1 Assume that an organisation X has hired you for the task of Ethical Hacking. The organisation wants to know whether the ports ranging from 80- 1000 at IP address 192.168.1.1 is in open/closed/filtered state. How will you complete this task. N

a) nmap -p 80-1000 192.168.1.1

2 Certified Hacker is a professional hacking company and assume you are an employee of it. A target IP address 192.168.1.1 is assigned to identify the IP. protocols supported by the targeted system. How would you identify it

a) nmap -sV 192.168.1.1

3 Using Kali Linux start displaying all the hosts that are up and running, along with their respective MAC Addresses and device information for the IP address 10.0.2.1/24

sudo nmap -sn -PR 10.0.2.1/24

4 Using the Kali Linux tool perform an operation to scan port 80 at IP address 192.168.1.1

sudo nmap -p 80 192.168.1.1

5 Using the Kali Linux tool Perform an operation to scan ports 80, 443 at IP address 192.168.1.1

sudo nmap -p 80,443 192.168.1.1

6 Using the Kali Linux tool Perform Stealth Syn Scan to scan the IP address 10.0.2.1

sudo nmap -sS 10.0.2.1

7 Using the Kali lInux tool Perform perform a stealth scan with version detection along with OS detection to scan the IP address 10.0.2.1

sudo nmap -sS -sV -O 10.0.2.1

8 Determine the operation performed by the command Nmap -p T:80 192.168.1.1

`nmap -p T:80 192.168.1.1`

9 Using the Kali lInux – Nmap tool determine which IP Protocols (TCP, UDP, ICMP, etc.) are supported by target host given by the IP address 192.168.1.1

sudo nmap -sO 192.168.1.1

10 Determine the operation performed by the command Nmap -sU 192.168.1.1

sudo nmap -sO 192.168.1.1

11 In your view is it possible to determine the OS of a target system. If YES, then determine the OPERATING SYSTEM of the target IP address: 192.168.1.1

sudo nmap -O 192.168.1.1

12 Determine the operation performed by the command nmap -p U:53 192.168.1.1

nmap -p U:53 192.168.1.1

13 Determine the operation performed by the command nmap -p U:53,79,113,T:21-25,80,443,8080 192.168.1.1

nmap -p U:53,79,113,T:21-25,80,443,8080 192.168.1.1

14 Write and execute a command in the Kali Linux – Nmap Tool to determine if a host is protected by any Packet Filters or Firewall

nmap -sS -PN <target\_host>

15 The simple default scan above will check the 1000 most well known ports for each IP address. What if you want to scan ALL ports of the IP range under scope.Write a command to perform scanning of all 65535 ports

nmap -p- -T4 <target\_IP\_range>

16 Determine the operation performed by the command nmap 192.168.10.1 192.168.10.111 192.168.10.222

nmap 192.168.10.1 192.168.10.111 192.168.10.222

17 Determine the operation performed by the command nmap 192.168.10.100-230

nmap 192.168.10.100-230

18 Determine the operation performed by the command nmap -p 1-65535 192.168.10.0/24

nmap -p 1-65535 192.168.10.0/24

19 Perform a Horizontal scan for the IP addresses 192.168.10.1 192.168.10.111 192.168.10.222

nmap -sS -p 80,443 192.168.10.1,192.168.10.111,192.168.10.222

20 Determine the operation performed by the command nmap $ nmap router

The command `nmap router` is performing a basic scan on a target host named "router". This will attempt to discover open ports and running services on the host using a default set of options and port ranges.

By default, `nmap` will perform a TCP SYN scan on the 1000 most common TCP ports. If any ports are found to be open, `nmap` will try to determine the service running on that port and display it in the output.

The output of this command will show a list of open ports and services running on the "router" host, along with information about the operating system, if possible. It will also show the status of each port (open, closed, filtered, etc.) and other details such as the version of the service running on that port.

21 Determine the operation performed by the command nmap $ nmap -T4 192.168.1.1.Identify the role of T4 in the command

`nmap -T4 192.168.1.1`

22 Determine the operation performed by the command nmap server1 server2 server2.nixcraft.net.in

`nmap server1 server2 server2.nixcraft.net.in`

23 Execute the following command using the HARBVESTER tool and enlist the information gathered

theHarvester -d www.flipkart.com -b all -l 200

`theHarvester -d www.flipkart.com -b all -l 200`

24 Execute the following command using the HARBVESTER tool and enlist the information gathered

theHarvester -d www.myntra.com -b all -l 150

`theHarvester -d www.myntra.com -b all -l 150`

25 Execute the following command using the HARBVESTER tool and enlist the information gathered

theHarvester -d www.microsoft.com -b all -l 100

"theHarvester -d www.microsoft.com -b all -l 100"

26 Using the Wireshark tool perform data capture operation that was sent in packets

1. Open Wireshark on your computer.

2. Select the network interface you want to capture data on. You can choose your Ethernet or Wi-Fi interface depending on your network configuration.

3. Click the "Capture Options" button (gear icon) in the top-left corner of the Wireshark window.

4. In the "Capture Interfaces" window, select the interface you want to capture data on and click the "Start" button.

5. Wireshark will start capturing packets on the selected interface. You can filter the packets by protocol or other criteria using the filter bar.

6. To stop the packet capture, click the "Stop" button in the top-left corner of the Wireshark window.

27 Using the harvester tool you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers, and SHODAN computer database. From the above listed information that can be gatehered from the tool identify for the following command

theHarvester -d www.saveetha.com -b all -l 300

- Emails related to the domain "saveetha.com"

- Subdomains of "saveetha.com"

- Hosts related to "saveetha.com"

- Employee names associated with "saveetha.com"

- Open ports and banners related to "saveetha.com"

28 Using theHarvester to gather information about the domain "www.saveetha.com", with a limit of 300 results, using all available data sources (the "-b all" flag), and to export the results in two formats: HTML and XML files. The result will be saved in the current working directory and will be named "test".

theHarvester -d www.saveetha.com -b all -l 300 -f test -h test.html -x test.xml

29 Using Kalilinux nmap tool show the information about email account ,usernames, hostnames and subdomains from different public sources in kali linux operating systems

theHarvester -d example.com -l 500 -b all -f filename

30 Using Kalilinux nmap tool to perform various host Discovery scanning using Nmap in Kali Linux operating systems. (i)Only port scan (ii)Only host discover

nmap -p <port(s)> <target>

```

For example, to scan port 80 of the host with IP address 192.168.1.1, use the following command:

```

nmap -p 80 192.168.1.1

```

To perform a host discovery scan using Nmap in Kali Linux, use the following command:

```

nmap -sn <target>

```

For example, to discover hosts on the network with IP address range 192.168.1.1-192.168.1.255, use the following command:

```

nmap -sn 192.168.1.1-255

31 You are a systems administrator for a small business, and your customers are reporting connectivity issues. Your goal is to troubleshoot the problem by executing the traceroute and ifconfig commands in Windows operating systems

The traceroute command is used to trace the path taken by packets across an IP network. It shows the IP addresses of the routers in between the source and destination and the time taken for each hop. To execute the traceroute command in Windows, you can open the Command Prompt and type "tracert <destination IP address>".

The ifconfig command is used to display network interface configuration details such as IP address, netmask, and network interface status. To execute the ifconfig command in Windows, you can open the Command Prompt and type "ipconfig".

32 A network administrator for a company and you have been asked to investigate a possible security breach on the network. Your goal is to use Wireshark to capture and analyze network traffic to identify any suspicious activity. Specifically, you want to examine the packets that use SSDP and look at different header fields and payloads of the concerned packets

1. Start Wireshark and select the network interface to capture traffic on.

2. Start capturing traffic by clicking on the "Capture" menu and selecting "Start".

3. Wait for some traffic to be captured, then filter the captured packets to show only those using the SSDP protocol by typing "ssdp" in the filter field and pressing Enter.

4. Analyze the captured SSDP packets by looking at the different header fields and payloads. Some of the fields to pay attention to include:

- SSDP method (e.g. M-SEARCH, NOTIFY)

- SSDP URI (e.g. /rootdesc.xml)

- Host IP address and port number

- User-Agent header field

- ST header field

5. Look for any anomalies in the SSDP traffic that may indicate a security breach, such as suspicious user agents or ST values.

6. If any suspicious activity is detected, further investigation and remediation steps should be taken.

33 Ram is a network administrator for a large enterprise and he have been experiencing some network performance issues. His goal is to analyze the network packet transmission using a packet analyzer tool to identify the cause of the problem

1. Install Wireshark on his computer.

2. Start a packet capture by selecting the network interface he wants to monitor.

3. Let the capture run for some time to capture enough packets.

4. Stop the capture and use Wireshark's filtering capabilities to focus on the packets he wants to analyze. For example, he can filter by IP address, protocol, port number, etc.

5. Analyze the packet headers and payloads to identify any anomalies or issues. For example, he can look for packet loss, high latency, retransmissions, errors, etc.

6. Use Wireshark's statistics and performance analysis features to get a summary of the network traffic and performance metrics.

7. Based on his analysis, he can take appropriate actions to address the performance issues, such as optimizing network settings, upgrading hardware, or fixing configuration issues.