MIT World Peace University
Cyber Threat Modelling

Assignment 1

Naman Soni Roll No. 06

Contents

1 Aim

To learn how to scan a host using nmap and understand the output.

2 Objective

- To perform network mapping using nmap.
- To learn about the various options available in nmap.
- TO Scan a network using nmap.

3 Theory

3.1 *Network Mapping*

Network mapping is the process of discovering devices and hosts on a computer network, and creating a map of the network topology. This map can include information such as IP addresses, MAC addresses, open ports, and services running on the network. Network mapping is often used for security assessments and troubleshooting network issues.

3.2 *Diffrent tools for Network Mapping*

3.2.1 *Nmap*

Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan. Nmap is available for all major operating systems, including Linux, Windows, and Mac OS.

The Nmap Security Scanner is an open source tool which helps us to find out what ports are open on any given IP address.

3.2.2 *Zenmap*