NCS-CYBERSECURITY FORUM & WORKSHOP June-2025

Ageebee Silas Faki PhD,

Department of Cybersecurity

Baze University, Abuja

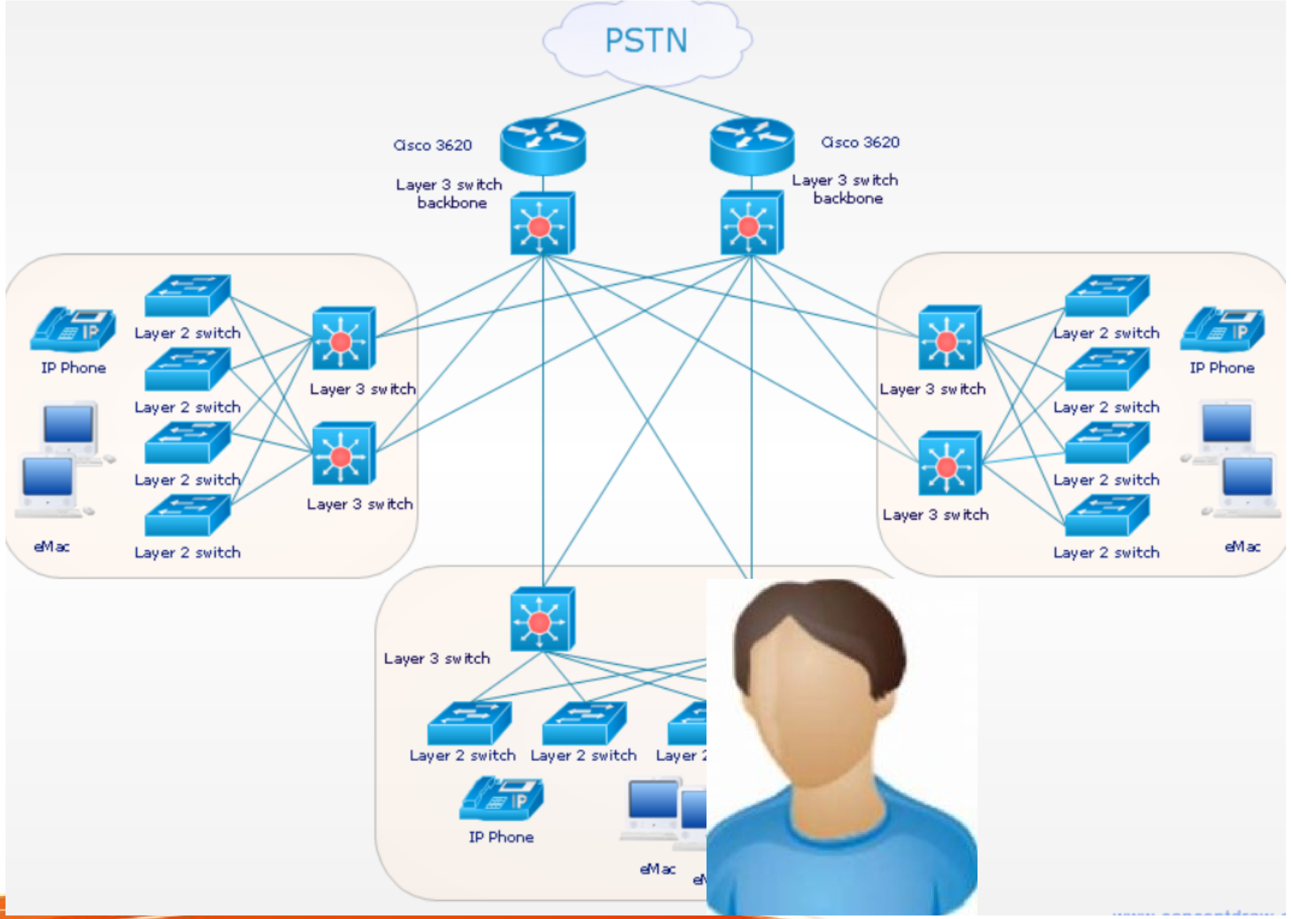
Practical Intelligence Gathering and Surveillance Using ZENMAP (NMAP)

A Comprehensive Guide to Network Reconnaissance

A Network

Security Elements
(Asset)

Hardware
Software
Users



Introduction

- **What is ZENMAP?**
  - – The official GUI for Nmap (Network Mapper), a powerful open-source network scanner
  - – Designed for beginners (GUI-based) and experts (advanced profiling).

- **Why Use ZENMAP?**
  - – Simplifies complex Nmap commands.
  - – Provides visual network topology and scan comparisons.
  - – Saves scans in searchable databases

Key Features of Zenmap

- **Profile-Based Scanning** – Predefined scan types (Quick, Intense, Full).
- **Interactive Network Mapping** – Visualizes host connections.
- **Scan Comparison** – Detects changes between scans.
- **Command Builder** – Helps generate Nmap commands.
- **Database Storage** – Saves results in XML or text formats

Installation and Setup

- Download & Install:
  - Available for Windows, macOS, Linux from **nmap.org**

- Pre-installed in Kali Linux (**under Information Gathering**).

- Alternative Install Methods:
  - **Linux: sudo apt-get install zenmap**
  - **Windows: Download .exe installer**

Zenmap (Nmap) scanning syntax

nmap <scan_type> <options> <target>

- *Scant_type are the switches*
- *Options may be port, or you want output or etc*
- ***Example***
- *nmap –sS –P 22 192.168.1.0*

Port

- A Port is a logical address of a 16-bit unsigned integer that is allotted to every application on the computer that uses the internet to send or receive data.

- **Types of Port**
- Ports are further divided into three categories:
  - Well Known Port
  - Registered port
  - Dynamic Port

1. Well Known Port

- It is from the range 0 to 1023
- It is reserved for common and specifically used service
- It is used by some widely adopted protocols and services like HTTP (port 80), FTP(port 21), DNS(Port 53), SSH(port 22), etc…..

2.Registered Port

- It is from range 1024 to 49151
- These are used by applications or services that are not as common
- But it is used by those applications or services which require its specific port
- Organizations can ask IANA(Internet Assigned Number Authority) for any specific port number within this range

3. Dynamic Port

- It is from range 49152 to 65535
- It is also known as Ephemeral or Private Port
- It is used for those connections that are temporary or short-lived
- It is not registered or assigned and can be used by any process

Importance of Port Numbers

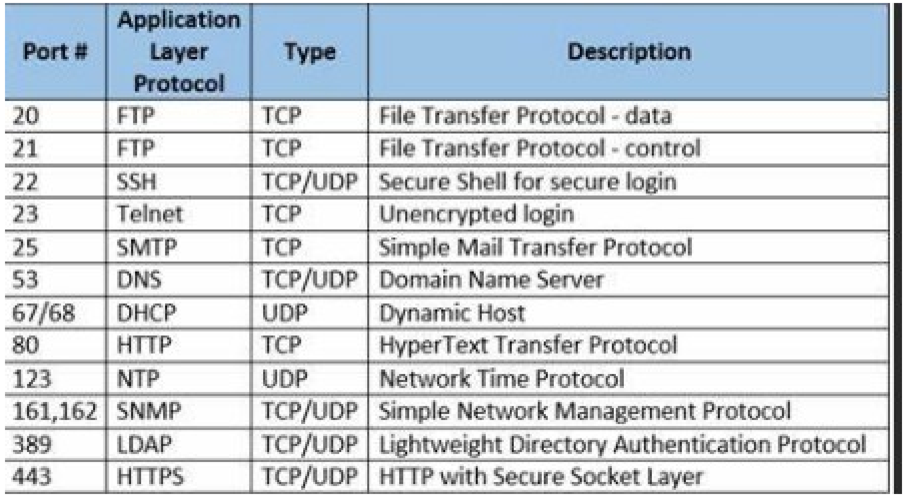
- **Identification of service-** Different application/services that work on the same device can be differentiated by their port numbers.
  - For example, HTTP (Port number 80) and SMTP(port number 25) in the same computer uses different port number to ensure their data goes to the correct service
  - **Efficient Data Routing-** When a network device receives data from different places it uses port numbers to efficiently route those data packets to the respective application

- **Block traffic from specific applications/services-** When we have to block incoming or outgoing traffic from a specific application/service then we need to install a firewall and specify the port number of that application/service. We block traffic from/to some specific applications/services when we find any potential threats from those applications/services

- **Scalability of services-** Many services can run simultaneously on the same device and can be differentiated using their port number. This helps the device to scale and support many services at the same time.

Common Port

Some port are secures and some are highly insecure.
It is nice to understand what service run on which port



Port #	Application Layer Protocol	Type	Description
20	FTP	TCP	File Transfer Protocol - data
21	FTP	TCP	File Transfer Protocol - control
22	SSH	TCP/UDP	Secure Shell for secure login
23	Telnet	TCP	Unencrypted login
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP/UDP	Domain Name Server
67/68	DHCP	UDP	Dynamic Host
80	HTTP	TCP	HyperText Transfer Protocol
123	NTP	UDP	Network Time Protocol
161,162	SNMP	TCP/UDP	Simple Network Management Protocol
389	LDAP	TCP/UDP	Lightweight Directory Authentication Protocol
443	HTTPS	TCP/UDP	HTTP with Secure Socket Layer

nmap at a glance

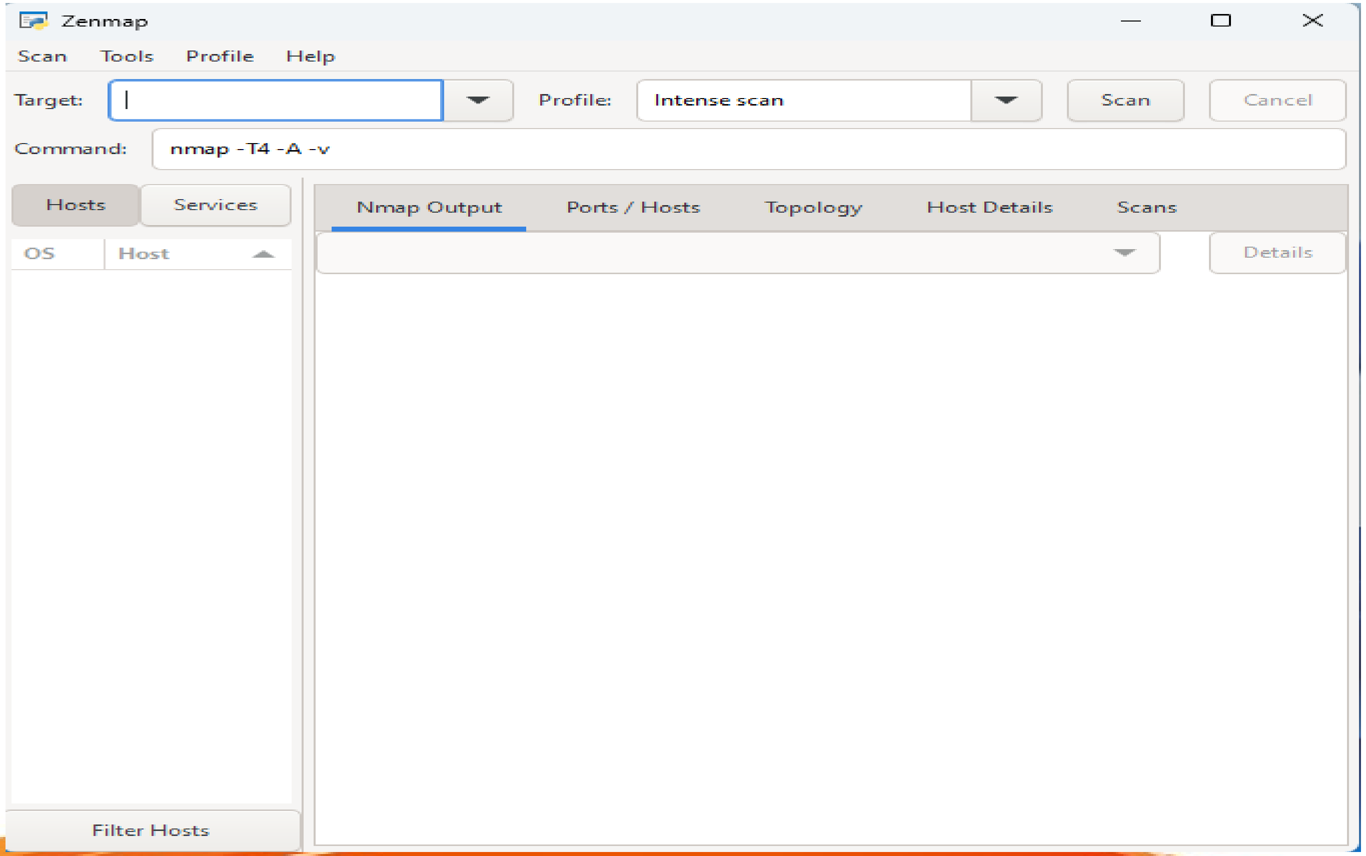
- IP/Host/Port Scanning
- Service Discovery
- OS detection
- Version detection
- Scriptable Interaction with Target (NSE)
- Information on target including reverse DNS names. Device types, MAC addresses

Who uses nmap

- ✓ Penetration Testers/Ethical hackers use it for information gathering
- ✓ IT personal use it for inventory
- ✓ Cybercriminals use it for post intrusion activities

Reconnaissance using nmap (Zenmap)

- Download and install nmap for windows (or any other distribution)

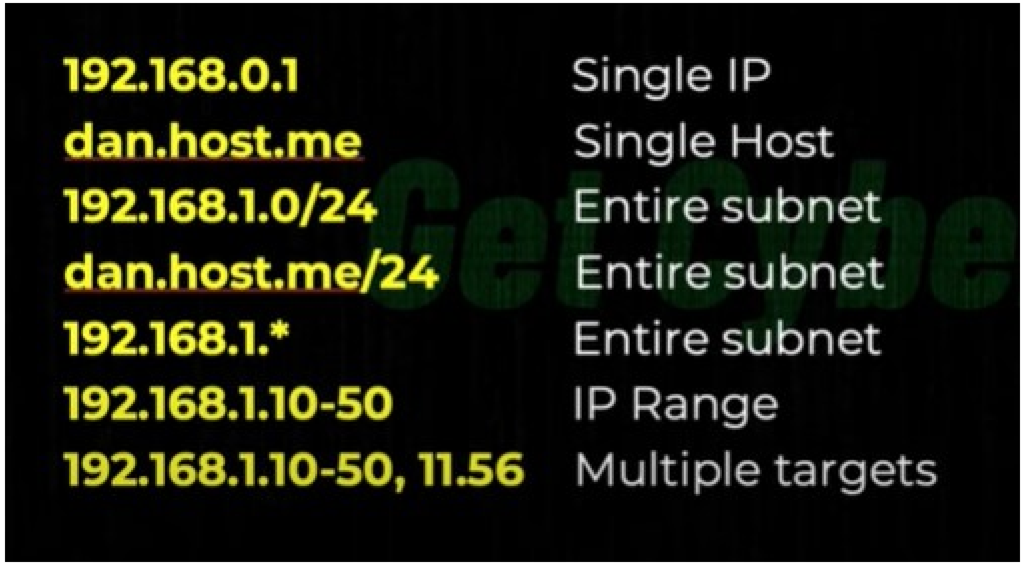


Target:

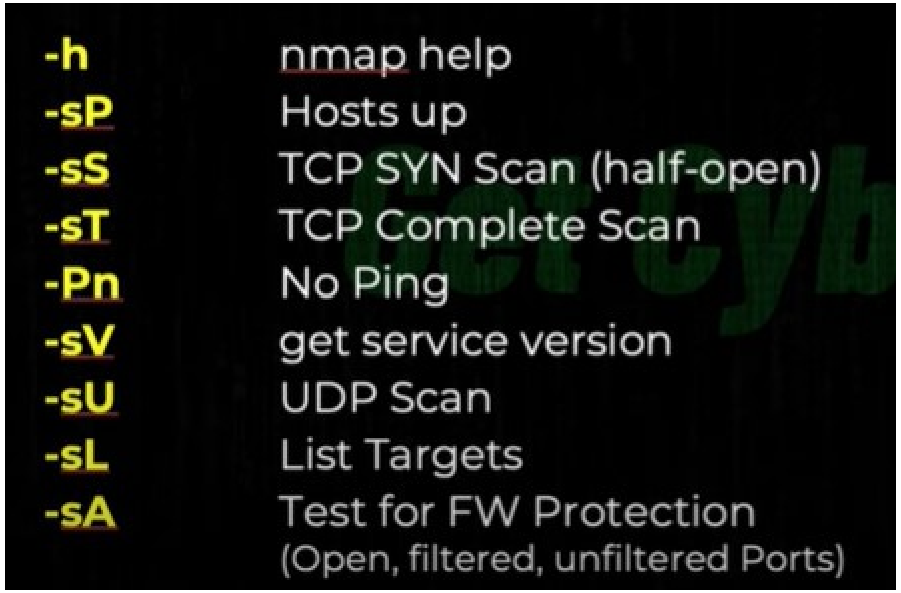
Profile: Intense scan

Command: nmap -T4 -A -v

Target Options and Basic Scan Options

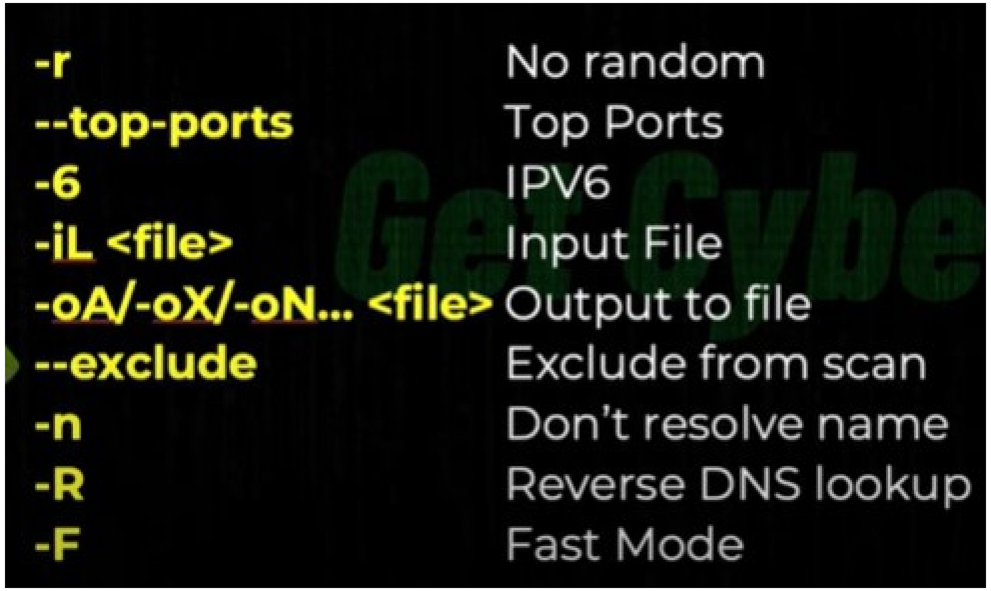


192.168.0.1	Single IP
dan.host.me	Single Host
192.168.1.0/24	Entire subnet
dan.host.me/24	Entire subnet
192.168.1.*	Entire subnet
192.168.1.10-50	IP Range
192.168.1.10-50, 11.56	Multiple targets

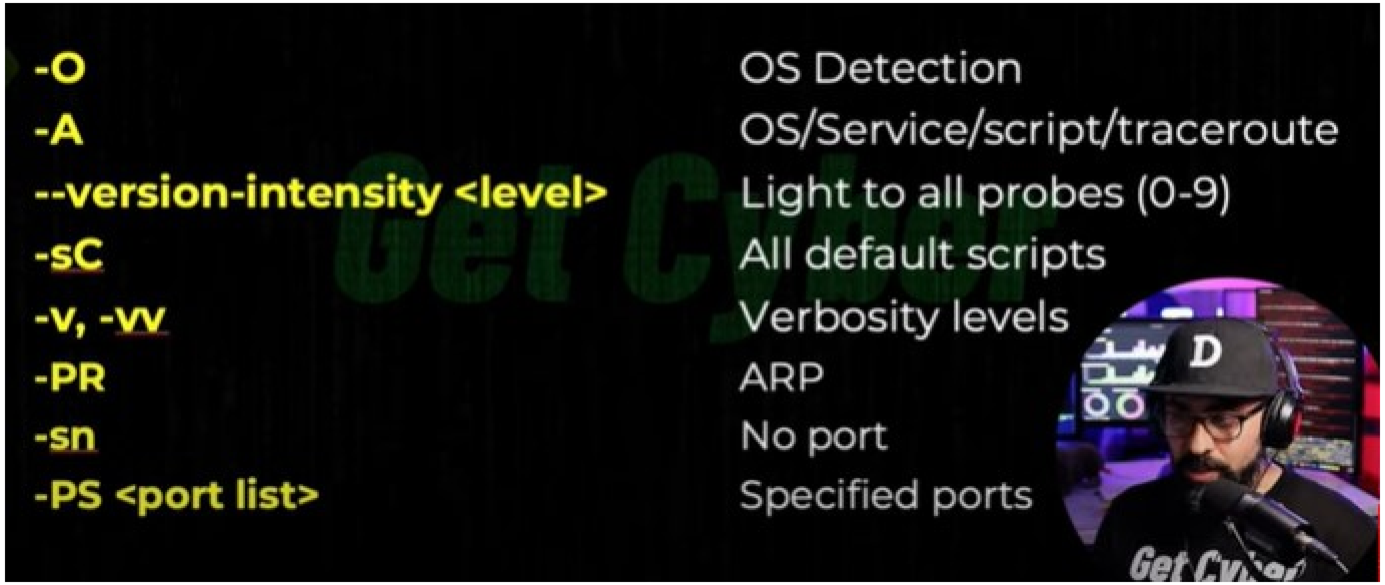


-h	nmap help
-sP	Hosts up
-sS	TCP SYN Scan (half-open)
-sT	TCP Complete Scan
-Pn	No Ping
-sV	get service version
-sU	UDP Scan
-sL	List Targets
-sA	Test for FW Protection (Open, filtered, unfiltered Ports)

Basic Scan Options Continue



-r	No random
--top-ports	Top Ports
-6	IPV6
-iL <file>	Input File
-oA/-oX/-oN... <file>	Output to file
--exclude	Exclude from scan
-n	Don't resolve name
-R	Reverse DNS lookup
-F	Fast Mode

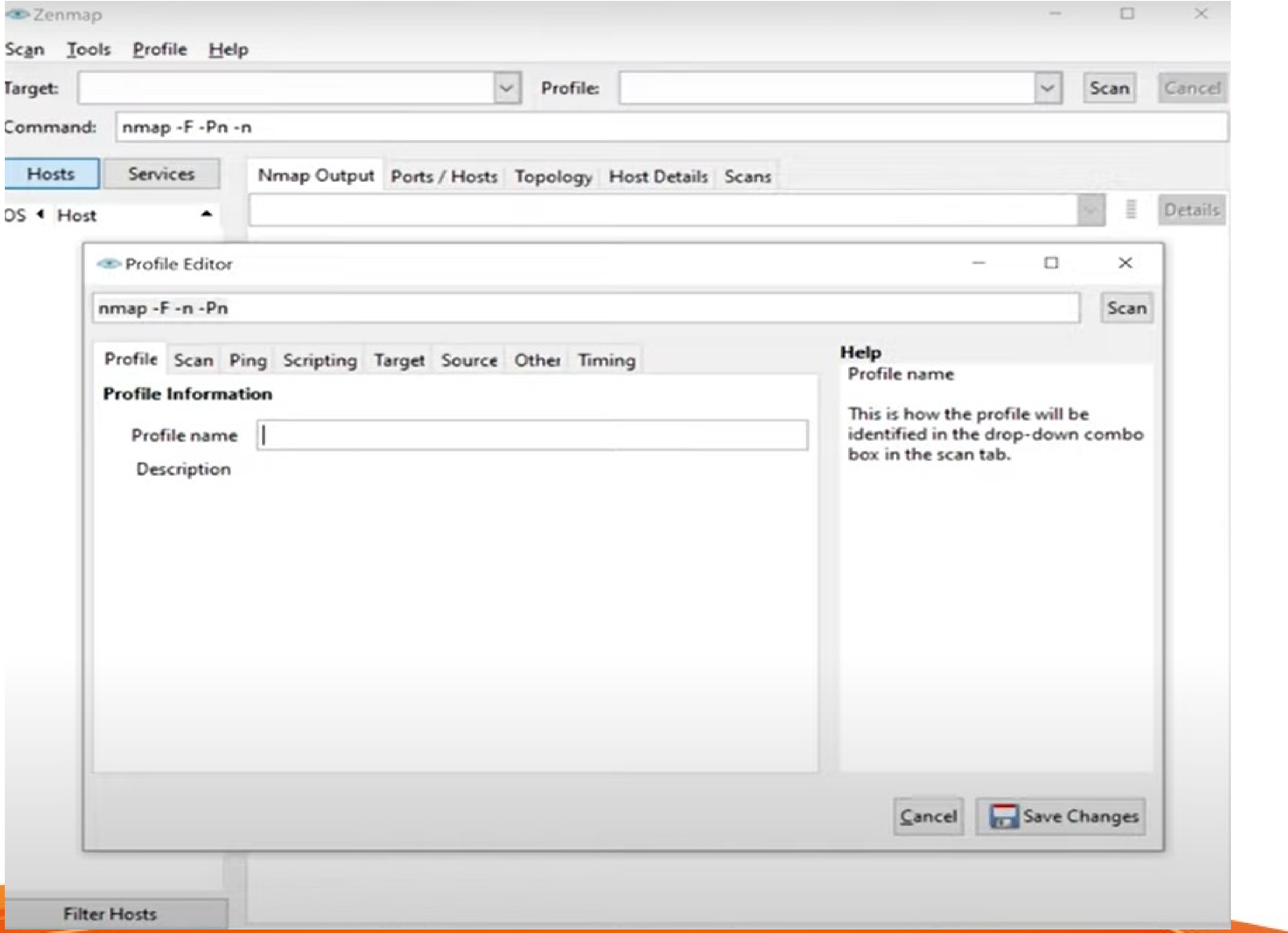


-O	OS Detection
-A	OS/Service/script/traceroute
--version-intensity <level>	Light to all probes (0-9)
-sC	All default scripts
-v, -vv	Verbosity levels
-PR	ARP
-sn	No port
-PS <port list>	Specified ports

Steps for network Scanning (best practices)

- ✓First, check for live system
- ✓Discover open ports
- ✓Scan beyond IDS
- ✓Banner Grabbing
- ✓Scan Vulnerabilities
- ✓Network Diagram Proxies

Host discovery Scan (52.209.77.0/24)



Command: nmap -F -Pn -n

nmap -F -n -Pn

Profile Information

Profile name

Description

Help

Profile name

This is how the profile will be identified in the drop-down combo box in the scan tab.

Checking for Live Devices

- End of Lecture