Exploring The Lab Environment

(CompTIA Security + SY – 601)

Objectives:

- To understand and navigate the Lab Environment
- To familiarize with a variety of Servers
- To perform Network configurations
- To identify Appliance VMs

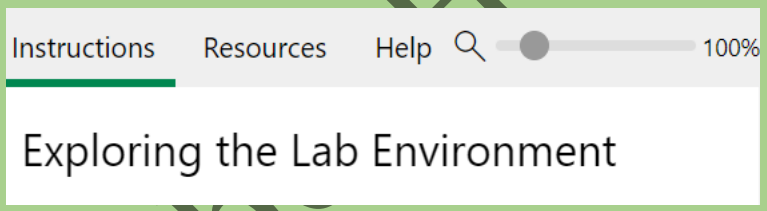
Resources:

- Instructions, Resources and Help Tabs
- Virtual Keyboard
- Virtual Machines
- Network Connection

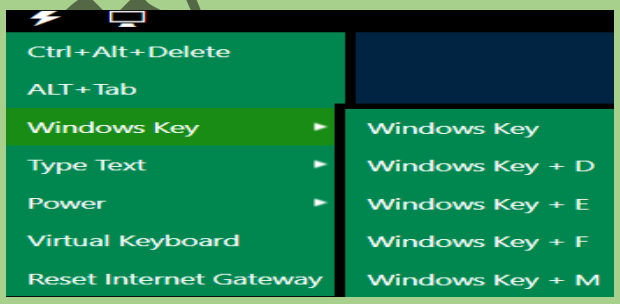
Instructions:

1. Get familiar with the lab environment by navigating through the following:

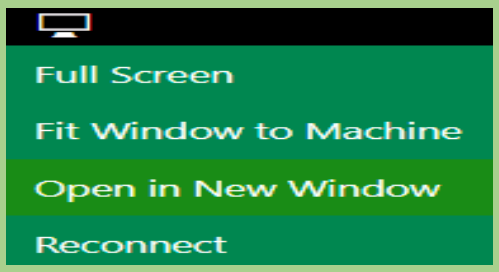
- Instructions
- Resources
- Help



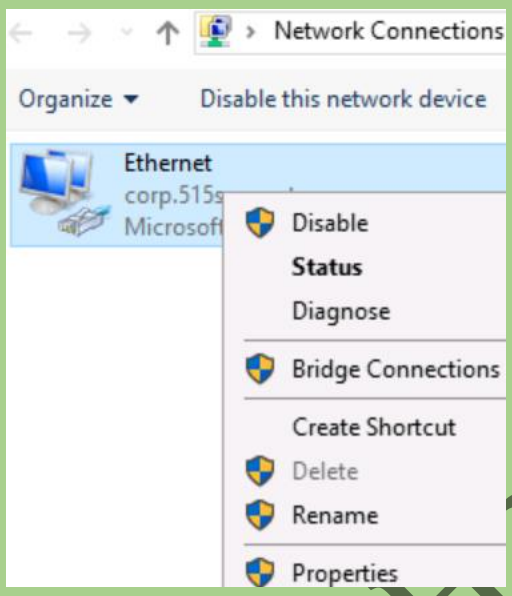
2. Navigate the lab interface via the **Lightning** icon



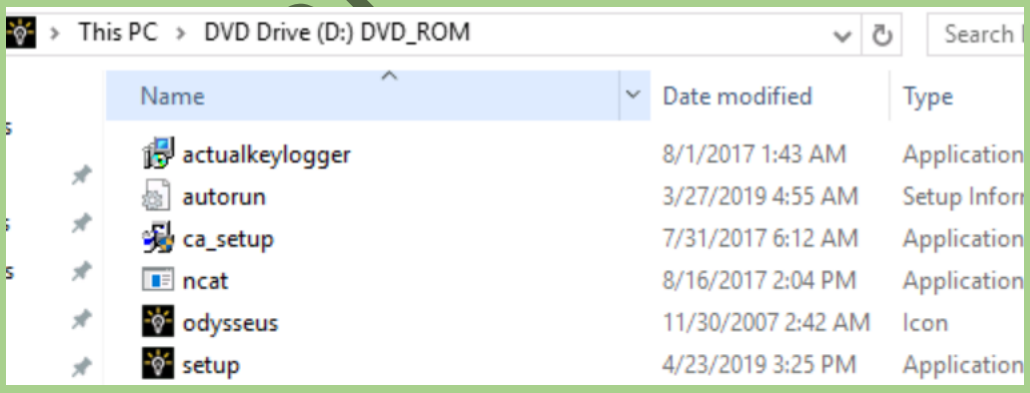
3. Navigate the Lab Interface via the **Display** icon



4. Explore the **Window VM**
5. Configure the network connection



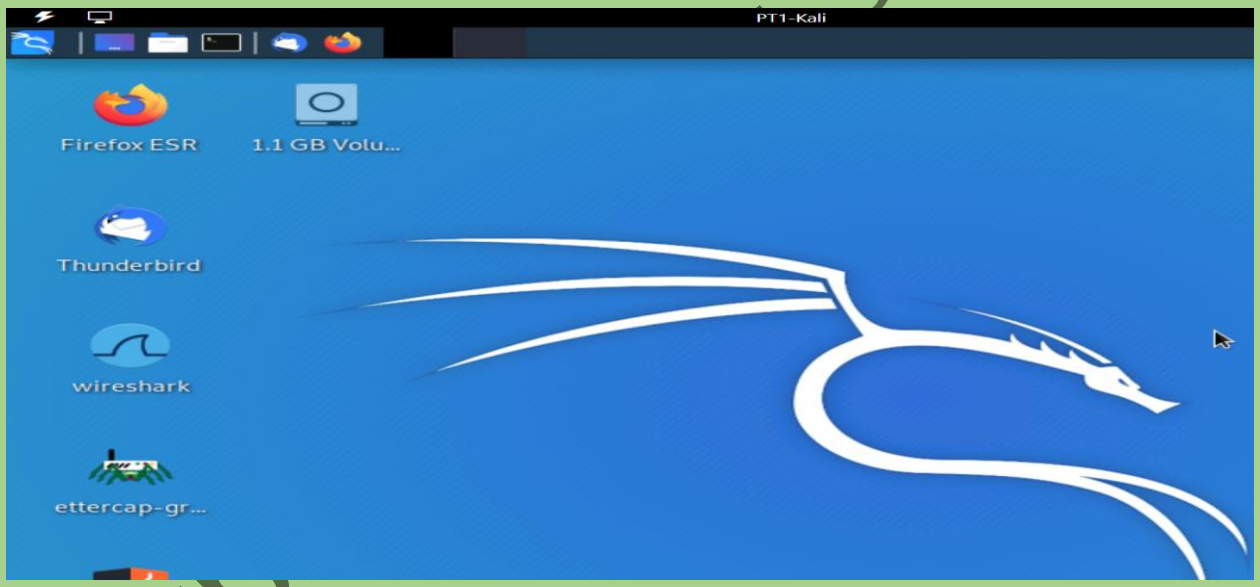
6. Verify the configured network connection
7. Load a DVD 'ODYSSEUS' in **MS1** optical drive



8. Run as an administrator on **Windows Powershell**

9. Explore the **Kali VM**

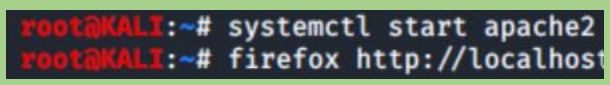
10. Get Familiar with the **Kali VM** desktop icon



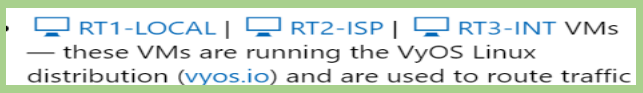
11. Run **ip a command** to check the network adapter connected

12. Start a web server by running the commands:

- service apache2 start
- firefox http://localhost



13. Identify various Appliance VMs



Observations:

1. Different servers were observed under the **Resources** tab
2. Steps for performing the lab activities were accessed via the **Instructions** tab
3. Access to 'Submit a Support Request' was obtained via the **Help** tab
4. The **Lightning** icon gave access to the Virtual keyboard
5. The **Display** icon gave versatile options:
6. The Windows **VM** gave access to **DC1** and **MS1**
7. The Network Connections Console gave access to the **Ethernet** adapter
8. The contents of the **'ODYSSEUS'** DVD were observed in File Explorer
9. An elevator Powershell prompt was opened via the **Windows Powershell**
10. The **Kali VM** was accessed by typing in a Username and Password
11. The **Kali VM** desktop contained the following icons: Firefox, Wireshark, Ettercap, Burpsuite, Network
12. The IP was observed by running the **ip a command**
13. The following **Appliance VMs** were observed:
14. The **ipconfig command** discovered Ip addresses that were stored in **ipconfig.txt** file in the desktop

Results:

- The lab environment was conveniently navigated via the **Resources**, **Instructions** and **Help** tabs
- A variety of servers allowed easy manoeuvering across **Virtual Machines** VMs
- Virtual Machines allowed utilization of security and **command line tools**
- Network connections were configured to allow proper functioning of the **Virtual Machines**
- A variety of **Appliance VMs** were identified within the VMs

Conclusion:

The lab environment is key in providing Virtual Machines VMs that allow offering of Cyber Security practical drills in a convenient environment for beginners who want to interact with command line tools

Future Work:

The Lab environment can be use to create Cyber Security practical-based training.