TASK-3

QUESTION:

Choose 3 Educational domains from different networks.

1.Scan the complete network.

2.Filter the Ip addresses in the n/w which are having the ports 22,80,3306 open.

3.Gather the following details:

* Services.
* Versions.
* Banner Details.
* Operating Systems.

With and without Vpn.

Summary:

This document explains how to use ZENMAP to scan a target network and collect the necessary information.

A graphical user interface (GUI) for the well-known network scanner Nmap is called Zen map. It has a user-friendly interface that makes it simple for users to set up and execute Nmap scans as well as analyse and interpret the results.

Summary of steps:

1. Google dorks are used to find the target educational domains.
2. Ping command can be used to find the IP address of the target domain.
3. NMAP is used to find the number of hosts that are live.
4. NMAP is used to filter the Hosts based on ports and port numbers.
5. Finally, the details are gathered by intense scan in Zen map.

**Domain 1:** [**https://www.lcwu.edu.pk/**](https://www.lcwu.edu.pk/)

College for Women University Lahore

Ip address: 5.9.157.157

Steps:

1. Open Zenmap and type the command:

nmap -p 22,80,3306 5.9.157.1-255

1. Now click on scan.
2. Then Filter the hosts 22,80,3306 using the command in the filter hosts’ tab:

op:22 op:80 op:3306

1. After filtering the hosts, we get 9 Ip addresses containing the open ports 22,80,3306.
2. It gives the following result.

Graphical user interface, text, application, chat or text message, email

Description automatically generated

Now to gather the details of the following Ip addresses we use Intense scan of Zenmap.

1. 5.9.157.24

Open Zenmap and then use intense scan on the domains.

Operating system: AVtech Room Alert 26W environmental monitor

Graphical user interface, text, application

Description automatically generated

2. 5.9.157.107

Operating system: Sony Bravia HX720-series TV

Graphical user interface, text, application

Description automatically generated

3. 5.9.157.110

Operating system: Linux 2.6.32

Graphical user interface, text, application, email

Description automatically generated

4. 5.9.157.119

Operating system: Linux 2.6.32

Graphical user interface, text, application, email

Description automatically generated

1. 5.9.157.169

Operating system: Linux 2.6.32

Graphical user interface, text, application, email

Description automatically generated

1. 5.9.157.182

Operating system: Linux 2.6.32

Graphical user interface, text, application

Description automatically generated

1. 5.9.157.186

Operating system: Linux 2.6.32

Graphical user interface, text, application

Description automatically generated

1. 5.9.157.212

Operating system: Linux 2.6.32

Graphical user interface, text, application

Description automatically generated

1. 5.9.157.218

Operating system: Linux 3.11 - 4.1

Graphical user interface, text, application, email

Description automatically generated

* As we can see the following scans have been performed without VPN.
* When we try to connect to VPN and run the scans, NMAP doesn’t connect and fails to perform the scans on the given target network.
* Graphical user interface, text, application, email

  Description automatically generated

**Domain 2:** [**https://www.buitms.edu.pk/**](https://www.buitms.edu.pk/\)

Balochistan University of Information Technology, Engineering and Management Sciences

Ip address: 121.52.157.122

Command: nmap -p 22,80,3306 121.52.157.1-255

Follow the same steps mentioned above and perform the scans for the remaining domains.

Before filtering Hosts:

Graphical user interface, text, application, email

Description automatically generated

47 hosts are up.

After Filtering Hosts:

Graphical user interface, text, application

Description automatically generated

We are left with one host with all the three ports open.

OS information for the Host:

1. 121.52.157.122

Operating system: Microsoft Windows XP SP3

Graphical user interface, text, application

Description automatically generated

**Domain 3:** [**https://ilmauniversity.edu.pk/**](https://ilmauniversity.edu.pk/)

ILMA UNIVERSITY

Ip address: 154.16.171.172

Command: nmap -p 22,80,3306 154.16.171.1-255

Follow the same steps mentioned above and perform the scans for the remaining domains.

Before filtering Hosts:

Graphical user interface, text, application, email

Description automatically generated

69 hosts are up.

After Filtering Hosts:

Graphical user interface, text, application, email

Description automatically generated

We are left with two host with all the three ports open.

Now to gather the details of the following Ip addresses we use Intense scan of Zenmap.

1. 154.16.171.209

Operating system: Linux 2.6.32

Graphical user interface, text, application

Description automatically generated

1. 154.16.171.253

Operating system: Linux 2.6.32

Graphical user interface, text, application

Description automatically generated

**Conclusion:**

In the above document we have seen how to scan a given network, scan all the open ports in each network, and then how to find out the banner details using the ZENMAP GUI tool.

Zenmap supports advanced features such as scripting, OS detection, service, and application.

version detection, and vulnerability scanning. It can also be used to generate reports and export scan results in various formats.