NMAP Intro

Legend:

Input Command

Output of the previous command

Prerequisites

- Ubuntu 22.04 Server Powered up
- Ubuntu Server on Bridged mode
- From Host OS, ssh to the Ubuntu Server

NMAP Introduction

Nmap, short for "Network Mapper," is a powerful open-source tool used for network exploration and security auditing. It's designed to discover hosts and services on a computer network, thus creating a map of the network and the services running on it. Nmap operates by sending packets to the target network and then analyzing the responses to determine the topology and services available.

Here are some key features and functionalities of Nmap:

Host Discovery: Nmap can discover hosts on a network by sending packets and analyzing responses. It supports various host discovery techniques such as ICMP (Ping), TCP SYN scan, TCP ACK scan, and others.

Port Scanning: Nmap can scan for open ports on target hosts to identify which services are running. It supports different scan types including TCP SYN scan (default), TCP connect scan, UDP scan, and more.

Service Version Detection: Nmap can determine the version of services running on open ports by analyzing the responses received from those services. This helps in identifying specific software and its version, which can be crucial for security auditing and vulnerability assessment.

Operating System Detection: Nmap can often deduce the operating system running on a target host by analyzing subtle differences in network packet responses.

Scripting Engine (NSE): Nmap includes a powerful scripting engine called Nmap Scripting Engine (NSE) that allows users to write and execute custom scripts to automate tasks, perform advanced scanning techniques, and gather additional information from target hosts.

Output Options: Nmap provides various output options including plain text, XML, and grepable formats, which can be useful for logging, further analysis, and integration with other tools.

Flexibility and Customization: Nmap is highly flexible and customizable, allowing users to specify scan options, target ranges, and more, to suit their specific needs and requirements.

Nmap is widely used by network administrators, security professionals, and ethical hackers for network exploration, security assessments, vulnerability scanning, and network inventory management.

However, it's important to note that Nmap can also be used maliciously, so it should only be used on networks and systems where you have proper authorization and permission.

EXERCISE 1 – installing and using NMAP

Task 1 - Installation

sudo apt install nmap -y

Using the Advanced Package Tool install the nmap application.

Task 2 – Basic Single Target Usage

Using the following link:

https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/

Via the CLI in your Ubuntu Server you will be conducting internet scans vs a single host.

Read step by step the above website tutorial and conduct the specific simple scanning listed below via nmap against `scanme.nmap.org`

1. Basic Scan
2. Stealth Scan
3. Version ScanPort Scanning
4. OS Scan
5. Aggressive Scan

Make sure the target of your scans are `scanme.nmap.org`

Task 3 – Discovery Scans

Nmap, the Network Mapper, can conduct discovery scans in a local network using various techniques to identify live hosts, open ports, and services running on those ports.

These scans are essential for network administrators to understand the topology of their network, the hosts on their network, and identify potential security vulnerabilities.

1. ICMP Echo (Ping) Scan:

Nmap sends ICMP echo requests (ping) to the target hosts to check if they are online and responsive.

This scan is performed using the `-sn` or `--ping` option.

Example: `nmap -sn 192.168.1.0/24`

2. TCP SYN Scan:

Nmap sends TCP SYN packets to the target hosts and analyzes their responses to determine if the ports are open, closed, or filtered.

This scan is performed using the `-sS` option.

Example: `nmap -sS 192.168.1.0/24`

3. TCP ACK Scan:

Nmap sends TCP ACK packets to the target hosts to determine if the ports are filtered by firewalls.

This scan is performed using the `-sA` option.

Example: `nmap -sA 192.168.1.0/24`

4. UDP Scan:

Nmap sends UDP packets to the target hosts to identify open UDP ports.

This scan is performed using the `-sU` option.

Example: `nmap -sU 192.168.1.0/24`

5. TCP Connect Scan:

Nmap attempts to establish a full TCP connection with the target hosts to determine if the ports are open.

This scan is performed using the `-sT` option.

Example: `nmap -sT 192.168.1.0/24`

6. ARP Scan:

Nmap uses ARP requests to discover hosts on the local network without sending packets to each individual IP address.

This scan is performed using the `-PR` option.

Example: `nmap -PR 192.168.1.0/24`

7. Host Discovery:

Nmap combines various discovery techniques, such as ARP scanning, ICMP ping, and TCP ping, to identify live hosts in the network.

This scan is performed using the `-sn` or `--ping` option along with other scan types.

Example: `nmap -sn -PS -PA -PU 192.168.1.0/24`

These are just a few examples of how Nmap can conduct discovery scans in a local network. Nmap provides a wide range of options and scan types to meet various network scanning requirements. It's important to use Nmap responsibly and ensure that you have proper authorization before scanning networks.

Conduct a discovery scan of your host network and note the outcome.

Please note that each learner's individual network might be the same or might be different, so providing learners with the input to the nmap command would provide no value.

At this point of your education, by using ipconfig, or ip addr, or ifconfig the learner should be able to combine the ip address of the host computer or virtual machine and the subnet mask to be able to configure the nmap scan correctly.

Why would we run Discovery Scans

The CIS (Center for Internet Security) Control 1, also known as "Inventory and Control of Hardware Assets," is often regarded as one of the most important controls in cybersecurity for several reasons:

Visibility and Awareness: Control 1 emphasizes the importance of knowing what hardware assets are present within an organization's network. Without a comprehensive inventory of hardware assets, it's challenging to understand the attack surface and assess potential risks adequately. By maintaining an inventory, organizations gain visibility into their infrastructure, enabling better decision-making and resource allocation.

Security Hygiene: Control 1 promotes good security hygiene by ensuring that organizations regularly update and maintain an accurate inventory of their hardware assets. This includes not only traditional IT devices such as servers, workstations, and networking equipment but also IoT devices, mobile devices, and any other endpoints connected to the network. By continuously monitoring and updating the inventory, organizations can identify unauthorized devices or deviations from the baseline configuration, which could indicate security incidents or policy violations.

Risk Management: Knowing what hardware assets are present allows organizations to assess and prioritize risks effectively. It enables them to focus resources on securing critical assets and identifying vulnerabilities that could be exploited by attackers. By understanding the scope and nature of their hardware assets, organizations can implement appropriate security controls and mitigation strategies to reduce the likelihood and impact of security incidents.

Compliance and Governance: Control 1 helps organizations meet regulatory requirements and industry standards related to asset management and information security. Many compliance frameworks, such as PCI DSS, HIPAA, and GDPR, require organizations to maintain an inventory of hardware assets as part of their overall security program. By implementing Control 1, organizations can demonstrate compliance with these requirements and strengthen their overall governance posture.

CIS Control #1, "Inventory and Control of Hardware Assets," emphasizes the importance of maintaining an accurate inventory of hardware assets within an organization's network. Nmap discovery scans can play a crucial role in fulfilling this control by providing visibility into the network infrastructure. Here's how Nmap discovery scans work in alignment with CIS Control #1:

Identifying Live Hosts:

Nmap can conduct various discovery scans, such as ICMP (Ping) scans, ARP scans, and TCP SYN scans, to identify live hosts on the network.

By scanning for live hosts, Nmap helps organizations discover all devices connected to their network, including servers, workstations, routers, switches, IoT devices, and more.

This information contributes to building an inventory of hardware assets by listing all active devices present on the network.

Detecting Open Ports:

In addition to identifying live hosts, Nmap can also scan for open ports on these hosts.

By detecting open ports, Nmap provides insights into the services and applications running on each device.

This information helps organizations understand the functionality and purpose of each device, further enriching the inventory of hardware assets.

Mapping Network Topology:

Nmap scans can reveal the network topology by identifying relationships between devices, such as routers, switches, and connected hosts.

Understanding the network topology aids in categorizing and organizing hardware assets based on their roles and dependencies.

It allows organizations to visualize the network layout and identify critical assets and potential points of failure.

Continuous Monitoring:

Nmap scans can be scheduled and automated to run regularly, providing continuous monitoring of the network environment.

By regularly updating the inventory of hardware assets with the results of Nmap scans, organizations ensure that the inventory remains accurate and up-to-date.

Continuous monitoring helps detect unauthorized or rogue devices that may have been added to the network without authorization, enhancing security posture and compliance with CIS Control #1.

In summary, Nmap discovery scans contribute to CIS Control #1 by enabling organizations to identify, categorize, and control hardware assets within their network. By leveraging Nmap's capabilities for network discovery and scanning, organizations can maintain an accurate inventory of hardware assets, which is essential for effective cybersecurity management and compliance with regulatory requirements.