Task 1: Basic Network Scanning Using Nmap

Name: Alfiya Siddiqui

Internship: Oasis Infobyte (OIBSIP)

Task: Basic Network Scanning with Nmap

Tool Used: Nmap

1. Introduction

Network security is an essential part of modern computing systems. One of the first steps in securing a system is identifying the open ports and services running on it. This task focuses on performing a basic network scan using Nmap to understand how exposed services can be detected and analyzed.

2. Objective

The objective of this task is:

To perform a basic network scan using Nmap

To identify open ports and running services on a system

To analyze the security significance of the identified open ports

3. Tool Description

Nmap (Network Mapper) is an open-source network scanning tool used for network discovery and security auditing. It helps in identifying open ports, running services, and potential vulnerabilities in a networked system.

4. Methodology

The following steps were performed to complete the task:

1. Installed Nmap on the system
2. Opened Command Prompt / Terminal
3. Executed the command nmap localhost
4. Observed the open ports and services
5. Saved the scan results and took screenshots
6. Analyzed the security implications of each open port

5. Scan Command Used

```
nmap localhost
```

Task 1: Basic Network Scanning Using Nmap

6. Findings (Open Ports Identified)

Port Number	Service	Description
135	MS RPC	Used for Windows system communication
445	SMB	File and printer sharing service
902	VMware	Virtual machine communication
912	VMware Auth	VMware authentication service
1521	Oracle DB	Oracle database listener
3306	MySQL	MySQL database service
5500	Oracle EM	Oracle Enterprise Manager
7070	HTTP Alt	Alternate web service port

7. Analysis and Explanation

The scan results indicate that multiple services are running on the system, including database services, virtual machine services, and Windows system services. Open ports provide access points to these services. If such ports are exposed without proper security measures, attackers may exploit them to gain unauthorized access or perform malicious activities.

8. Security Significance

Database ports such as 1521 and 3306 are highly sensitive and must be protected

SMB and RPC services are common attack targets in Windows systems

VMware services indicate active virtual machines

Web service ports can expose applications or admin panels

9. Recommendations

To improve system security, the following measures are recommended:

1. Disable unused services
2. Restrict access to database ports using firewalls
3. Use strong authentication mechanisms
4. Regularly monitor open ports using tools like Nmap
5. Keep all systems and services updated

Task 1: Basic Network Scanning Using Nmap

10. Conclusion

This task demonstrated how Nmap can be used for basic network scanning and security assessment. Identifying open ports helps in understanding potential security risks and taking preventive measures. Nmap is an effective tool for beginners to learn network security fundamentals.