MINOR PROJECT

FOOTPRINTING WITH NMAP

HARSHINI RAJYA SHRI.S

INTRODUCTION:

Foot printing is a crucial phase in the process of ethical hacking and penetration testing. It involves gathering information about a target system or network to identify potential vulnerabilities. NMAP (Network Mapper) is a powerful open-source tool widely used for network discovery and security auditing. This report explores the concept of foot printing with a focus on NMAP.

OVERVIEW:

NMAP is a versatile tool that provides a range of features for network reconnaissance. It can be used to discover hosts, services, and open ports on a network. NMAP operates by sending packets to target hosts and analyzing the responses to determine the network's structure and potential vulnerabilities.

NMAP's significance lies in its versatility and comprehensive feature set. As a network reconnaissance tool, NMAP facilitates the identification of hosts, services, and open ports within a network. Its operational methodology revolves around sending packets to target hosts and analyzing responses to unveil the network's structure.

HOST DISCOVERY:

One of NMAP's fundamental functions is identifying live hosts on a network. This is achieved through techniques such as ICMP echo requests, TCP SYN/ACK packets, or other probing mechanisms. The

insights gained from this process are crucial for understanding the scope and composition of a network.

PORT SCANNING:

NMAP excels in port scanning, a process that reveals open ports on target hosts. Various scan types, including TCP SYN scan, UDP scan, or XMAS scan, offer detailed information about the services running on specific ports, aiding in the identification of potential attack vectors.

SERVICE VERSION DETECTION:

By analyzing responses from open ports, NMAP can determine the versions of services running on target hosts. This information is pivotal for identifying known vulnerabilities associated with specific software versions, thereby enhancing the precision of subsequent security assessments.

OS FINGERPRINTING:

NMAP's capability to guess the operating system running on a target machine is a valuable asset. This is accomplished by analyzing characteristics such as TCP/IP stack behavior and responses to specific packets. OS fingerprinting enables the tailoring of subsequent attacks to the target's vulnerabilities.

PORT SCANNING:

Once active hosts are identified, the next step is to scan their ports to find open ports. Open ports can give clues about the services and applications running, which can be targeted for vulnerabilities.

bash

n map -p 1-65535 [target IP]

OPERATING SYSTEM DETECTION:

Nmap can also be used to make an educated guess about the operating system running on a target machine. This is useful for tailoring further attacks to the specifics of the operating system.

bash

n map -O [target IP]

SCRIPT SCANNING:

Nmap's scripting engine (NSE) allows for more advanced discovery and exploitation by using scripts written to automate a wide variety of networking tasks, from vulnerability detection to more sophisticated network attacks.

bash

n map --script=default, vuln [target IP]

CONCLUSION:

Nmap is a versatile tool for foot printing, capable of revealing a wealth of information about a target network that can be used for further penetration testing or for securing a network against potential vulnerabilities. Proper use of Nmap combined with a thorough understanding of network protocols and security can significantly contribute to the security posture of IT environments.

This report has provided a concise overview of foot printing with NMAP, covering key techniques and practical applications. It's important to note that ethical hacking should only be performed with proper authorization to ensure legal and responsible use of these tools.