MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

ZTS Assignment

on

NMAP (Network Mapper)

SUBMITTED

BY

Rahul T N : 251091010017

Harsh Dhakate : 251091010019

Under the Guidance of:

Dr.Manoj T
Assistant Professor
School of Computer Engineering
Manipal Institute of Technology

Zero Trust Security (CSS5112)
July-November 2025

GitHub Repositories link:

Harsh Dhakate: ***https://github.com/HarshDhakate/Nmap_ZTS_Assignment.git***

Rahul T N: ***https://github.com/mrrahulshetty/NMAP---Network-Mapper***

1. INTRODUCTION TO NMAP TOOL

1.1 What is Nmap?

Nmap (Network Mapper) is a powerful, open-source network scanning tool created by Gordon Lyon (pseudonym: Fyodor Vaskovich) in September 1997. It is used for network discovery, security auditing, and vulnerability scanning. Nmap allows cybersecurity professionals, system administrators, and network engineers to identify active devices on a network, detect open ports, determine running services, and identify potential security vulnerabilities.

Nmap has become the industry standard for network reconnaissance and is widely trusted by security professionals, penetration testers, and network administrators worldwide. The tool is actively maintained and continuously updated with new features and detection capabilities.

1.2 Why Use Nmap?

Nmap is widely used in the cybersecurity field for several compelling reasons:

- **Network Discovery**: Quickly identify all devices connected to a network.
- **Port Scanning**: Determine which ports are open and which services are running.
- **Service Detection**: Identify running applications and their versions.
- **OS Fingerprinting**: Determine the operating system and version of target devices.
- **Vulnerability Assessment**: Identify potential vulnerabilities through NSE scripts.
- **Security Auditing**: Conduct comprehensive security assessments.
- **Network Inventory**: Maintain accurate records of network devices and services.
- **Incident Response**: Quickly assess the network during security incidents.

1.3 Key Features of Nmap

- **Host Discovery**: Identify active hosts on a network using various ping methods.
- **Port Scanning**: Enumerate open, closed, and filtered ports with multiple techniques.
- **Version Detection**: Detect service versions running on open ports.
- **Operating System Detection**: Fingerprint the target's OS and version.
- **NSE (Nmap Scripting Engine)**: Automate advanced scanning tasks using Lua scripts.
- **Multiple Output Formats**: Save results in Normal, XML, Grepable, or Script Kiddie formats.
- **Zenmap GUI**: Graphical interface for users preferring visual interaction.
- **Stealth Options**: Multiple evasion techniques to avoid detection.

1.4 How Nmap Works

Nmap operates by sending specially crafted network packets to target hosts and analyzing the responses received (or lack thereof). The basic operation involves:

1. **Target Specification**: The User defines the IP addresses or hostnames to scan.

2. **Host Discovery**: Nmap determines which hosts are online using ping methods.
3. **Port Scanning**: For each active host, Nmap scans specified ports to determine their state.
4. **Service Detection**: Nmap probes open ports to identify running services and versions.
5. **OS Fingerprinting**: Sends specially crafted packets and compares responses to known OS signatures.
6. **NSE Scripting**: Optional automation of specific scanning tasks.
7. **Output Generation**: Results presented in user-specified format.

2. INSTALLATION ON DIFFERENT OPERATING SYSTEMS

2.1 Installation on Linux

For Debian-based Systems (Ubuntu, Kali Linux, Debian, Linux Mint)

Step 1: Update Package Manager

sudo apt update

Explanation: Refreshes the package manager's database to get the latest package information.

Step 2: Install Nmap

sudo apt install nmap -y

Explanation: Downloads and installs Nmap from official repositories. The *-y* flag automatically answers "yes" to all prompts.

Step 3: Verify Installation

nmap -version

Explanation: Displays the installed Nmap version and build information, confirming successful installation.

Expected Output:

Nmap version 7.92 (https://nmap.org)
Platform: linux
Compiled with: liblua-5.3.5, libpcap 1.10.1, libpcre 8.45, libssh2 1.10.0, zlib 1.2.11
...

2.2 Installation on Windows

Step 1: Download the Installer

- Visit the official Nmap website: https://nmap.org/download.html.
- Download the latest *.exe* installer (e.g., *nmap-7.94-setup.exe*)

- Look for the “Microsoft Windows binaries” section.

Step 2: Run the Installer

- Double-click the downloaded *nmap-setup.exe* file.
- Click “Yes” when Windows prompts for permission to make changes.
- Read and accept the license agreement.
- Select components to install:
    - **Nmap** (core tool) – REQUIRED.
    - **Zenmap** (GUI) – Recommended.
    - **Ncat** (netcat replacement) – Optional.
    - **Ndiff** (scan comparison) – Optional.
    - **Nping** (packet generation tool) – Optional.

Step 3: Choose Installation Directory

- Default directory: *C:\Program Files (x86)\Nmap.*
- You can change this or keep default.
- Click “Next” to continue.

Step 4: Complete Installation

- Click “Install” to begin installation.
- Wait for installation to complete.
- Click “Finish” when done.
- The installer will automatically launch Npcap setup.

Step 5: Install Npcap (Windows Packet Capturing Driver)

- Npcap installer appears automatically.
- Accept the license agreement.
- Choose installation options (default is fine).
- Click “Install”.
- Restart may be required (allow if prompted).

Step 6: Verify Installation

- Open Command Prompt (Press *Win+R*, type *cmd*, press Enter).
- Type the command:

nmap -version

- If installed correctly, it displays version information.

Step 7: Optional - Add to System Path

If *nmap* command is not recognized globally:

- Open Start Menu → Search “Environment Variables”
- Click “Edit the system environment variables”
- Click the “Environment Variables” button at the bottom.
- Under “System Variables”, find and select “Path”
- Click “Edit” → “New” - Add *C:\Program Files (x86)\Nmap*
- Click OK on all dialogs - Restart Command Prompt.

2.3 Installation on macOS

Step 1: Install Homebrew (if not already installed)

/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

Explanation: Downloads and installs Homebrew package manager for macOS.

Step 2: Install Nmap

brew install nmap

Explanation: Installs Nmap using Homebrew.

Step 3: Verify Installation

nmap -version

Expected Output: Version and build information similar to Linux.

3. CONFIGURATION OF NMAP

3.1 Understanding Nmap Configuration Files

Nmap uses configuration files to customize its behavior and store settings. Understanding where these files are located helps you personalize Nmap’s functionality.

Configuration File Locations

On Linux and macOS: - System-wide configuration: */usr/share/nmap/* or */usr/local/share/nmap/* - Per-user configuration: *~/.nmap/* (home directory) - NSE scripts: */usr/share/nmap/scripts/*

On Windows: - Installation directory: *C:\Program Files (x86)\Nmap* - Scripts directory: *C:\Program Files (x86)\Nmap\scripts* - Configuration files: Same installation directory.

3.2 Default Configuration

Nmap comes with sensible defaults for most configurations. Understanding these defaults helps you optimize scans:

- **Default Scan Type**: TCP SYN scan (*-sS*).
- **Default Port Range**: Top 1,000 most commonly used ports.
- **Default Timing**: Polite mode (*-T3*).
- **Default Output**: Interactive (displayed on screen).
- **Default Host Discovery**: ICMP, TCP, and ARP.

3.3 Custom Configuration for Different Scenarios

For Fast Network Inventory Scanning:

nmap -T5 -p 1-1000 -sS --min-parallelism 100

For Comprehensive Security Audit:

nmap -A -T4 -sV -sC -O --script vuln,default -p- 2>&1 | tee audit.log

For Stealth Scanning (IDS Evasion):

nmap -T1 -sS -f --data-length 200 -D 192.168.1.101,192.168.1.102,ME

For Vulnerability Assessment:

nmap -sV --script vuln,default -p- --script-timeout 600

4. ESSENTIAL NMAP COMMANDS

4.1 Basic Scanning Commands

4.1.1 Scan a Single Target

nmap 192.168.1.1

Explanation: Performs a basic SYN scan on the target IP address, scanning the top 1,000 most common ports. This is the default behavior when no special options are specified.

Output shows: - Host status (up/down) - Port states (open/closed/filtered) - Service names associated with ports.

4.1.2 Scan Multiple Targets

nmap 192.168.1.1 192.168.1.2 192.168.1.3

Explanation: Scans three different IP addresses in sequence, useful for scanning specific known hosts.

4.1.3 Scan a Range of Hosts

nmap 192.168.1.1-50

Explanation: Scans IP addresses from 192.168.1.1 to 192.168.1.50 (50 hosts total). Useful for scanning consecutive IP ranges.

4.1.4 Scan an Entire Subnet

nmap 192.168.1.0/24

Explanation: Scans all 256 hosts in the 192.168.1.0/24 network using CIDR notation. The /24 means the last 8 bits can vary.

4.1.5 Scan Using Input File

nmap -iL targets.txt

Explanation: Reads target IP addresses from a text file (one IP per line) and scans them all. Useful for scanning many targets from a list.

targets.txt example:

192.168.1.1
192.168.1.5
example.com
10.0.0.0/24

4.2 Port Scanning Techniques

4.2.1 TCP SYN Scan (Stealth Scan) - DEFAULT

nmap -sS 192.168.1.1

How it works: - Sends SYN packet (connection request) - Analyzes response: - SYN-ACK = port open - RST = port closed - No response = port filtered.

Advantages: - Fast and stealthy (doesn’t complete full connection) - Default scan type - Works well through firewalls.

Disadvantages: - Requires root/administrator privileges on Linux/macOS - May not work on all systems.

4.2.2 TCP Connect Scan

nmap -sT 192.168.1.1

How it works: - Completes full three-way TCP handshake - Determines port state based on connection result.

Advantages: - Works without root privileges - More reliable on some systems - Works in restricted environments.

Disadvantages: - Slower than SYN scan - Connections appear in system logs - May trigger alerts.

4.2.3 UDP Scan

nmap -sU 192.168.1.1

How it works: - Sends UDP packets to target ports - Analyzes ICMP responses.

Advantages: - Finds UDP-based services (DNS, SNMP, DHCP, etc.) - Useful for comprehensive port assessment.

Disadvantages: - Very slow (ICMP rate limiting) - Can be combined with TCP scan: *nmap -sS -sU 192.168.1.1*

4.2.4 TCP FIN Scan

nmap -sF 192.168.1.1

How it works: - Sets only FIN flag on packet - RFC 793 compliant systems: - No response = port open/filtered - RST = port closed.

Advantages: - Bypasses some simple firewalls - Stealthier than SYN scan.

Disadvantages: - Unreliable against non-compliant systems - Modern firewalls easily detect.

4.2.5 TCP NULL Scan

nmap -sN 192.168.1.1

How it works: - Sets no TCP flags on the packet - Similar behavior to FIN scan.

Advantages: - Very stealthy - Bypasses some firewalls.

Disadvantages: - Works only against RFC-compliant systems - Unreliable on modern systems.

4.2.6 TCP Xmas Scan

nmap -sX 192.168.1.1

How it works: - Sets FIN, PSH, and URG flags - Named “Xmas” because flags light up like a Christmas tree.

Advantages: - Firewall evasion potential.

Disadvantages: - Very unreliable - Most modern firewalls detect it.

4.2.7 ACK Scan

nmap -sA 192.168.1.1

How it works: - Determines firewall state (not port state) - Unfiltered = firewall allows packets - Filtered = blocked by firewall.

Advantages: - Maps firewall rules - Useful for firewall analysis.

Disadvantages: - Doesn’t determine if ports are open/closed - Specific use case.

4.3 Port Specification

4.3.1 Scan Specific Port

nmap -p 80 192.168.1.1

Explanation: Scans only port 80 on the target.

4.3.2 Scan Multiple Specific Ports

nmap -p 22,80,443,3306 192.168.1.1

Explanation: Scans only the specified ports (SSH, HTTP, HTTPS, MySQL).

4.3.3 Scan Port Range

nmap -p 1-1000 192.168.1.1

Explanation: Scans ports 1 through 1000.

4.3.4 Scan All Ports

nmap -p- 192.168.1.1

Explanation: Scans all 65,535 TCP ports (takes longer but is comprehensive).

4.3.5 Scan Common Ports

nmap -F 192.168.1.1

Explanation: Fast scan of the top 100 most commonly used ports. Good for quick assessments.

4.4 Host Discovery

4.4.1 Ping Scan (Host Discovery Only)

nmap -sn 192.168.1.0/24

Explanation: - Determines which hosts are online without port scanning - Uses ICMP echo, TCP SYN/ACK, and ARP requests - Fast method to discover active devices - Does NOT perform port scanning.

Output:

Nmap scan report for 192.168.1.1
Host is up (0.0045s latency)
Nmap scan report for 192.168.1.5
Host is up (0.0052s latency)

4.4.2 TCP SYN Ping

nmap -PS 192.168.1.1

Explanation: Uses TCP SYN packets on port 80 for host discovery. Bypasses ICMP filters.

4.4.3 TCP ACK Ping

nmap -PA 192.168.1.1

Explanation: Uses TCP ACK packets for host discovery. Different method than SYN ping.

4.4.4 UDP Ping

nmap -PU 192.168.1.1

Explanation: Uses UDP packets for host discovery. Useful for discovering hosts blocking TCP.

4.4.5 ARP Ping

nmap -PR 192.168.1.1

Explanation: Uses ARP requests (only works on the local network). Most reliable for LAN discovery.

4.5 Service and Version Detection

4.5.1 Service Version Detection

nmap -sV 192.168.1.1

Explanation: - Probes open ports to determine service versions - Sends service-specific requests to identify applications - Longer scan time but provides valuable information - Example output: Apache 2.4.41, OpenSSH 7.4.

Output example:

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.6
443/tcp open https Apache httpd 2.4.6

4.5.2 OS Detection

nmap -O 192.168.1.1

Explanation: - Attempts to fingerprint operating system - Requires root privileges on Linux/macOS - Sends specially crafted packets and analyzes responses - Compares results against database of known OS signatures.

Output example:

Running: Linux 4.15 - 5.6
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.15-5.6

4.5.3 Aggressive OS Detection Guess

nmap -O --osscan-guess 192.168.1.1

Explanation: Makes an educated guess about OS if confidence is low, showing probability score (e.g., 95% confidence).

4.6 NSE (Nmap Scripting Engine) Scripts

4.6.1 Run Default Scripts

nmap -sC 192.168.1.1

Or equivalently:

nmap --script=default 192.168.1.1

Explanation: Runs default category NSE scripts for common vulnerability checks. Useful for basic security assessment.

4.6.2 Run Vulnerability Detection Scripts

nmap --script=vuln 192.168.1.1

Explanation: Runs all vulnerability detection scripts against the target. Scans for known CVEs and weaknesses.

4.6.3 Run Specific Script

nmap --script=smb-os-discovery 192.168.1.1

Explanation: Runs a specific NSE script (in this case, SMB OS discovery). Many specialized scripts are available.

4.6.4 Run Multiple Script Categories

nmap --script="default,vuln,exploit" 192.168.1.1

Explanation: Runs scripts from multiple categories (comma-separated). Combines different scanning capabilities.

4.6.5 Check SMB Vulnerabilities

nmap --script=smb-vuln-ms17-010 -p 445 192.168.1.1

Explanation: Checks for EternalBlue vulnerability (CVE-2017-0144) on SMB service. Critical for Windows systems.

4.7 Output Options

4.7.1 Normal Output to File

nmap 192.168.1.1 -oN output.txt

Explanation: Saves scan results in a normal (human-readable) format. Easy to read but harder to parse.

4.7.2 XML Output

nmap 192.168.1.1 -oX output.xml

Explanation: Saves in XML format for parsing by other tools. Better for automated processing.

4.7.3 Grepable Output

nmap 192.168.1.1 -oG output.grep

Explanation: Saves in a grep-friendly format for processing with command-line tools like grep and awk.

4.7.4 All Formats

nmap 192.168.1.1 -oA results

Explanation: Saves in all three formats (.nmap, .xml, .gnmap). Creates three files: results.nmap, results.xml, results.gnmap.

4.7.5 Verbose Output

nmap -v 192.168.1.1
nmap -vv 192.168.1.1

Explanation: Increases verbosity level; *-vv* shows even more details. Useful for troubleshooting.

4.7.6 Debugging Output

nmap -d 192.168.1.1
nmap -dd 192.168.1.1

Explanation: Enables debugging information for troubleshooting scan issues.

4.8 Firewall/IDS Evasion

4.8.1 Fragment Packets

nmap -f 192.168.1.1

Explanation: Splits packets into small fragments to bypass simple packet filters. *-f* sends 8-byte fragments, *-ff* sends 16-byte fragments.

4.8.2 Decoy Scanning

nmap -D 192.168.1.100,192.168.1.101,192.168.1.102,ME 192.168.1.1

Explanation: - Sends scan packets from multiple decoy addresses - “ME” represents your actual IP - Makes it harder to identify actual scanner - Does not hide your IP but confuses logs

4.8.3 Spoof Source IP

nmap -S 192.168.1.50 192.168.1.1

Explanation: Spoofs source IP (requires raw socket access, responses may not return). Advanced technique.

4.8.4 Idle Zombie Scan

nmap -sI zombie.host 192.168.1.1

Explanation: Uses another host (zombie) to perform scan (very stealthy but slow). Advanced evasion technique.

5. NMAP COMMAND REFERENCE TABLE

Table 1: Quick Command Reference

Purpose	Command	Time	Use Case
Quick Network Discovery	nmap -sn 192.168.1.0/24	< 1 min	Identify all active hosts
Basic Port Scan	nmap 192.168.1.1	2-3 min	Standard reconnaissance
Full Port Scan	nmap -p- 192.168.1.1	10-30 min	Complete port enumeration
Fast Scan	nmap -F 192.168.1.1	1-2 min	Quick overview of the top 100 ports
Service Detection	nmap -sV 192.168.1.1	3-5 min	Identify running services
OS Detection	nmap -O 192.168.1.1	10-15 min	Determine the operating system
Aggressive Audit	nmap -A -T4 192.168.1.1	15-30 min	Comprehensive security scan
Stealth Scan	nmap -sS -T1 -f 192.168.1.1	20-60 min	Avoid IDS/firewall detection
Firewall Testing	nmap -sA -p 1-1000 192.168.1.1	5-10 min	Test firewall rules
Vulnerability Scan	nmap –script vuln 192.168.1.1	10-20 min	Find CVEs and security issues
Web Server Audit	nmap -p 80,443 -sV –script http-vuln* 192.168.1.1	5-10 min	Web application security check
Database Discovery	nmap -p 3306,5432,1433 192.168.1.0/24	5-15 min	Locate database servers
SSH Port Check	nmap -p 22 192.168.1.1	1-2 min	Check SSH access
Multiple Target Scan	nmap 192.168.1.1 192.168.1.2 192.168.1.3	3-5 min	Scan specific hosts
Exclude Sensitive Hosts	nmap 192.168.1.0/24 –exclude 192.168.1.100	2-4 min	Skip protected systems

Table 2: All Scanning Techniques Comparison

Scan Type	Command	Detection	Advantages	Disadvantages	Root Required
TCP SYN	-sS	SYN-ACK=Open, RST=Closed	Fast, stealthy, default	Needs tuning sometimes	Yes
TCP Connect	-sT	Full handshake success=Open	No root needed, reliable	Slow, detectable, completes connection	No
UDP	-sU	ICMP unreachable=Closed	Finds UDP services	Very slow, ICMP rate limited	Yes
FIN	-sF	No Response=Open, RST=Closed	Stealth, firewall bypass	Unreliable, RFC-dependent	Yes
NULL	-sN	No Response=Open, RST=Closed	Very stealthy, bypass	Unreliable on modern systems	Yes
ACK	-sA	RST=Unfiltered, No Response=Filtered	Firewall mapping	Doesn’t show port state	Yes
Xmas	-sX	No Response=Open, RST=Closed	Named for appearance	Very unreliable	Yes

6. PRACTICAL USE CASES

Use Case 1: Network Discovery and Host Inventory

Scenario: Network administrator needs to create an inventory of all active devices on the company network.

Objective: Identify all active hosts, their services, and operating systems for network documentation.

Step-by-Step Commands:

Step 1: Discover all active hosts

nmap -sn 192.168.1.0/24 -oG hosts.grep

Explanation: This ping scan identifies all active hosts on the network and saves the results in a format that is easily parsed using grep.

Expected Output:

Host: 192.168.1.1 (gateway.local) Ports: 0/0
Host: 192.168.1.5 (server1.local) Ports: 0/0
Host: 192.168.1.10 (workstation.local) Ports: 0/0

Step 2: Scan each discovered host for services

nmap -sV -p 1-1000 192.168.1.1 192.168.1.5 192.168.1.10 -oX inventory.xml

Explanation: This identifies running services and versions on each discovered host.

Expected Output:

Nmap scan report for 192.168.1.1
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.4
80/tcp open http Apache httpd 2.4
443/tcp open https Apache httpd 2.4

Step 3: Generate a detailed report

nmap -A 192.168.1.0/24 -oA network_audit

Explanation: Comprehensive scan of all hosts with all detection methods.

Output Files Generated: - network_audit.nmap (human-readable) - network_audit.xml (machine-readable) - network_audit.gnmap (grepable format).

Business Value: Creates an accurate network inventory for asset management, compliance reporting, and security baseline.

Use Case 2: Firewall Rule Testing

Scenario: Network administrator needs to verify firewall rules are working correctly.

Objective: Validate that the firewall is properly blocking/allowing traffic on configured ports.

Step-by-Step Commands:

Step 1: Standard SYN scan to identify open ports

nmap -sS -T4 192.168.1.1

Explanation: Baseline scan to see which ports respond as open through the firewall.

Step 2: ACK scan to determine firewall state

nmap -sA -p 1-1000 192.168.1.1

Explanation: Shows which ports the firewall recognizes as unfiltered vs filtered.

Step 3: Analyze filtered vs closed ports

nmap -sS -p 1-10000 192.168.1.1 | grep filtered

Explanation: Identifies ports blocked by the firewall (filtered status).

Expected Analysis: - Open ports = allowed through firewall - Filtered ports = blocked by firewall - Closed ports = no service running - Unfiltered ports = firewall allows, but port closed.

Business Value: Verifies firewall configuration is correct, tests rules work as intended, and validates security perimeter.

Use Case 3: Remote Access Service Identification

Scenario: The Security team needs to locate SSH, RDP, and other remote access services.

Objective: Identify and audit remote access services on the network.

Step-by-Step Commands:

Step 1: Find hosts with SSH (port 22) and RDP (port 3389)

nmap -sS -p 22,3389,5900 192.168.1.0/24

Explanation: Searches for common remote access services.

Step 2: Identify SSH versions

nmap -sV -p 22 192.168.1.0/24

Explanation: Determines SSH versions for vulnerability assessment.

Expected Output:

22/tcp open ssh   OpenSSH 7.4 (protocol 2.0)

Step 3: Check for SSH vulnerabilities

nmap --script ssh-vuln*,ssh2-enum-algos -p 22 192.168.1.100

Explanation: Detects SSH version vulnerabilities and weak algorithms.

Business Value: Identifies remote access services, detects outdated SSH versions, and supports access control policy.

7. COMMON ISSUES AND TROUBLESHOOTING

Issue 1: “Host seems down”

Error Message:

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn Nmap done: 1 IP address (0 hosts up) scanned in 3.31 seconds

Root Causes: - Target host is blocking ICMP packets (ping requests) - Firewall configured to drop ICMP - Host is genuinely offline or unreachable - Network connectivity issues between scanner and target

Solution 1: Use -Pn flag (Skip Ping/Host Discovery)

nmap -Pn 192.168.1.1

Explanation: Assumes the host is up and skips the host discovery phase. Directly scans for ports.

When to use: When you know the host is up but not responding to ping.

Solution 2: Specify Host Discovery Method

nmap -PS -p 22,80,443 192.168.1.1

Explanation: Uses TCP SYN packets on specific ports for host discovery instead of ICMP.

When to use: When ICMP is blocked but TCP is allowed.

Solution 3: Verify Connectivity First

ping 192.168.1.1
tracert 192.168.1.1 (Windows)
traceroute 192.168.1.1 (Linux/macOS)

Explanation: Check basic network connectivity to the target.

Prevention: Always verify connectivity before running scans.

Issue 2: “Permission denied”

Error Messages:

Warning: Starting Nmap scan with unprivileged user; only root can use this option. socket troubles in nsock_iocb_dispatch() from ncrlib

Root Causes: - User lacks root/administrator privileges - Certain scan types require raw socket access - Running from restricted environment (Docker, VM) - SELinux or AppArmor restricting access.

Solution 1: Use sudo (Linux/macOS)

sudo nmap -sS 192.168.1.1

Explanation: Runs Nmap with root privileges required for SYN scan.

When to use: When you have sudo access and need raw sockets.

Solution 2: Use TCP Connect Scan (No Root Required)

nmap -sT 192.168.1.1

Explanation: TCP Connect scan works without raw sockets (slower but functional).

When to use: When you don't have root access.

When to use: Best alternative for non-root users.

Solution 3: Run as Administrator (Windows)

- Right-click Command Prompt → "Run as administrator"
- Then run: *nmap -sS 192.168.1.1*

Issue 3: "RST from Your IP"

Error Messages:

Received port unreachable message from your IP
Received reset from your IP

Root Causes: - Local firewall interfering with scans - Incorrect routing configuration - Local antivirus/security software blocking scans - Previous scan process still running - Network interface misconfiguration.

Solution 1: Check Local Firewall

Linux (UFW):

sudo ufw status
sudo ufw disable

macOS:

System Preferences → Security & Privacy → Firewall → Turn Off

Windows:

Settings → Privacy & Security → Windows Firewall → Toggle Off

When to use: For testing purposes on isolated systems.

Solution 2: Add an Exception to the Firewall

Windows (Better approach): - Settings → Privacy & Security → Windows Firewall → Advanced Settings - Inbound Rules → New Rule - Create rule to allow *nmap.exe*

When to use: Instead of disabling the entire firewall.

Solution 3: Use a Different Scan Technique

nmap -sT 192.168.1.1

Explanation: TCP Connect avoids raw socket issues.

Solution 4: Check the Default Gateway

route print (Windows)
netstat -rn (Linux/macOS)

Explanation: Verify the routing configuration is correct.

Prevention: Understand firewall rules before running scans; test on isolated systems first.

Issue 4: "No Ports Found Open"

Problem: Scan completes but shows no open ports.

Possible Causes: - All ports actually closed (host has no open ports) - All ports filtered by firewall - Wrong IP address targeted - Scan completed too quickly without giving enough time - Host is offline despite appearing to respond to ping.

Solution 1: Verify the Host is Up First

ping 192.168.1.1
nmap -sn 192.168.1.1

Explanation: Confirm the host is actually online and responding.

Solution 2: Scan All Ports, Not Just Top 1000

nmap -p- 192.168.1.1

Explanation: Scans all 65,535 ports instead of just the top 1000.

Time cost: Takes 10-30 minutes or more.

When to use: When important services are on non-standard ports.

Solution 3: Check UDP Ports

nmap -sU 192.168.1.1

Explanation: UDP services may be running even if TCP ports are closed.

When to use: To check for DNS, NTP, SNMP, etc.

Solution 4: Use Verbose Output for Troubleshooting

nmap -v -p- 192.168.1.1

Explanation: Shows detailed output of what's happening during scan.

When to use: For debugging why no ports are found.

Table 3: Troubleshooting Quick Reference

Problem	Quick Fix	Alternative	Prevention
Host seems down	nmap -Pn 192.168.1.1	nmap -PS -p 22,80 192.168.1.1	Verify connectivity first
Permission denied	sudo nmap -sS 192.168.1.1	nmap -sT 192.168.1.1	Understand privilege needs
Timeout expired	nmap -F 192.168.1.1	nmap -T5 192.168.1.1	Adjust timing for the network
No ports found	nmap -p- 192.168.1.1	nmap -Pn -p- 192.168.1.1	Verify the target is correct
Service detection failed	nmap -sV –version-intensity 9	Manually verify	Keep Nmap updated
Getting RST from IP	Disable local firewall	Use -sT scan	Check firewall rules

8. LIVE DEMO SCENARIOS

Demo 1: Basic Network Reconnaissance

Objective: Discover active hosts and open ports on a network.

Commands to Execute:

Step 1: Discover all active hosts on the subnet

nmap -sn 192.168.1.0/24

Output:

```
┌──(harsh㉿Kali)-[~]
└─$ nmap -sn 192.168.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 21:38 IST
Nmap scan report for 192.168.100.1
Host is up (0.0026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.100.2
Host is up (0.0022s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.100.3
Host is up (0.0019s latency).
MAC Address: 08:00:27:BC:84:D6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.4
Host is up (0.0017s latency).
MAC Address: 08:00:27:FB:37:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.6
Host is up (0.0046s latency).
MAC Address: 08:00:27:7B:F4:97 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.100.5
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 22.07 seconds
```

Analysis: 6 active hosts discovered on the network at .1, .2, .3, .4, .5, and .6.

Step 2: Perform a SYN scan on discovered hosts

nmap -sS -T4 192.168.1.1 192.168.1.5

Output:

```
┌──(harsh㉿Kali)-[~]
└─$ nmap -sS -T4 192.168.100.6 192.168.100.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 21:40 IST
Nmap scan report for 192.168.100.6
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7B:F4:97 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.4
Host is up (0.0021s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:FB:37:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (2 hosts up) scanned in 12.25 seconds
```

Analysis: - 192.168.100.6 is running SSH, HTTP, HTTPS (likely a web server) - 192.168.100.4 is running 3389 ms-wbt-server.

Step 3: Identify service versions

nmap -sV -p 22,80,443,3306 192.168.1.1 192.168.1.5

Output:

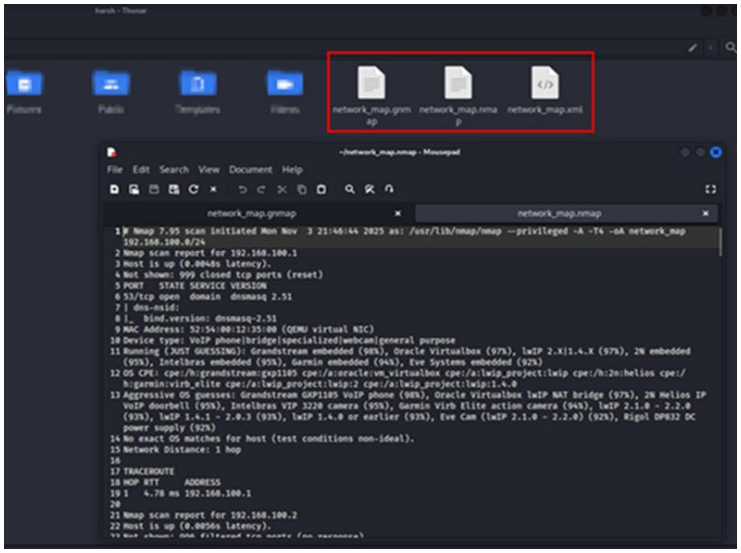
```
┌──(harsh㉿Kali)-[~]
└─$ nmap -sV -p 22,80,443,3306 192.168.100.4 192.168.100.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-03 21:44 IST
Nmap scan report for 192.168.100.4
Host is up (0.0015s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3306/tcp filtered mysql
MAC Address: 08:00:27:FB:37:56 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.6
Host is up (0.0024s latency).

PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp   open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp  closed https
3306/tcp open   mysql   MySQL 5.0.51a-3ubuntu5
MAC Address: 08:00:27:7B:F4:97 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 17.39 seconds
```

Analysis: - OpenSSH 4.7p1 (older, may have vulnerabilities) - Apache 2.2.8 (somewhat dated) - MySQL 5.0.51 (older version, no longer supported by vendor).

Step 4: Save detailed results

nmap -A -T4 192.168.1.0/24 -oA network_map

Output Files Created: - network_map.nmap (human-readable) - network_map.xml (machine-readable) - network_map.gnmap (grepable).



Key Takeaways: - Ping scan identifies active hosts quickly - Port scanning reveals services - Version detection enables vulnerability assessment - Saving results in multiple formats supports different use cases.

Demo 2: Vulnerability Detection

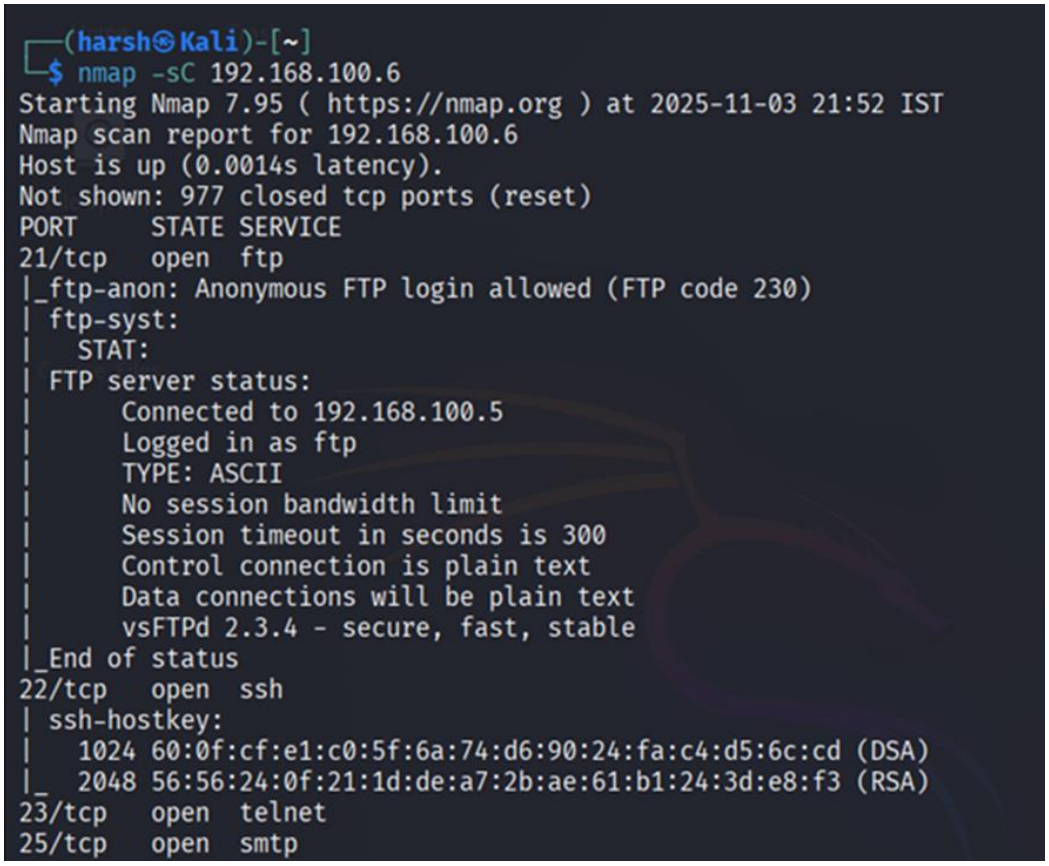
Objective: Identify potential vulnerabilities using NSE scripts.

Commands to Execute:

Step 1: Run default NSE scripts

nmap -sC 192.168.1.100

Output:

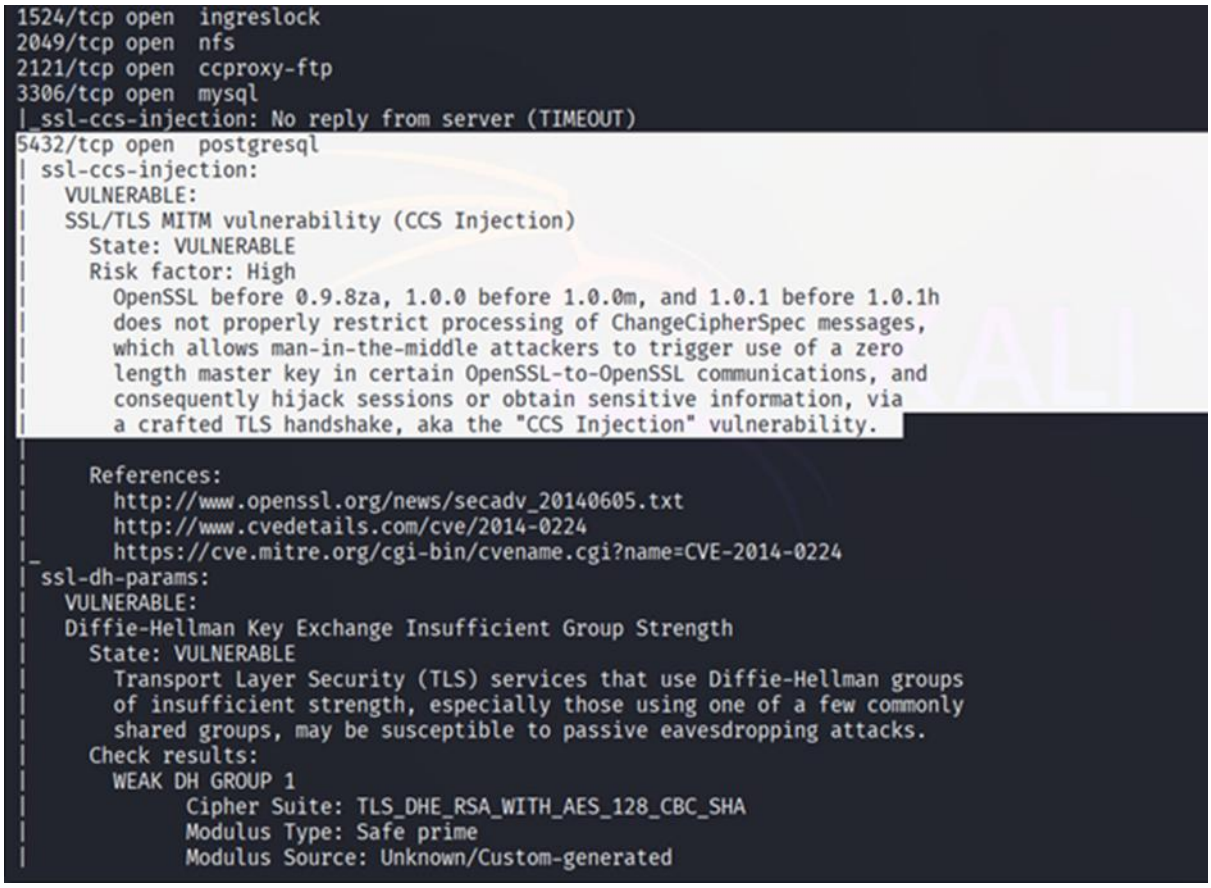


Analysis: - SSH keys found (for version tracking) - HTTP service identified - SSL certificate expiring (needs renewal).

Step 2: Run vulnerability detection scripts

nmap --script vuln 192.168.1.100

Output:

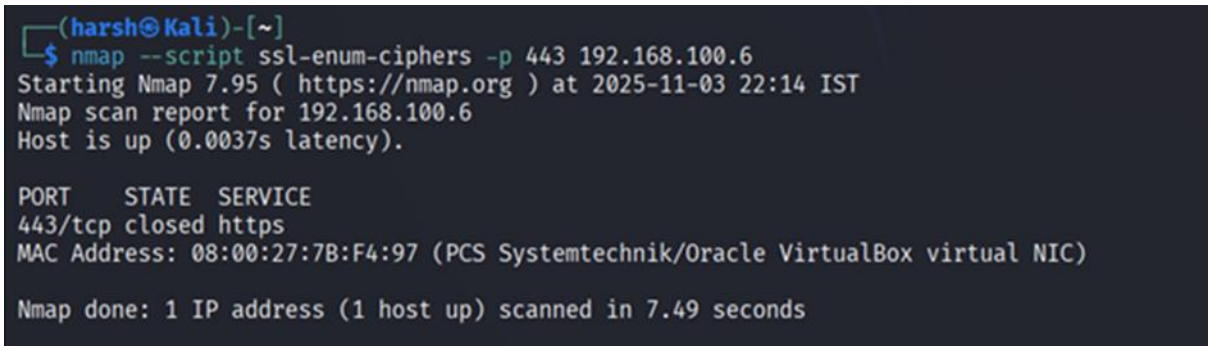


Analysis: - CVE-2014-0224 detected on SSL/TLS - This is a CRITICAL vulnerability requiring immediate patching.

Step 3: Check specific vulnerabilities

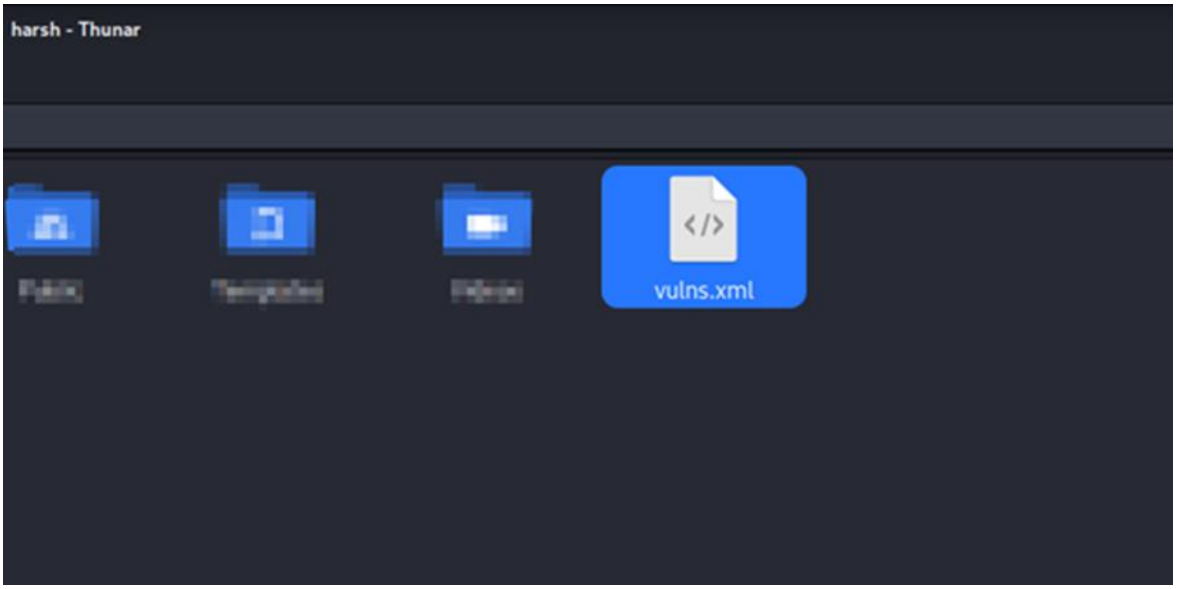
nmap --script ssl-enum-ciphers -p 443 192.168.1.100

Output:



Step 4: Generate vulnerability report

nmap -sV --script vuln,default -p- 192.168.1.100 -oX vulns.xml



Business Value: - Identifies critical vulnerabilities needing immediate action - Ranks risks by severity - Provides CVE numbers for vendor patches - Enables tracking of remediation progress.

Key Takeaways: - NSE scripts automate vulnerability detection - Results should be verified before reporting - CVE numbers help in patch management - Regular scanning supports vulnerability management program.

Demo 3: Firewall Analysis Scanning

Objective: Perform stealthy scanning to avoid detection and analyze the firewall.

Commands to Execute:

Step 1: Standard SYN scan (baseline)

nmap -sS 192.168.1.1

Expected Output:

Starting Nmap 7.92 (https://nmap.org) at 2025-11-02 12:30 IST
Nmap scan report for 192.168.1.1
Host is up (0.0032s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https

Analysis: 3 ports open, 997 closed (expected for standard scan).

Step 2: Stealthy scan with fragmentation

nmap -sS -f 192.168.1.1

Expected Output:

Same as above but packets are fragmented

Explanation: Packets are split into small fragments to potentially bypass IDS detection.

Step 3: Decoy scanning

nmap -sS -D 192.168.1.100,192.168.1.101,ME 192.168.1.1

Expected Output:

Same results but traffic appears to come from multiple sources

Explanation: - Sends scan packets from multiple decoy IPs - Makes it harder to identify actual scanner - Decoy IPs don't receive responses (but confuses logs) - "ME" identifies your actual position in decoy list.

Step 4: ACK scan for firewall analysis

nmap -sA -p 1-1000 192.168.1.1

Expected Output:

PORT STATE SERVICE
22/tcp unfiltered ssh
80/tcp unfiltered http
443/tcp unfiltered https
500/tcp filtered ike

Analysis: - Unfiltered = firewall allows traffic to reach those ports - Filtered = firewall is blocking traffic - Helps understand firewall configuration.

Step 5: Combined evasion techniques

nmap -sS -f -D 192.168.1.100,ME --data-length 200 -T1 192.168.1.1

Expected Output:

Same results but:
- Packets fragmented (-f)
- Coming from multiple sources (-D)
- Random data added (--data-length)
- Very slow timing (-T1)

Result: - Extremely stealthy scan - Very slow (20-60 seconds for top 1000 ports) - Avoids most IDS/firewall detection - Uses significant bandwidth and time.

Legal & Ethical Note: - Stealth scanning should ONLY be performed on systems you own - Unauthorized stealth scanning is illegal - Always get written authorization before any security testing - Decoy scanning may be detected by advanced monitoring.

Key Takeaways: - Different scan techniques bypass different security controls - ACK scans reveal firewall configuration - Evasion techniques should only be used in authorized testing - Stealth comes with a time/accuracy tradeoff.

9. BEST PRACTICES AND ETHICAL CONSIDERATIONS

9.1 Legal and Ethical Guidelines

CRITICAL: Always Obtain Authorization

Before conducting ANY network scan or penetration test:

1. **Get Written Permission**
    - Obtain written authorization from the network owner.
    - Specify scope (IP ranges, hosts, timeframe).
    - Document authorization before starting.
    - Keep authorization documentation for legal protection.
2. **Only Scan Authorized Targets**
    - Do NOT scan networks you don’t own.
    - Do NOT scan third-party systems without permission.
    - Do NOT conduct tests on public networks.
    - Unauthorized network scanning is ILLEGAL.
3. **Use Nmap Responsibly**
    - Understand that scanning can impact systems.
    - Avoid heavy scanning during production hours if possible.
    - Consider network load impact.
    - Scan during maintenance windows when feasible.
4. **Maintain Confidentiality**
    - Keep scan results confidential.
    - Do NOT share detailed scan results publicly.
    - Securely store scan data.
    - Only share results with authorized personnel.

9.2 Technical Best Practices

Scanning Best Practices:

1. **Start Conservative**
    - Begin with ping scans to find hosts.
    - Use the top 1,000 ports before a full port scan.
    - Verify results before proceeding.
    - Avoid aggressive scans on production systems.
2. **Use Appropriate Timing**
    - Use T3 (normal) for most scenarios.
    - Use T1-T2 for stealth operations on authorized tests.
    - Use T4-T5 only on fast, reliable networks.
    - Adjust for specific network conditions.
3. **Save Results Properly**
    - Always save in multiple formats.
    - Use descriptive filenames with dates.
    - Store in a secure location.
    - Maintain audit trail of scans.
4. **Document Your Scanning**
    - Record what you scanned and when.
    - Note any special circumstances.
    - Document findings and follow-up actions.
    - Create repeatable scanning procedures.
5. **Verify Findings**
    - Never trust tool output blindly.
    - Manually verify critical findings.
    - Cross-reference with official databases.
    - Check for false positives.

11. CONCLUSION

Nmap is an indispensable tool in cybersecurity for network reconnaissance and vulnerability assessment. This comprehensive guide provides:

- **Complete Installation Procedures**: Step-by-step instructions for Windows, Linux, and macOS.
- **In-Depth Command Reference**: 50+ commands with detailed explanations and examples.
- **Practical Use Cases**: Seven real-world scenarios demonstrating practical applications.

- **Troubleshooting Solutions**: Seven common issues with multiple solutions for each.
- **Live Demo Scenarios**: Four executable demonstrations from basic to advanced.
- **Best Practices**: Ethical and technical guidelines for responsible scanning.

Key Takeaways

1. **Nmap's Flexibility**: Supports multiple scanning techniques for different scenarios, from stealth to aggressive audits.
2. **Multiple Scan Types**: SYN, TCP Connect, UDP, FIN, and others provide options for different network conditions and permissions.
3. **Service Detection**: NSE scripts automate vulnerability detection and provide detailed system information.
4. **Network Security**: Comprehensive scanning supports network security audits, compliance verification, and incident response.
5. **Ethical Responsibility**: Always obtain authorization before scanning; unauthorized network scanning is illegal.
6. **Continuous Learning**: Regular practice and staying updated with new Nmap features improve proficiency.