

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

EXP.NO: 1(a)

DATE: 21-01-2025

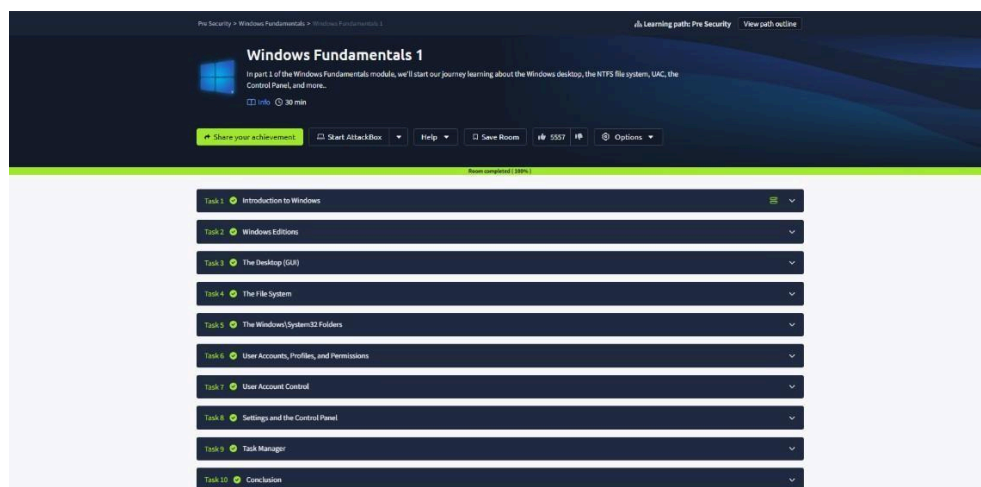
AIM:

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

ALGORITHM:

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

OUTPUT:



Room completed (100%)

Target Machine Information

Title	Target IP Address	Expires
WINFUN1.1	Shown in 0min 44s	58min 42s

Task 1: Introduction to Windows

The Windows operating system (OS) is a complex product with many system files, utilities, settings, features, etc. This module will attempt to provide a general overview of just a handful of what makes up the Windows OS, navigate the user interface, make changes to the system, etc. The content is aimed at those who wish to understand and use the Windows OS on a more comfortable level.

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

Start Machine

The virtual machine should open within your web browser.

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

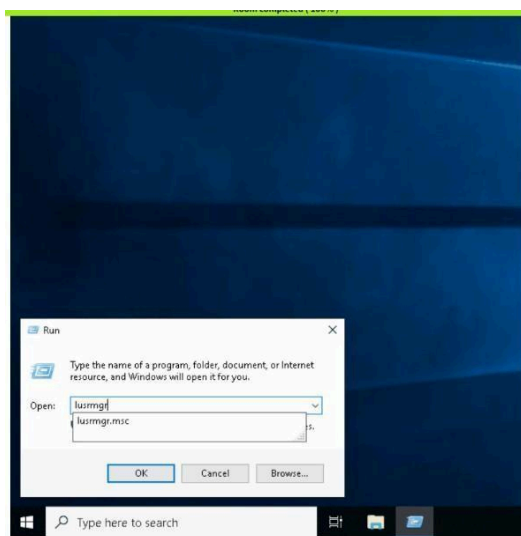
Machine IP: 10.10.10.10
User: administrator
Password: 1qaz!@WSX

Remote Desktop Preference

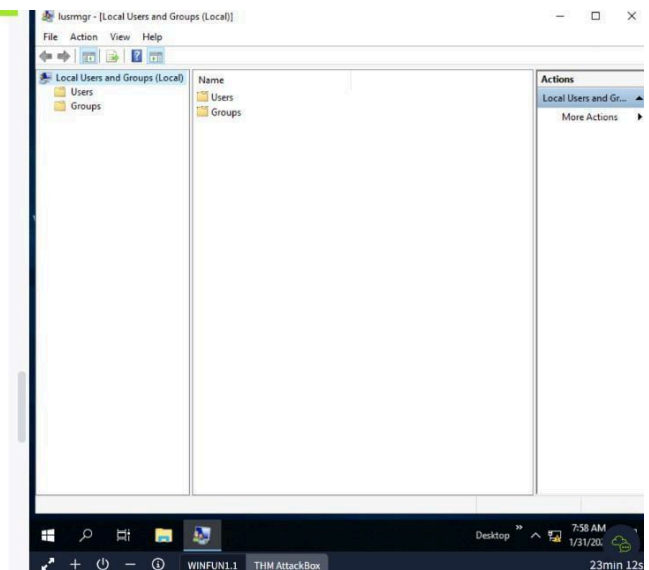
Profile Name: Quick Connect
Group: RDP - Remote Desktop Protocol
Protocol: RDP - Remote Desktop Protocol
File Command: command %h %u %p %q --option
Post Command: /path/to/command -opt1 arg %h %u %p %q --opt2 %u %p %q

Your machine is initializing...
Use the AttackBox to attack machines you start on tasks

Loading (15%)



Note: The Run Dialog Box allows us to run any file.



Room completed (100%)

Task 7: User Account Control

Task 8: Settings and the Control Panel

Task 9: Task Manager

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

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

You can access the Task Manager by right-clicking the taskbar.

Task Manager

✓ Lock the taskbar
⚙ Taskbar settings

Task Manager will open in Simple View and won't show much information.

Task Manager

There are no running apps

Applications Places System Fri 31 Jan, 16:22 AttackBox IP: 10.10.10.212

Terminal

File Edit View Search Terminal Help

01 Contents F1

This machine can access other... play on TryHackMe.

Please keep in mind the following:

1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.
5. If you are a subscriber, this machine is exposed to the internet and maybe automatically scanned. While the machine is secure, do not store sensitive files.

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. READMEs are located in /root/instructions
5. To use Empire & Starkiller, read the following file: /root/instructions/empire-starkiller.txt

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.

WINFUN1.1 THM AttackBox 16min 57s

1. Understanding the Windows Environment

- ☐ Overview of Windows OS versions and architecture.
- ☐ File system structure (C:, Program Files, Users).

2. Command-Line Basics (CMD & PowerShell)

- ☐ Navigating directories (cd, dir).
- ☐ Checking system information (echo %USERNAME%).

3. System Management

- ☐ Using **Task Manager** to monitor and manage running processes.
- ☐ Using tasklist and taskkill to interact with processes via CMD.

4. Windows Registry Introduction

- ☐ Exploring the **Registry Editor (regedit)**.
- ☐ Understanding registry hives like HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER.

5. Basic Networking in Windows

- ☐ Using commands like ipconfig, ping, and netstat to analyze network configurations.

6. User and Permissions Management

- ☐ Viewing current users (whoami, net user).
- ☐ Understanding access control and security policies.

Answer the questions below

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

BitLocker

✓ Correct Answer

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

What is the meaning of NTFS?

New Technology File System

✓ Correct Answer

What is the name of the other user account?

tryhackmebilly

✓ Correct Answer

What groups is this user a member of?

Remote Desktop Users,Users

✓ Correct Answer

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

Guest

✓ Correct Answer

What is the account description?

window\$Fun1!

✓ Correct Answer

What does UAC mean?

User Account Control

✓ Correct Answer

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

What is the keyboard shortcut to open Task Manager?

Ctrl+Shift+Esc

✓ Correct Answer

What is the system variable for the Windows folder?

%windir%

✓ Correct Answer

RESULT:

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