# Introduction

The network is arguably the most sought-after attack surface. For network administrators, nightmares involve hackers penetrating their network defenses and stealing valuable information from the organization. For hackers and penetration testers they dream of being able to enumerate all the weak points or dream up scenarios to gain a foothold and eventually escalate privileges. For the hacker the final pot of gold is exfiltration of data and for the pen tester to provide their clients a valuable report on what weak points to secure.

As a cyber-security analyst your task is to gain and understanding of how all of this is possible and eventually build the tools or leverage tools to provide insight into these problems.

**Problem Number 1:**

As a cyber-security analyst your task is to gain and understanding of how all of this is possible and eventually build the tools or leverage tools to provide insight into these problems.

# Setup

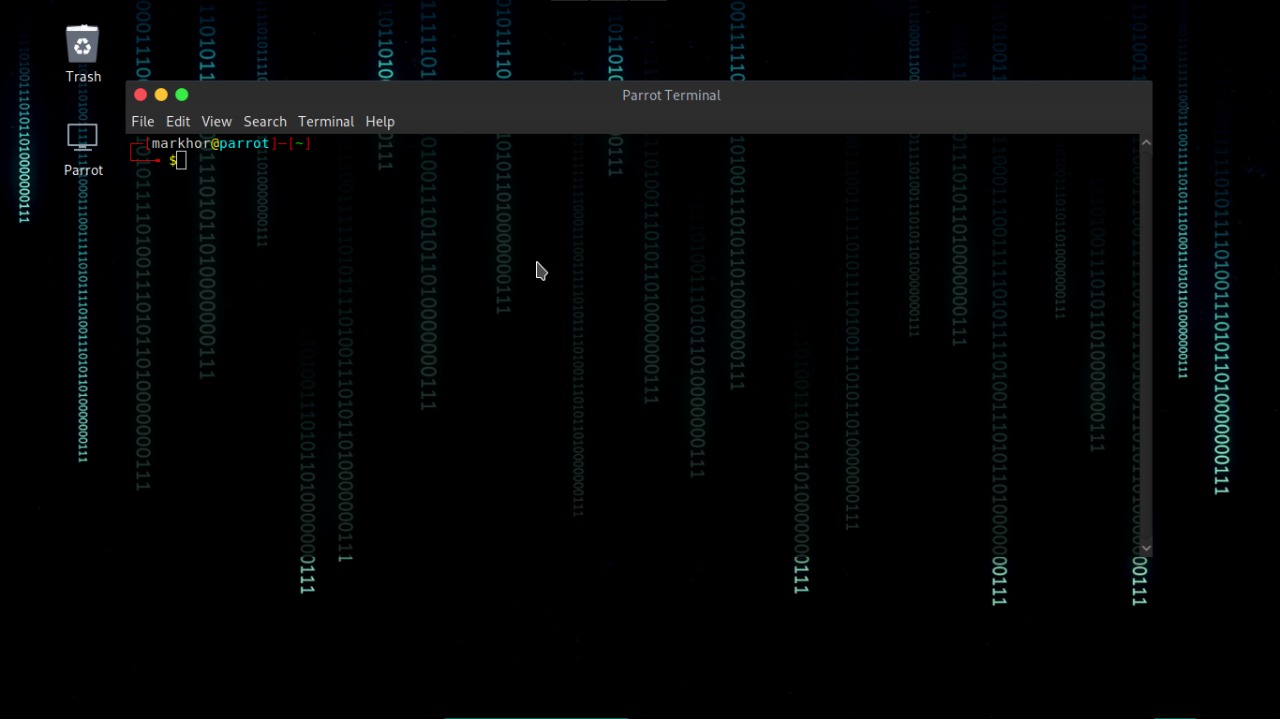
1. You will need a Linux VM (create a new one or use an existing one).
   1. **SNAPSHOT (and|or) CLONE THE VM, in case you need to recover the VM.**

**Ans:**

I have already installed Parrot OS. So there is no need of Virtual Machine.

**Screenshot:**

Here is screenshot of Parrot OS:

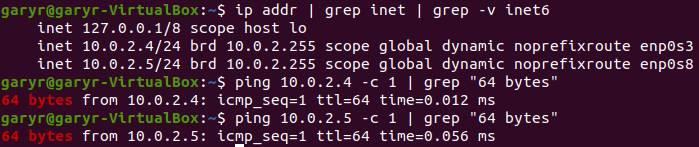
****

1. Before booting up the VM a few adjustments need to be made
   1. If using VirtualBox:

**File** > **Preferences** > **Network**

Add a new NatNetwork

* 1. Select the VM, open the settings for your VM
  2. Under Network Enable “**Adapter 2**”
  3. Click OK
  4. Confirm that both Networks are available and that you can ping the IP addresses associated with those interfaces.

See below for an example:

**Ans:**

Parrot OS is installed, so there is no need of Virtual Machine.

1. Copy the file **Portcreator2021**, provided on D2L, to your VM and execute it from the command line.

**CTRL+C terminates the application**.

**Ans:**

This file is not provided.

**Question Number 1**

**Part 1**

Name three purposes of the netcat tool?

**Ans:**

* Netcat is used for reading from and writing to network connections using TCP or UDP.
* It is to manage networks and monitor the flow of traffic data between systems.
* It is used for network scanning

**Part 2:**

Python provides a simple http(s) module, what is the name of the module?

**Ans:**

Python uses requests module for http and http(s).

**Part 3:**

Show images the module running using port 8989 and 80.

**Ans:**

Modules running on port 80 and 8989 is Requests. Here is an example of it:

