Republic of iraq
Ministry of Higher Education and
Scientific Research
University of Babylon
College of information Technology
Department of Information
Security

Secure Network scanning Using Nmap toolbox in Linux Ubuntu

A research project
submitted to the Council of the Information Security Department/College of Information Technology as part of the requirements for obtaining a bachelor's degree

By
Fouad Riyadh Flayeh Hassan

Supervised By
M.M.Ameer Sameer

January 2024

chapter one

1.1 Introduction

Network security refers to the practice of securing a computer network infrastructure against unauthorized access, misuse, modification, or denial of service. It involves implementing various technologies, processes, and policies to protect the integrity, confidentiality, and availability of data and resources within a network.

Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It's designed to scan networks, identify hosts, services, and open ports, and provide information about the operating systems and software running on those hosts. While Nmap has legitimate uses for network administrators and security professionals, it's also capable of being used maliciously for reconnaissance by attackers.

It is a powerful and versatile tool used to scan networks and discover devices connected to them. It is a free tool and is considered one of the most powerful programs used by hackers, Penetration Testers, and even security experts and network managers. The tool is capable of scanning an entire network domain in addition to its ability to perform Remote OS Fingerprint, that is, determine the operating system that is running on the device remotely.

The tool is available on several operating systems such as (Windows, Linux, Unix), but it is recommended to use Linux or one of the Unix systems.

Programming languages in which it was programmed: C, C++, Python, Lua. The tool works via a command line via the scripts found in this path: /usr/share/nmap/scripts .It allows system administrators and security professionals to analyze networks and identify potential security vulnerabilities. It was developed by Gordon Lyon in 1997 and is currently available as an open source tool.

Source: https://nmap.org

Nmap allows the discovery of hosts, ports, and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines, Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version