Host and Port Scanning Report

Introduction

Understanding the intricacies of network scanning tools like Nmap is crucial for effective reconnaissance. This report aims to analyze various scanning methods, their significance, and practical examples of host and port scanning using Nmap.

Scanning Objectives

- Discover open ports and associated services
- Identify service versions
- Gather information provided by services
- Determine the operating system of the target

Port States

Nmap provides insights into different states for scanned ports:

State	Description
open	Connection to the scanned port has been established
closed	TCP packet received contains an RST flag, indicating the port is closed
filtered	Nmap cannot determine if the port is open or closed due to no response or error code from the target
unfiltered	Port accessible, but its state (open or closed) cannot be determined
open	filtered
closed	filtered

Discovering Open TCP Ports

Scanning Top 10 TCP Ports

```
sudo nmap <target_ip> --top-ports=10
```

```
PORT     STATE    SERVICE

21/tcp   closed   ftp

22/tcp   open     ssh

23/tcp   closed   telnet

25/tcp   open     smtp

80/tcp   open     http

110/tcp  open     pop3

139/tcp  filtered netbios-ssn

443/tcp  closed   https

445/tcp  filtered microsoft-ds

3389/tcp closed   ms-wbt-server
```

Trace the Packets

```
sudo nmap <target_ip> -p 21 --packet-trace -Pn -n --disable-arp-ping
```

Connect Scan

Nmap TCP Connect Scan (-sT) uses the TCP three-way handshake to determine port state.

Example: Connect Scan on TCP Port 443

```
sudo nmap <target_ip> -p 443 --packet-trace --disable-arp-ping -Pn
-n --reason -sT
```

Filtered Ports

Filtered ports indicate firewall rules handling specific connections.

Example: Port 139 (Filtered)

```
sudo nmap <target_ip> -p 139 --packet-trace -n --disable-arp-ping
-Pn
```

Discovering Open UDP Ports

UDP Port Scan

```
sudo nmap <target_ip> -F -sU
```

Example: UDP Port 137 (Open)

```
sudo nmap <target_ip> -sU -Pn -n --disable-arp-ping --packet-trace
-p 137 --reason
```

Example: UDP Port 100 (Closed)

```
sudo nmap <target_ip> -sU -Pn -n --disable-arp-ping --packet-trace
-p 100 --reason
```

Version Scan

The -sV option provides additional information from open ports.

Example: Version Scan on Port 445

```
sudo nmap <target_ip> -Pn -n --disable-arp-ping --packet-trace -p
445 --reason -sV
```