# Problem 2 (15)

Nmap is a powerful port scanner that allows Gray, Black and White hat hackers to enumerate the network interfaces of a system. The hope is to determine if there are soft targets as well as if open ports that should be closed are available on the system.

In this section you will build a port scanner in Python. Your job will be to enumerate all available ports on your system.

1. Run the Tool downloaded from D2L (ie **./Portcreator2021**)
   1. The Portcreator2021 is simple tool that generates open ports on your network interfaces

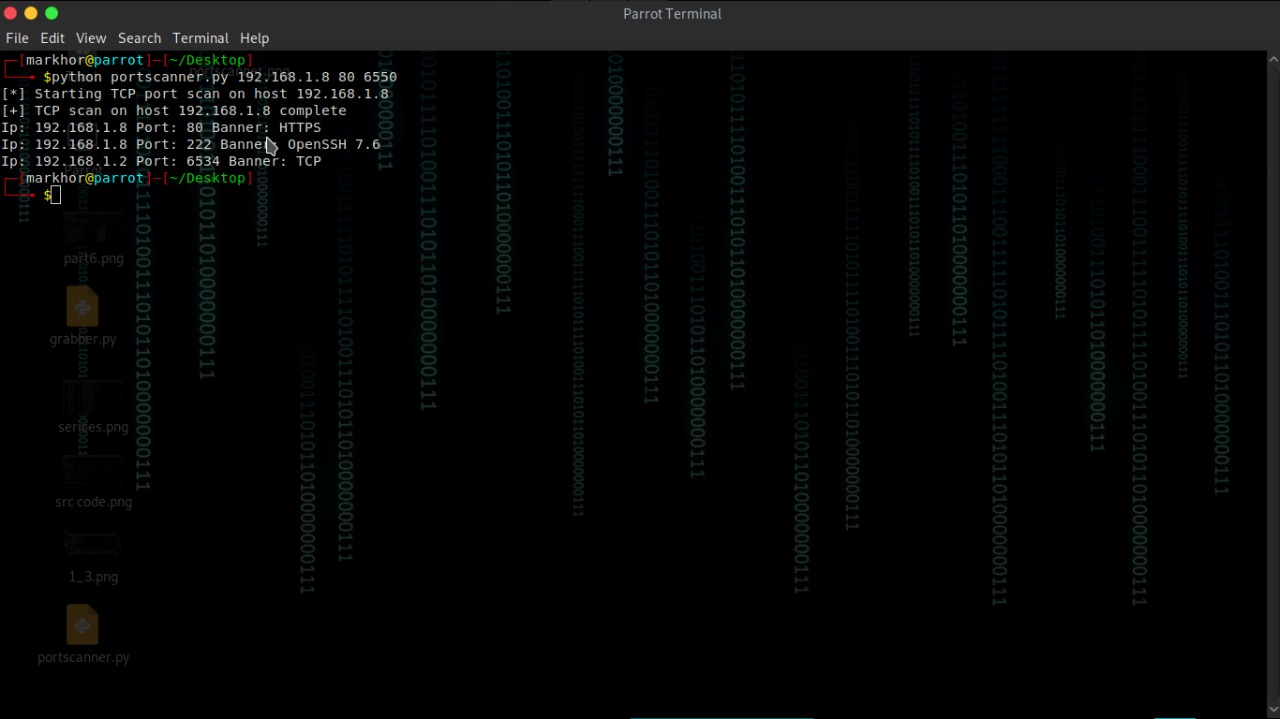
**Ans:**

This tool is not provided.

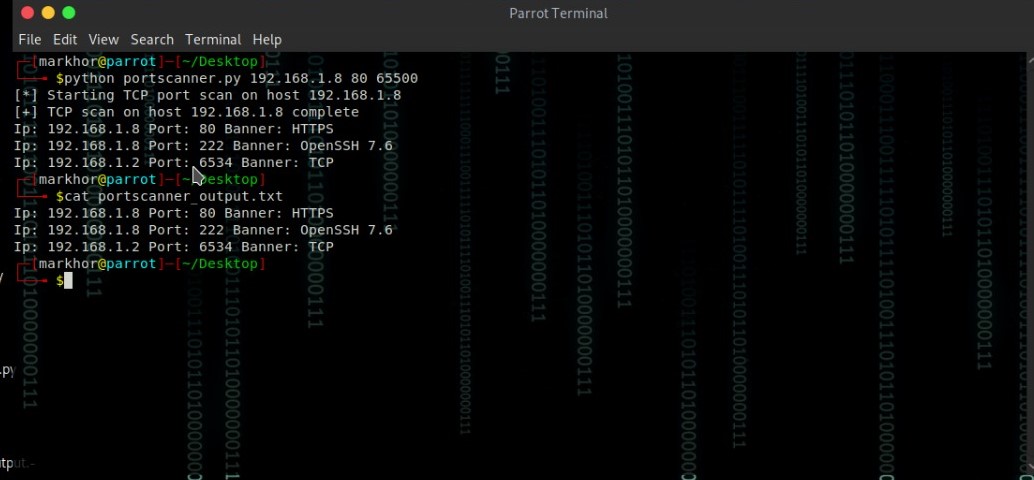
1. Provide screen shots showing the output of the port scanner. Only show the open ports?
   1. Generate a file with all the open ports on your 2 IP interfaces ONLY.

**Ans:**

Following is the screenshot of Open Ports captured by port scanner.



**Port Scanner and its output:**

****

**Question 2:**

**Answers the following Questions!**

**Part 1.**

How many possible TCP ports can there be on a system?

**Ans:**

There are TCP 65,535 ports available on a system.

**Part 2.**

Can a regular user generate ports below 1024?

**Ans:**

No regular user cannot generates ports below 1024 because it will cause server error.

**Part 3.**

Do open ports automatically mean that there is a vulnerability?

**Ans:**

Having an **open port** does not mean a **vulnerability**, although **vulnerability** management and strong credentials are necessary to prevent attacks.

**Part 4.**

What determines whether a port is vulnerable?

**Ans:**

An outdated and insecure **protocol**, which utilize no encryption for both data transfer and authentication.

**Part 5.**

Name at least two services (on Windows/Linux) that you should shut down if you find that service running.

**Ans:**

SSH and HTTP services should be closed. These are the services that are not secure.