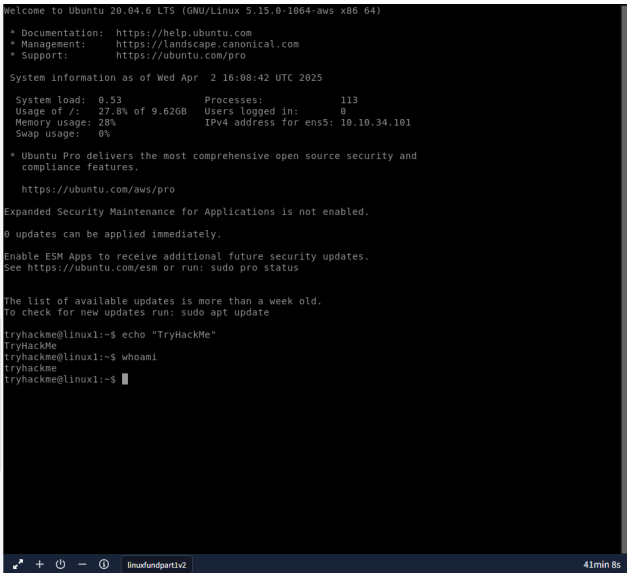
Task 3:


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

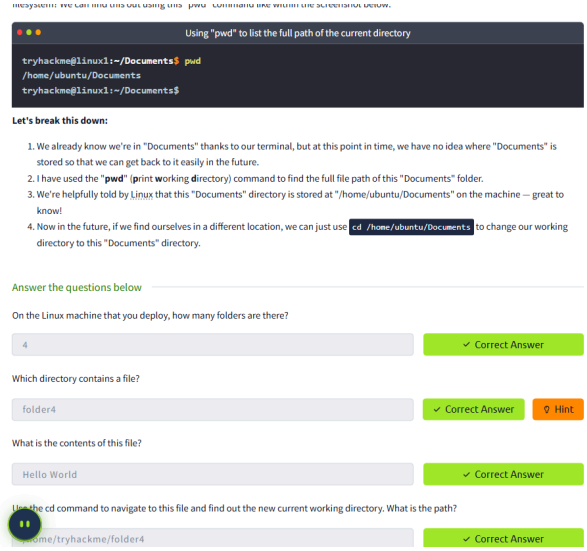

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Wed Apr 2 16:08:42 UTC 2025
System load: 0.53 Processes: 113
Usage of /: 27.8% of 9.62GB Users logged in: 0
Memory usage: 28% IPv4 address for ens5: 10.10.34.101
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

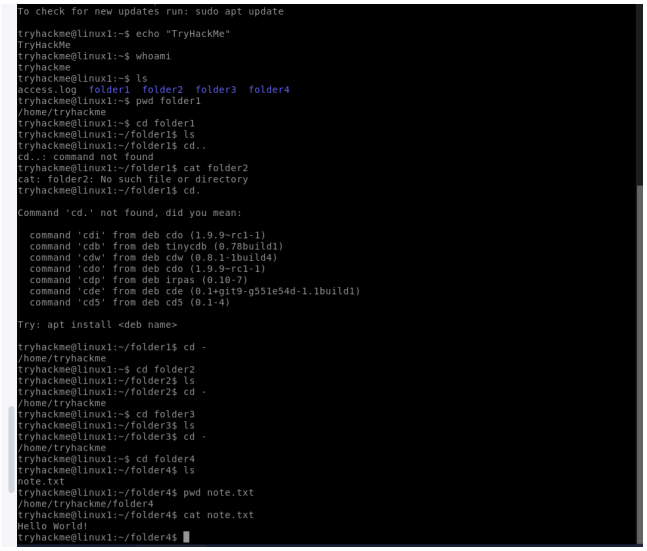
Task 4:


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

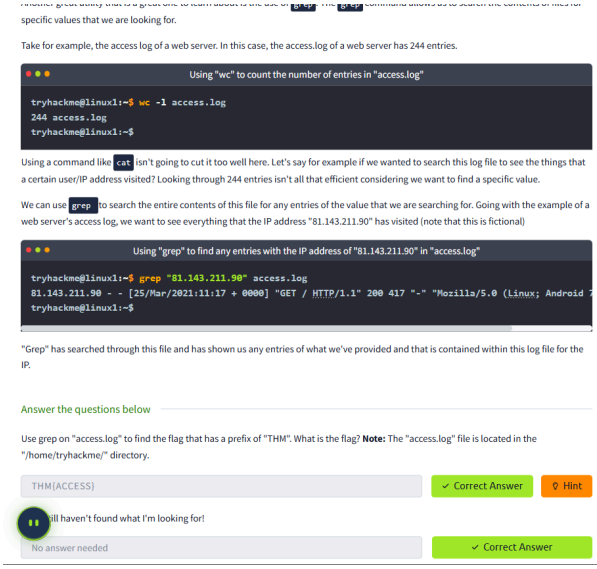

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1064-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Wed Apr 2 16:08:42 UTC 2025
System load: 0.53 Processes: 113
Usage of /: 27.8% of 9.62GB Users 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

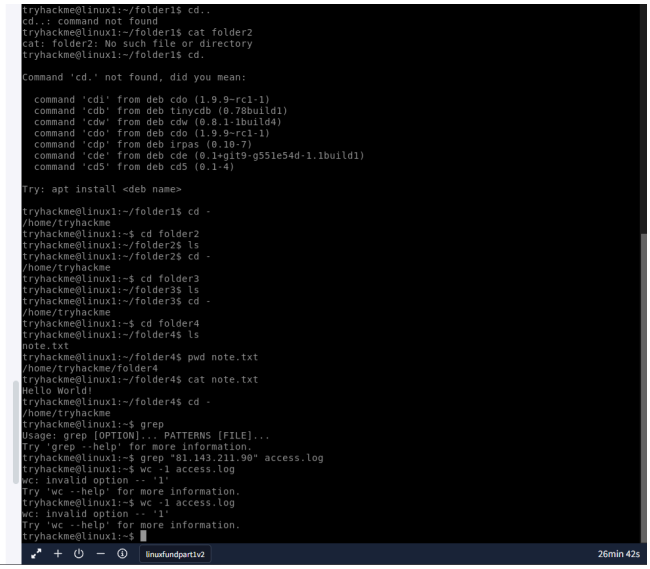
Task 5:


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" (print working directory) 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

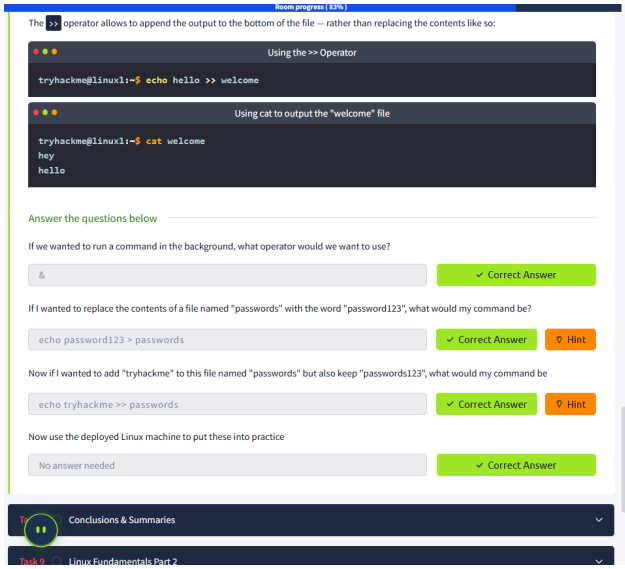

To check for new updates run: sudo apt update
tryhackme@linux1:~$ echo "TryHackMe"
TryHackMe
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log folder1 folder2 folder3 folder4
tryhackme@linux1:~$ pwd folder1
/home/tryhackme
tryhackme@linux1:~$ cd folder1
tryhackme@linux1:~/folder1$ 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$

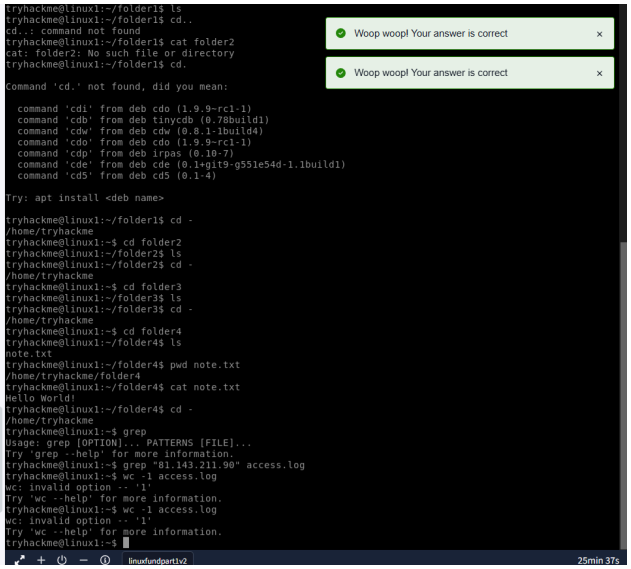
Task 6:


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
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
No answer needed
Correct Answer

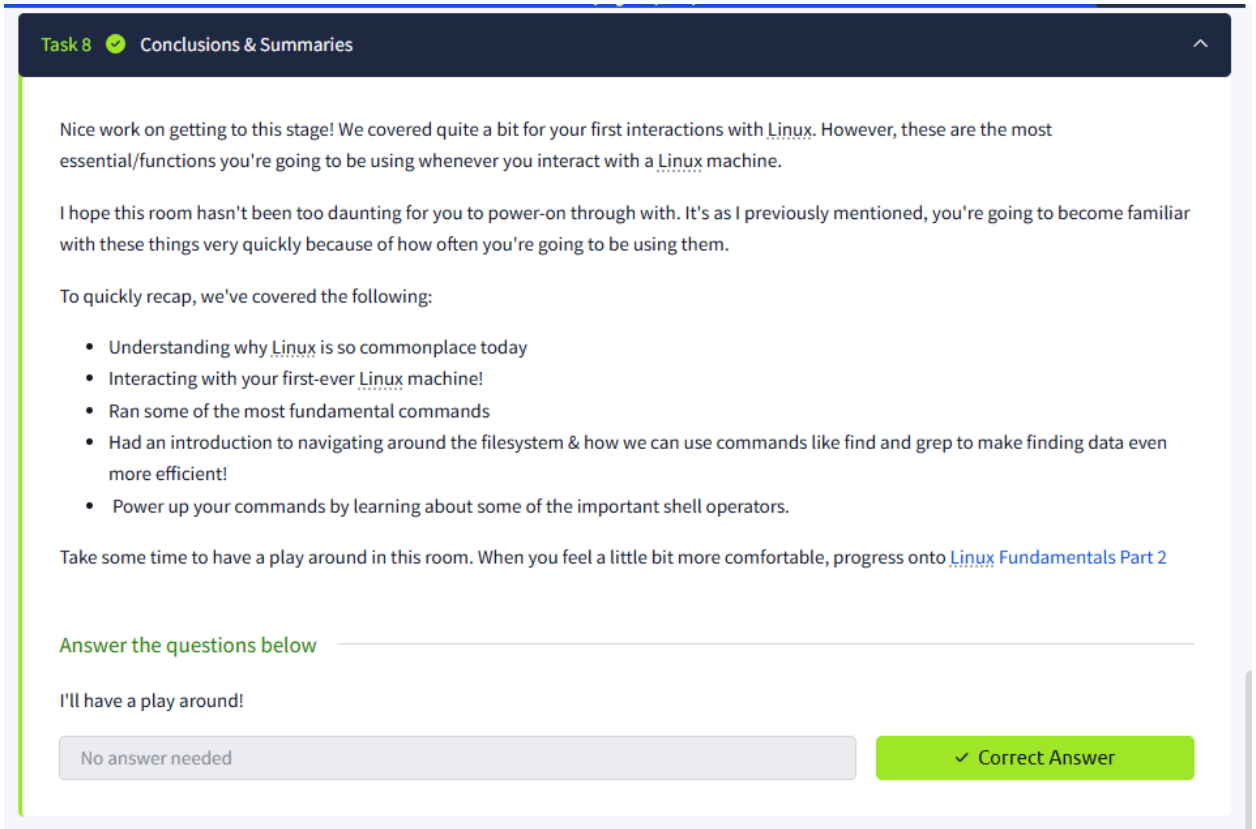

tryhackme@linux1:~/folder1$ cd..
cd..: command not found
tryhackme@linux1:~/folder1$ cat folder2
cat: folder2: No such file or directory
tryhackme@linux1:~/folder1$ cd.
Command 'cd.' not found, did you mean:
command 'cdi' from deb cdo (1.9.9~rc1-1)
command 'cdb' from deb tinycdb (0.78build1)
command '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:

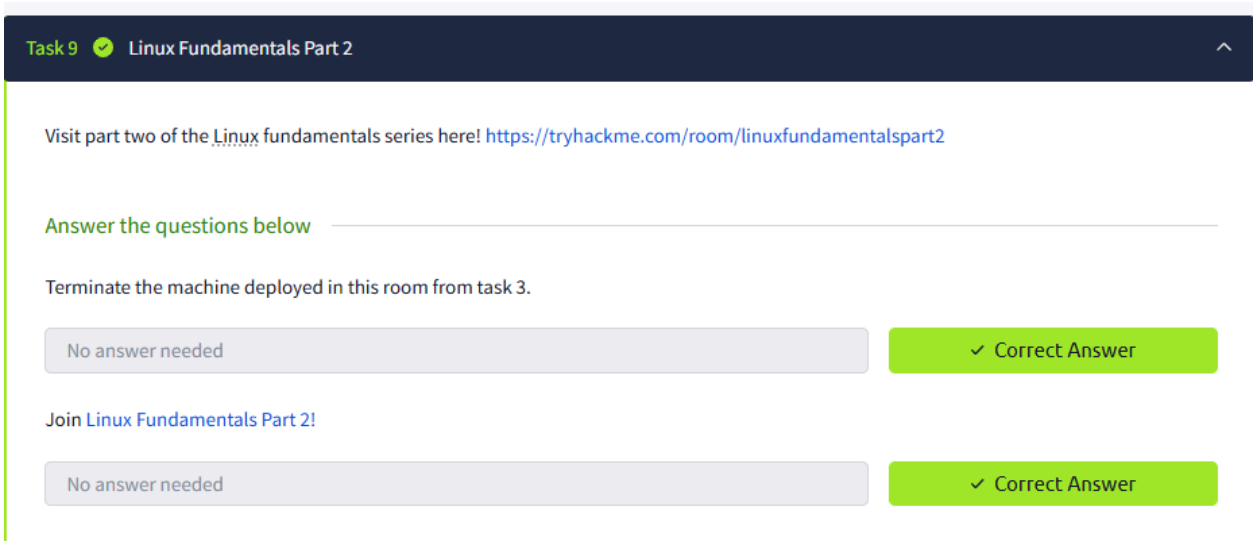

Room progress (83%)
The >> operator allows to append the output to the bottom of the file — rather than replacing the contents like so:
Using the >> Operator
tryhackme@linux1:~$ echo hello >> welcome
Using cat to output the "welcome" file
tryhackme@linux1:~$ cat welcome
hey
hello
Answer the questions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


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:

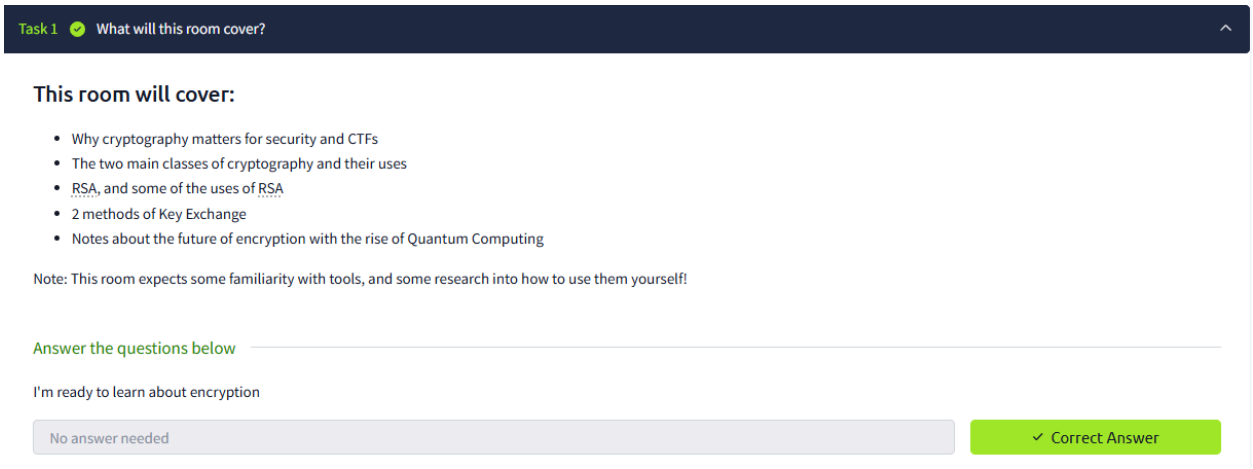
To understand and explore the Encryption used in cryptography techniques for security including two main classes of cryptography, RSA , uses of RSA, 2 methods of Key Exchange.

Algorithm:

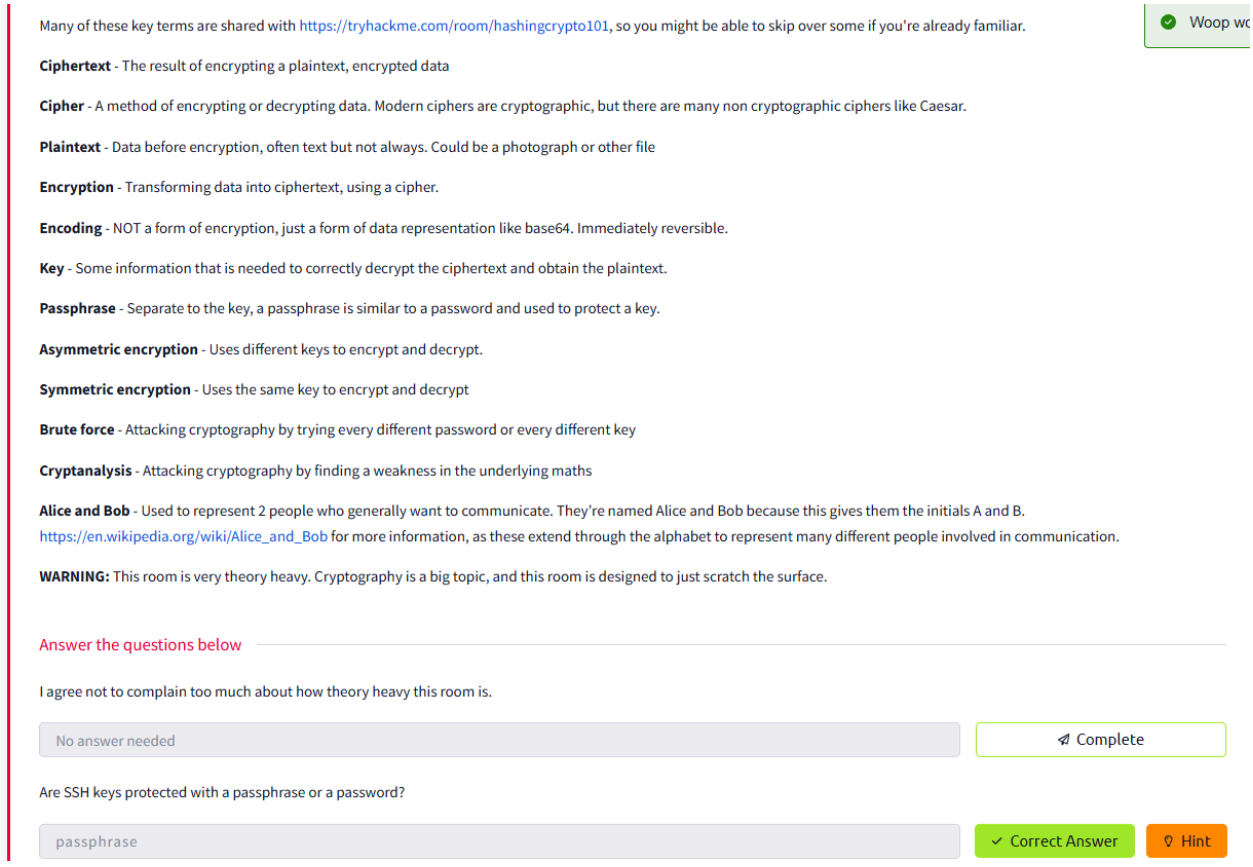
1. Access the lab in TryHackMe platform using the link below- https://tryhackme.com/room/linuxfundamentalspart1
2. Click join a room and execute tasks.
3. Learn the key terms of Encryption.
4. Learn why encryption techniques are so important.
5. Study crucial crypto math.
6. Study the types of encryption, 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:

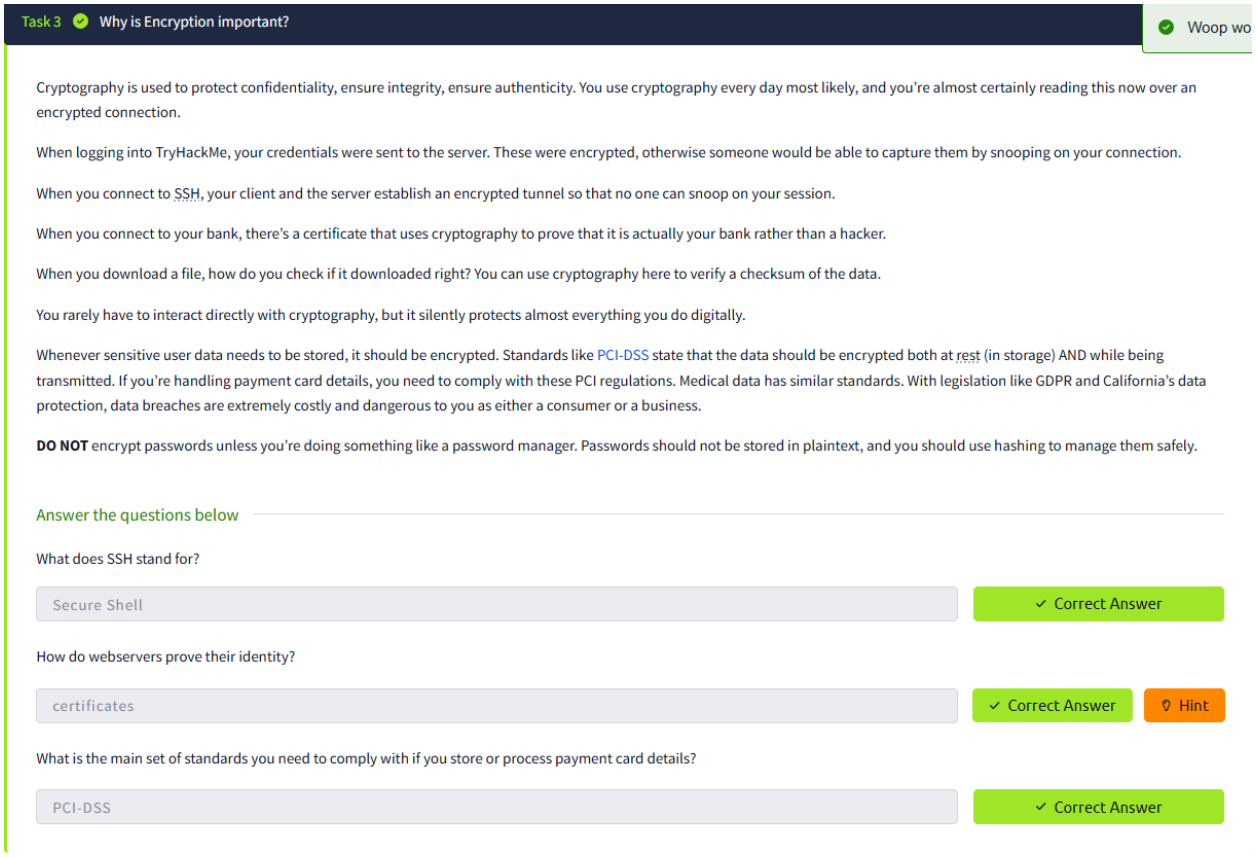
Task 1:



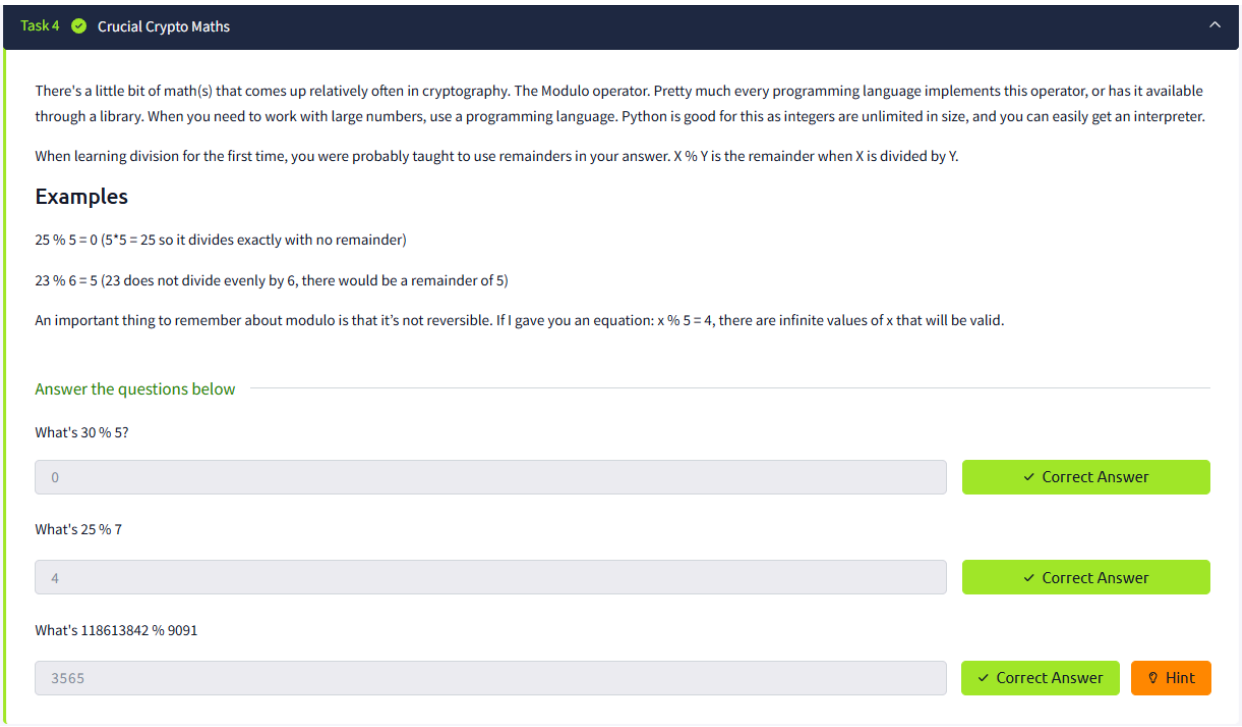
Task 2:



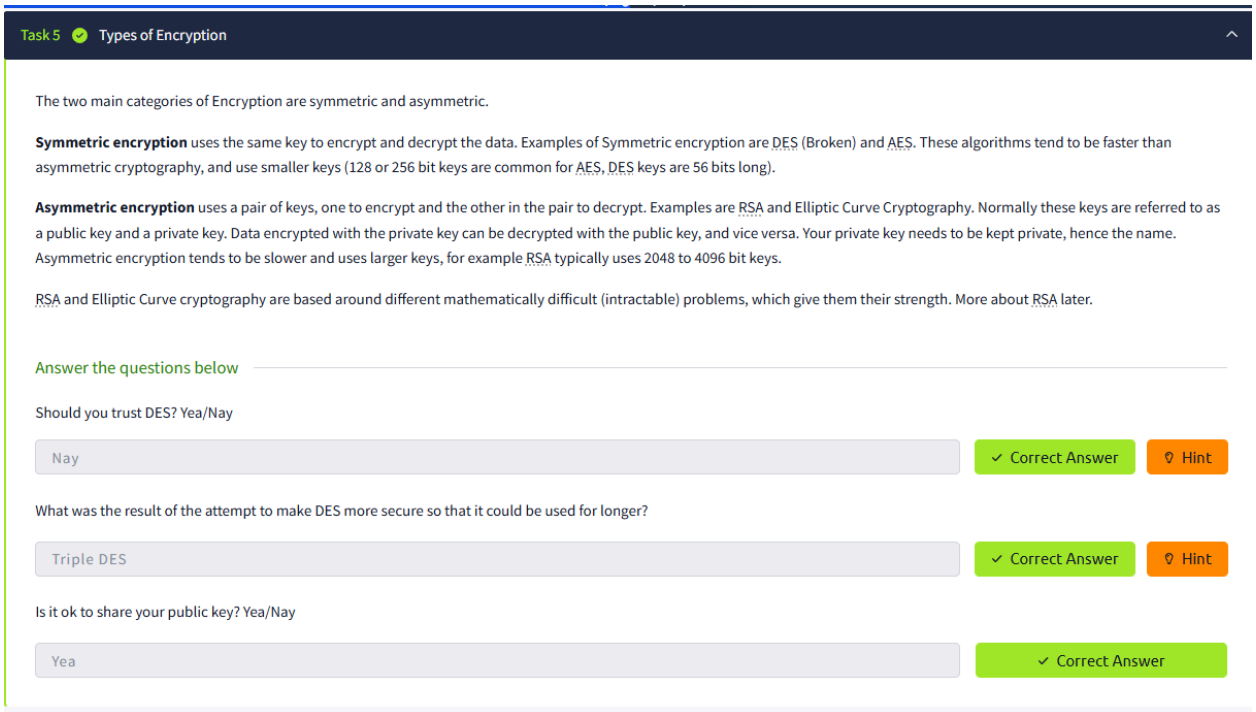
Task 3:


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

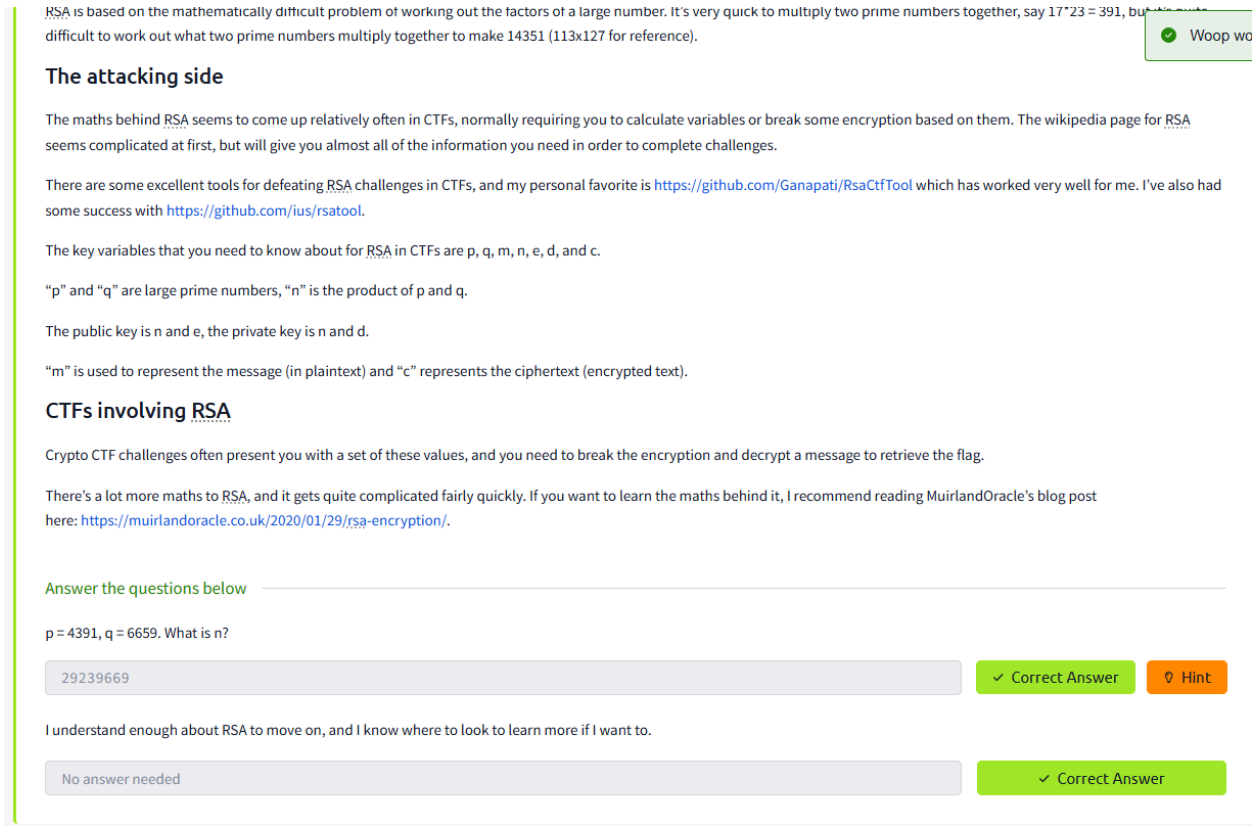
Task 4:


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

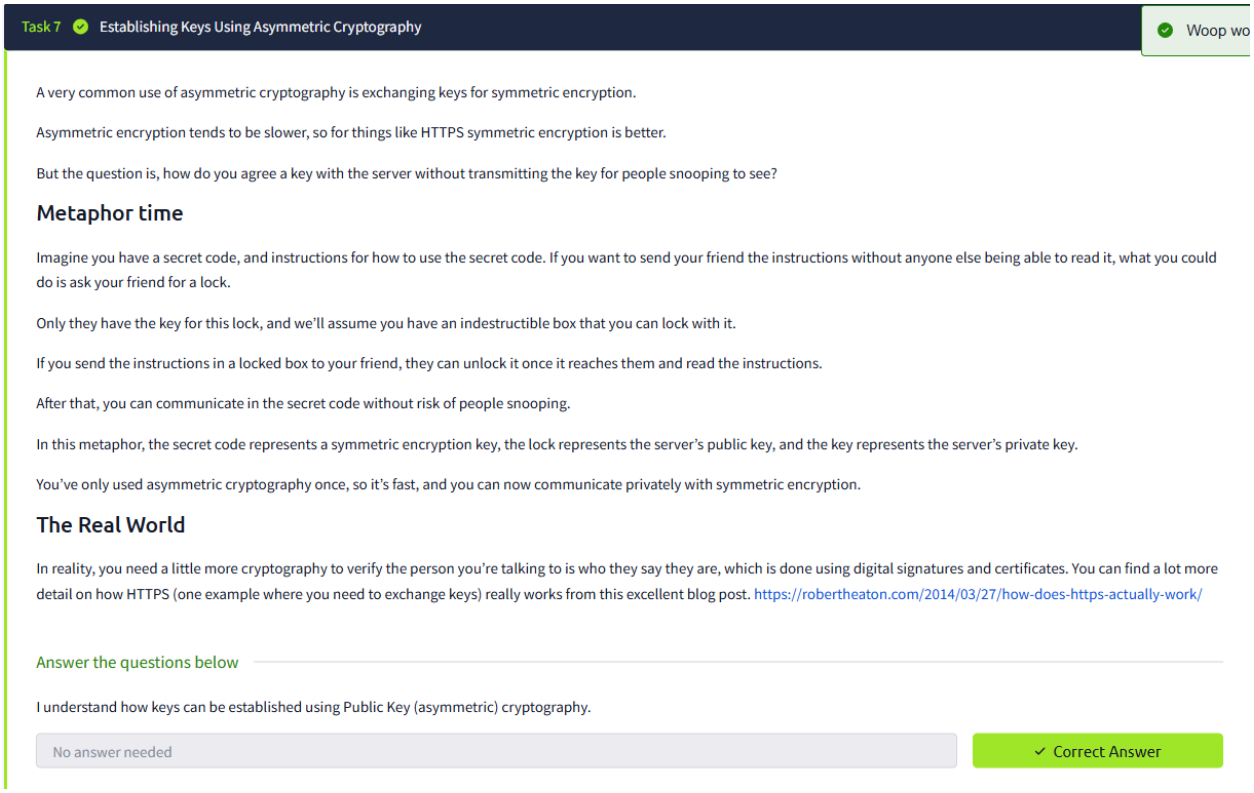
Task 5:


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

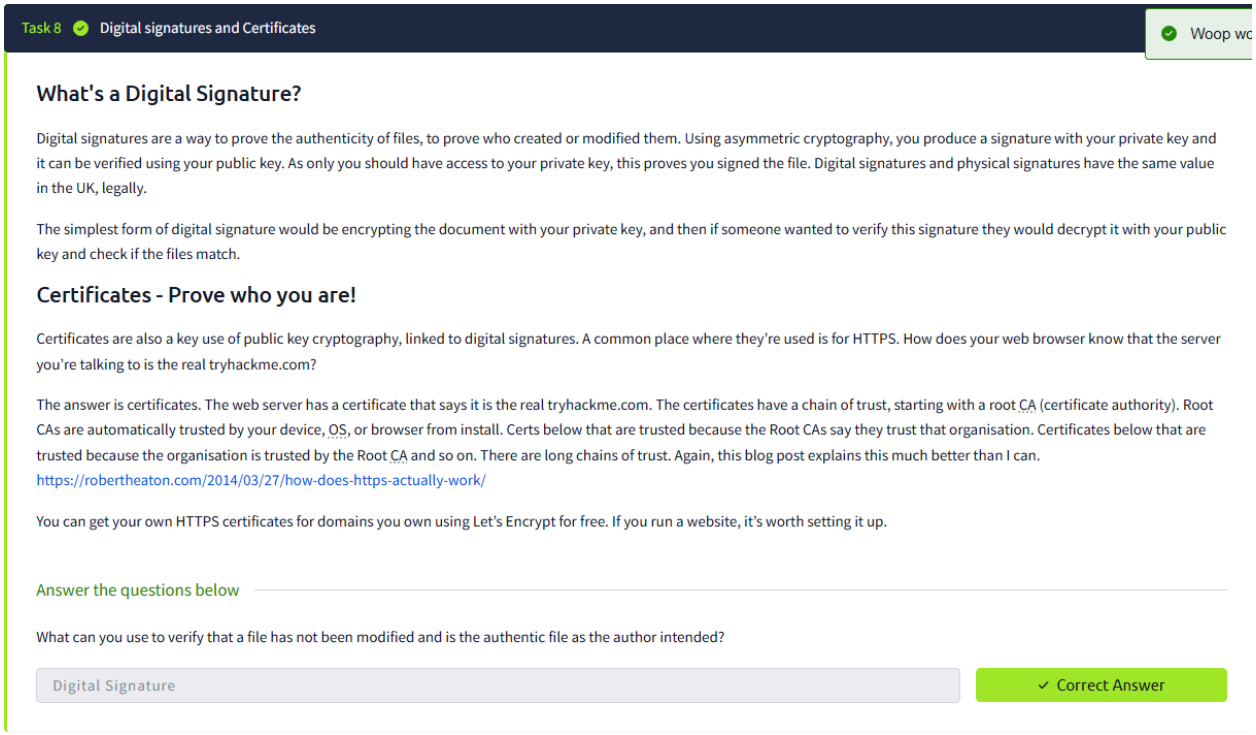
Task 6:


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

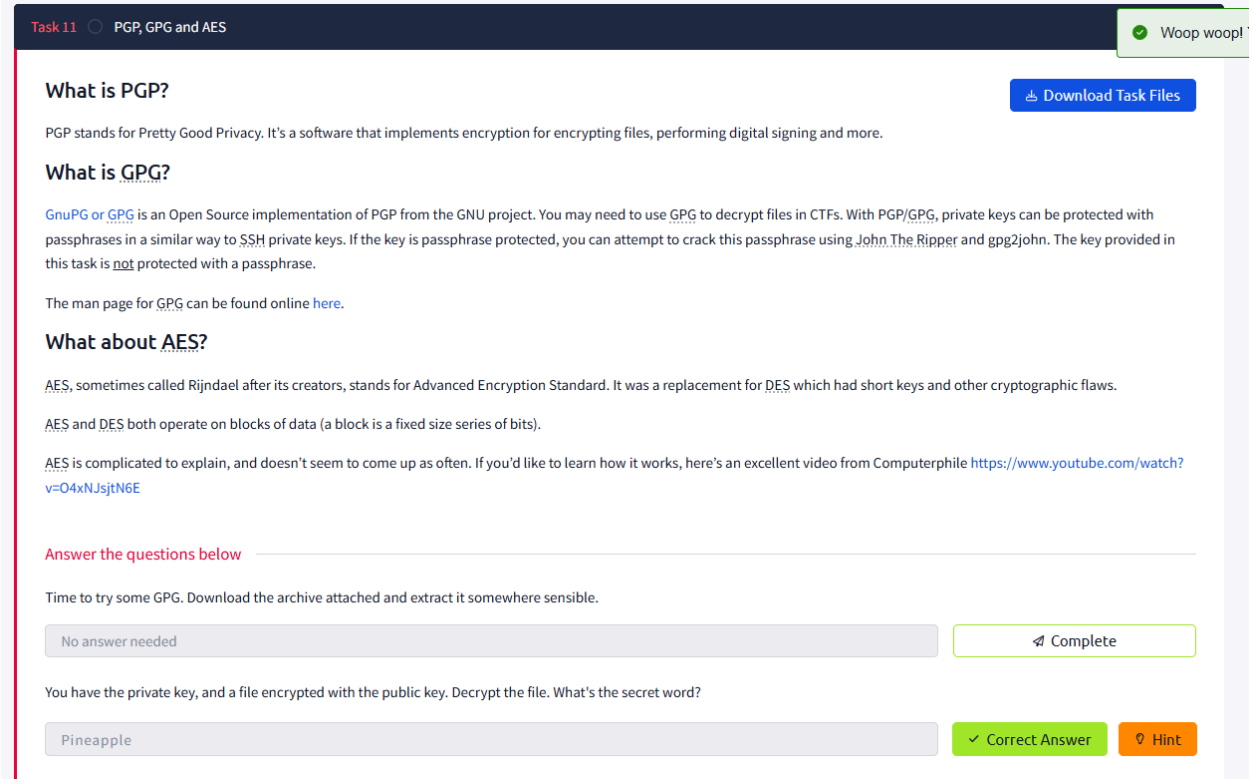
DH Key Exchange is often used alongside RSA public key cryptography, to prove the identity of the person you're talking to with digital signing. This prevents someone from attacking the connection with a man-in-the-middle attack by pretending to be Bob.

Answer the questions below

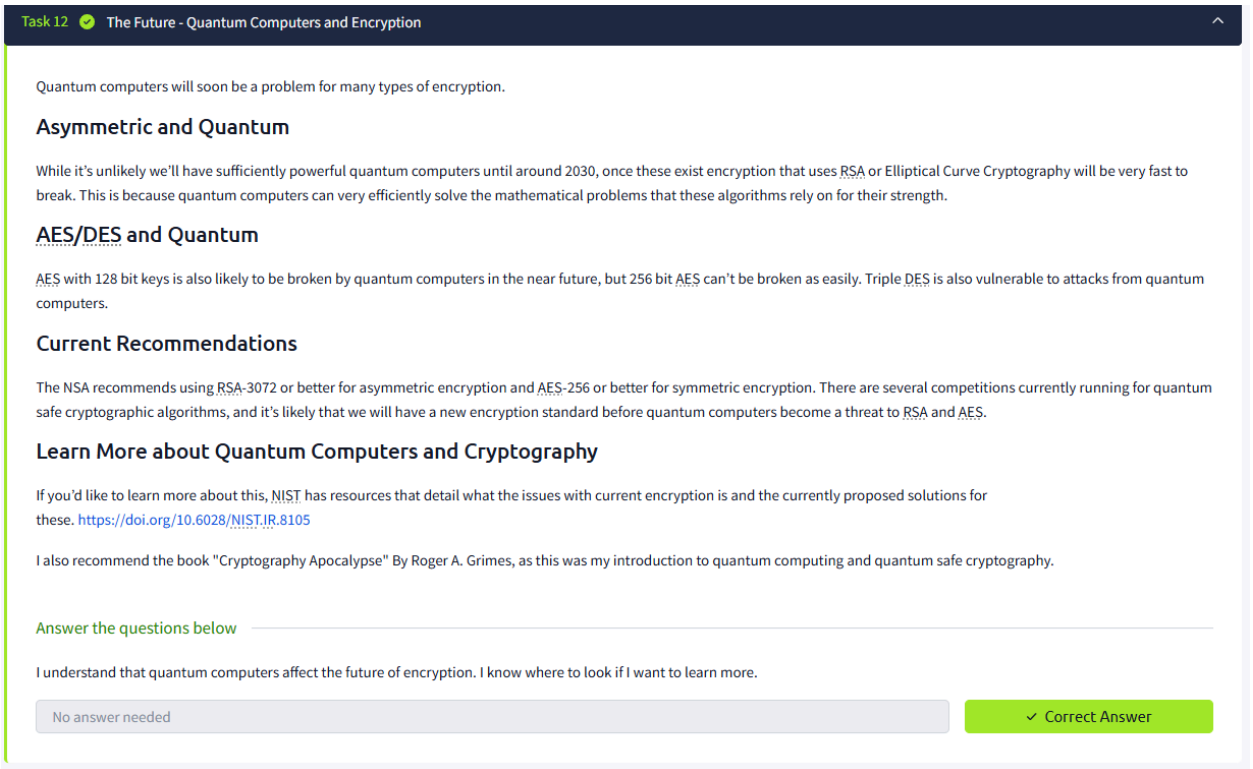
I understand how Diffie Hellman Key Exchange works at a basic level

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.

Ex. No.: 5

Encryption - Crypto 101

Aim:

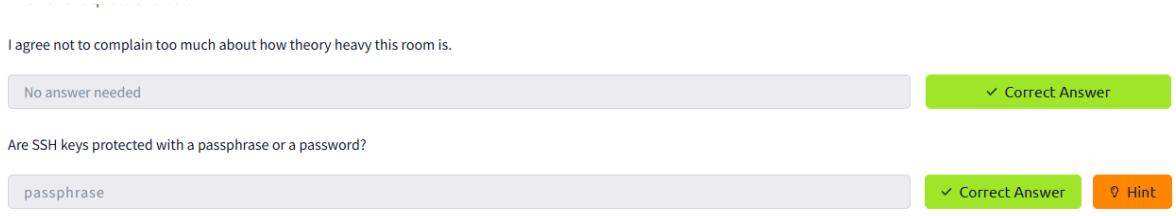
To provide an introduction to encryption, as part of a series on crypto

Algorithm:

1. Go to Encryption Crypto 101 Room, start the AttackBox, and open the in-browser terminal.
2. Learn essential cryptography terms, understand why encryption is important, and explore the math behind cryptography like prime numbers, mod operations, and factorization.
3. Compare symmetric vs asymmetric encryption with examples like AES and RSA.
4. Understand how RSA works, and how asymmetric keys are used for secure communication.
5. Study digital signatures, certificates, and SSH authentication to ensure data integrity and secure login.
6. Explore Diffie-Hellman key exchange, tools like PGP/GPG, and symmetric algorithm AES.
7. Learn how quantum computing could challenge current encryption methods and what post-quantum cryptography means.

Output:

Task 2:Introduction to Windows



Task 3 :Why is Encryption important?

What does SSH stand for?

Secure Shell ✓ Correct Answer

How do webservers prove their identity?

certificates ✓ Correct Answer Hint

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

PCI-DSS ✓ Correct Answer

Task 4:Crucial Crypto Maths

```
>>> 30%5
0
>>> 25%7
4
>>> 118613842%9091
3565
>>>
```

Task 5:Running First few Commands

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 5:Interacting With the Filesystem!

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check y
ction or proxy settings


Last login: Fri Feb 21 06:49:50 2025 from 10.100.2.151
tryhackme@linux1:~$ echo "TryHackMe"
TryHackMe
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$
```

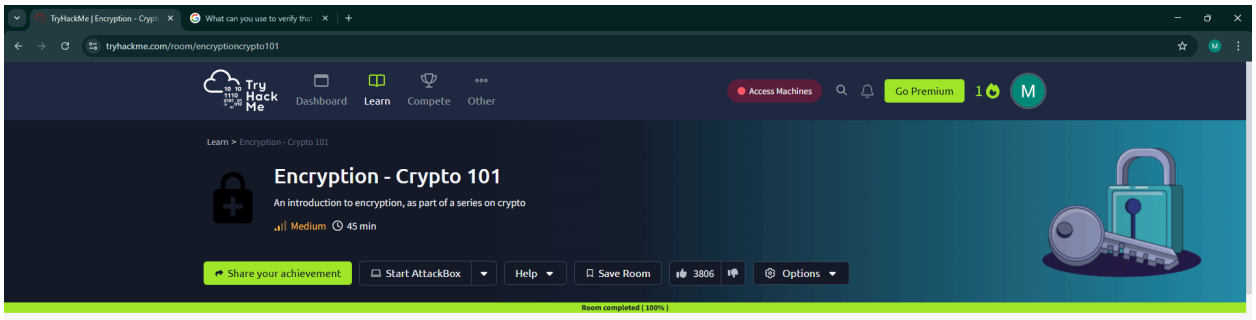
Task 6:

```
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:~$ find -name note.txt
./folder4/note.txt
tryhackme@linux1:~$ wc -l access.log
302 access.log
tryhackme@linux1:~$ grep "81.143.211.90" access.log
tryhackme@linux1:~$
```

Task 7:

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

tryhackme@linux1:~$ find -name note.txt
./folder4/note.txt
tryhackme@linux1:~$ wc -l access.log
302 access.log
tryhackme@linux1:~$ grep "81.143.211.90" access.log
tryhackme@linux1:~$ cd folder4 && note.txt
note.txt: command not found
tryhackme@linux1:~/folder4$ cd folder4 && cat  note.txt
-bash: cd: folder4: No such file or directory
tryhackme@linux1:~/folder4$ cd folder4 && cat note.txt
-bash: cd: folder4: No such file or directory
tryhackme@linux1:~/folder4$ cd folder4 & cat note.txt
[1] 1075
-bash: cd: folder4: No such file or directory
Hello World!
[1]+  Exit 1                  cd folder4
tryhackme@linux1:~/folder4$ echo password123>passwords123
tryhackme@linux1:~/folder4$
```

Task 9:



Description:

Task1:

- Linux device was started and booted.

Task2:

- **Linux** is used in a variety of everyday devices and systems, such as websites, car entertainment/control panels, Point of Sale (PoS) systems, and critical infrastructures like traffic light controllers.
- It's an open-source operating system with many **flavours** or distributions, like **Ubuntu** and **Debian**, each suited for different purposes.

Task3:

- Once deployed, a card will appear at the top of the room containing essential details, such as the **IP address** and the **expiry timer**.
- This card also provides buttons to manage the machine. Make sure to click **"Terminate"** when you're done to safely shut down the machine.

Task4:

- The Terminal in Linux is a text-based interface for interacting with the system. Basic commands like echo (to output text) and whoami (to display the current user) are essential for navigating and managing the system.
- echo - Outputs any text that you provide.
- whoami - Displays the current logged-in user.

Task5:

- To navigate and interact with the filesystem in Linux, use commands like ls (list directory contents), cd (change directory), cat (view file content), and pwd (print the current directory).
- These commands help you move through directories and manage files without a graphical interface. Practice these to become efficient in terminal-based file management.

Task6:

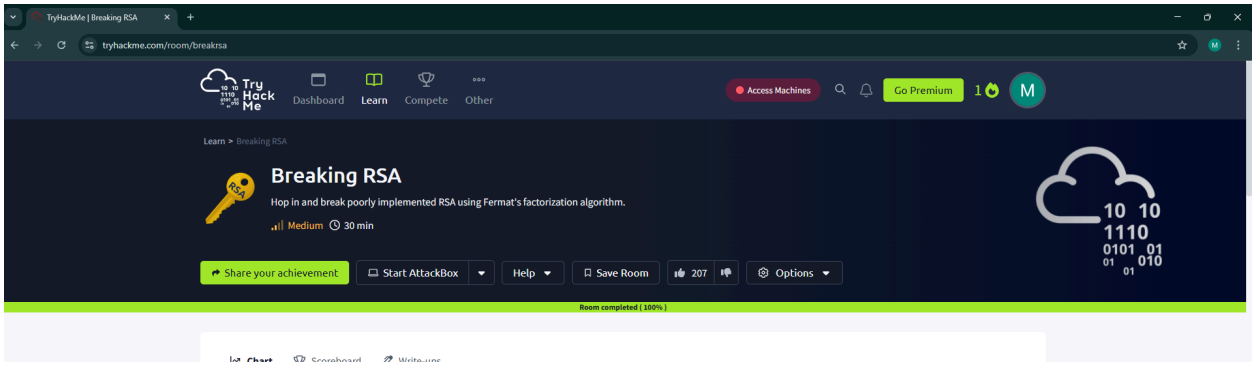
- The find command helps you quickly search for files across your system without needing to manually navigate through directories. For example, you can search for a file by name or use wildcards to find multiple files with specific extensions.
- grep is used to search through the contents of files for specific patterns or values. It's useful when you need to filter through logs or large text files.

Task7:

- Here's a breakdown of some essential Linux operators to help you work more efficiently:
- & - Executes a command in the background, allowing you to continue using the terminal.
- && - Runs multiple commands in a sequence, but the second command runs only if the first is successful.
- >> - Similar to >, but appends the output to the file instead of overwriting it.

Task8:

- Understanding why Linux is used to mastering basic terminal commands like ls, cd, find, and grep. Also learned how to efficiently navigate the filesystem and use powerful operators like &, &&, >, and >>.



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