**Aim of the Experiment:**

The **Windows Fundamentals 2** room on TryHackMe focuses on exploring Windows security features, user accounts, groups, permissions, and system logs.

**Algorithm for the Experiment:**

1. **Access the Windows System:**
   - If using a TryHackMe virtual machine, connect via **RDP**.
   - Otherwise, use your local Windows system.
2. **Explore User Accounts & Groups:**
   - Open **Command Prompt** and run:

   Identify user accounts and their roles.

- **Check File & Folder Permissions:**

- Right-click on any file/folder → **Properties** → **Security Tab** → View **permissions**.
- In **cmd**, check file permissions:

**3.Explore Windows Event Viewer:**

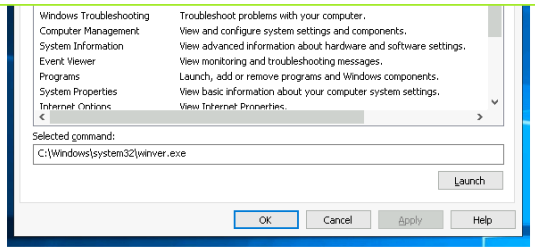
- Open **Event Viewer** (`eventvwr.msc`).
- Navigate to `Windows Logs` → `Security`, `System`, `Application`.
- Use PowerShell to retrieve event logs:

4. **Manage Windows Services:**

- Open **Services** (`services.msc`).
- View running services and their status.
- In **cmd**, check services:

5. **Explore Windows Defender & Security Features:**

- Open **Windows Security** (`windowsdefender://`).
- Check Defender status:




Notice the **Selected command** section. The information in this textbox will change per tool.

To run a tool, we can use the command to launch the tool via the run prompt, command prompt, or by clicking the Launch button.

Answer the questions below

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

PsShutdown ✓ Correct Answer

Whom is the Windows license registered to?

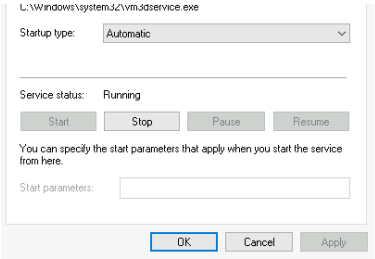
Windows User ✓ Correct Answer

What is the command for Windows Troubleshooting?

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

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

control.exe ✓ Correct Answer




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

```
NET ACCOUNTS            NET HELPMSG             NET STATISTICS
NET COMPUTER            NET LOCALGROUP          NET STOP
NET CONFIG              NET PAUSE               NET TIME
NET CONTINUE            NET SESSION             NET USE
NET FILE                NET SHARE               NET USER
NET GROUP               NET START               NET VIEW
NET HELP

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