Question 1: How could nmap work?

The tool nmap is a network exploration tool. It helps map out the computers and services that are available on a network. It can help detect operating systems and versions, and is scriptable for performing enhanced features.

How do you think nmap works? That is, how would you implement such a tool?

Question 2: How does nmap scan ports?

Test out the tool and look at the resulting pcap file to see how it works in practice. To do this, launch the tinycore VM with a pcap file specified, and inside the VM first install nmap:

```
tce-load -wi nmap
```

and then run it:

```
nmap -A -vv scanme.nmap.org
```

This runs nmap with operating system detection and verbose output for the domain scanme.nmap.org.

The choice of scanme.nmap.org is very important. Using nmap to scan a machine that you do not own or do not have express written permission to scan is considered an intrusive attack. It is imperative that you do not scan any machine other than the ones that you physically own or have express permission. The scanme.nmap.org is one such domain that is free to be scanned by anyone.

Look at the resulting pcap file and relate it to your hypothesis in Question 1.

Question 3: Why does it work a particular way?

Use the manual page for nmap to understand what the -r options does. Use that option in another scan and look at the resulting traffic, observing the resulting traffic. Come up with reasons why nmap would be default work the way it does?

Question 4: How does nmap detect running services?

Analyze the collected pcap file from Question 2 or 3, How did nmap interact with the server, that is, what messages were sent, and what messages did the server respond to nmap for the running services?

Question 5: UDP Scan

The tool can also scan a host for responses it gets on UDP ports. This is done with the -sU option. Do a UDP scan for scanme.nmap.org. This takes a long time, so retrict to a smaller set of ports, such as 1-100, with -p1-100. Look at which ports are running services and what they are. Note that this requires super user privileges, so run it with the sudo command.