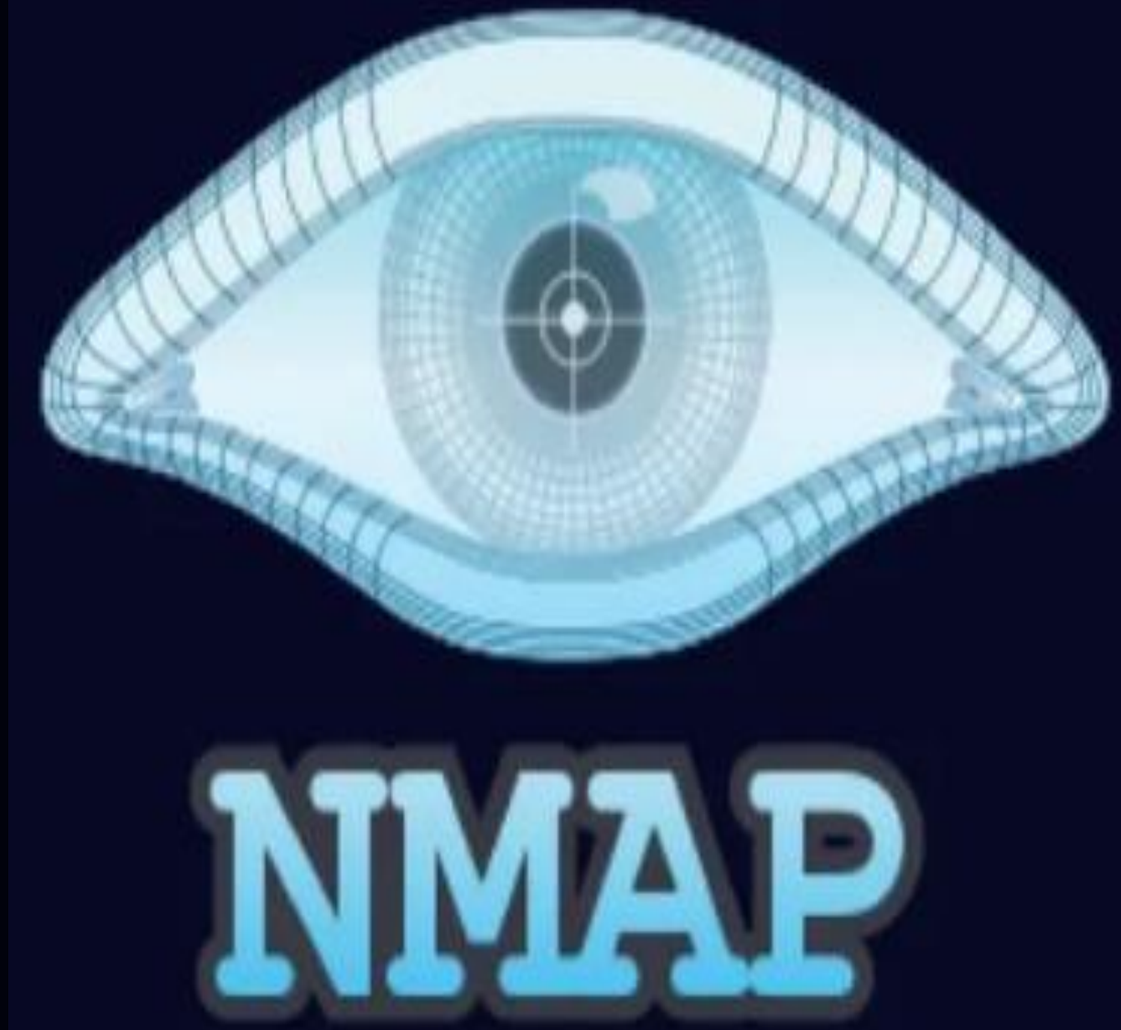
Nmap – Network Scanning and Security Auditing Tool

Kushal Goswami
PTID-CHE-SEP-25-219



Introduction to Nmap

Nmap (Network Mapper) is a **free and open-source** tool essential for network discovery, security auditing, and vulnerability scanning in modern IT environments.

This powerful utility helps security professionals and network administrators identify connected devices, discover open ports, enumerate running services, and determine operating system versions across network infrastructure.

Throughout this presentation, we'll demonstrate practical Nmap usage for comprehensive network scanning and auditing on Kali Linux.

Key Capabilities

- Network device discovery
- Port enumeration
- Service identification
- OS fingerprinting

About Nmap: Understanding Network Visibility

Device Discovery

Which devices are active and responsive on the network?

Port Analysis

Which ports are open and what services are running on them?

OS Detection

What operating system versions are being used across the network?

Nmap serves as a **proactive security measure**, enabling organizations to identify vulnerabilities and security gaps before malicious actors can discover and exploit them. By understanding your network's attack surface, you can strengthen defenses effectively.

Project Objectives

01

Demonstrate Practical Usage

Showcase real-world Nmap applications for comprehensive network auditing and security assessment.

02

Identify Network Components

Discover open ports, enumerate running services, and gather detailed OS information from target systems.

03

Execute Varied Scan Types

Perform multiple scanning techniques ranging from basic to aggressive reconnaissance, analyzing each result set.

04

Deliver Security Recommendations

Provide actionable insights and remediation strategies for identified vulnerabilities and security weaknesses.

Basic Scan: Initial Reconnaissance

Command Syntax

```
nmap 192.168.196.128
```

Purpose & Function

This foundational scan discovers **open ports** and identifies basic services running on the target host. It reveals host availability, open port numbers, service names, and MAC address details.

Common Services Discovered

- **FTP (Port 21)** - File transfer protocol
- **SSH (Port 22)** - Secure shell access
- **HTTP (Port 80)** - Web server
- **MySQL (Port 3306)** - Database service

This scan type provides the quickest overview of a target's accessible network services, forming the foundation for deeper investigation.

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.196.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 15:34 EDT
Nmap scan report for 192.168.196.128
Host is up (0.0040s 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: 00:0C:29:95:37:AE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds

┌──(root㉿kali)-[~]
└─#
```

Specific Port Scan: Targeted Analysis

Command Used

```
nmap -p 21,22,80,3306 192.168.196.128
```

Strategic Focus

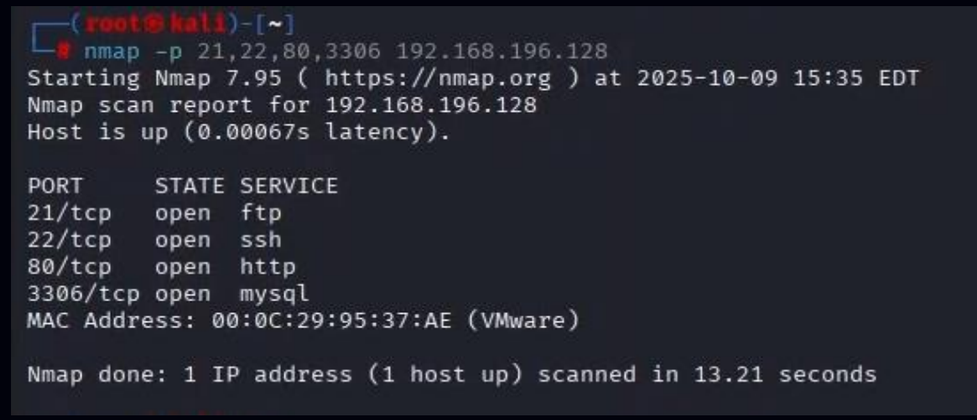
Scans only specified ports to concentrate reconnaissance on critical services, reducing scan time and noise.

Confirmed Results

Validates open status for FTP, SSH, HTTP, and MySQL services on the target system.

Best Practice Tip

Targeted port scanning is more efficient when you already know which services to investigate, making it ideal for follow-up scans after initial reconnaissance.



Service & Version Detection

Uncovering Software Details

```
nmap -sV 192.168.196.128
```

The `-sV` flag enables **version detection**, which probes open ports to determine exact service names and software version numbers. This intelligence is critical for vulnerability assessment.

vsftpd 2.3.4

FTP server version - **outdated and vulnerable** to known exploits

Apache 2.2.8

Web server version - legacy software with multiple security advisories

MySQL 5.0.51a

Database version - antiquated release with documented vulnerabilities

Security Alert: All detected versions are significantly outdated, indicating substantial security risks and known vulnerabilities that attackers could exploit.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.196.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 1
Nmap scan report for 192.168.196.128
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgr
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgr
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP eng
MAC Address: 00:0C:29:95:37:AE (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.M

Service detection performed. Please report any incorrec
Nmap done: 1 IP address (1 host up) scanned in 135.16 s

┌──(root㉿kali)-[~]
└─#
```

Operating System Detection

OS Fingerprinting Command

```
sudo nmap -O 192.168.196.128
```

The `-O` option activates **operating system detection**, which analyzes network stack characteristics to identify the target's OS and kernel version range.

Note: Requires root/sudo privileges

Detection Results

Identified OS: Linux kernel 2.6.x

Risk Assessment

The detected Linux 2.6.x kernel is extremely old and vulnerable. Modern systems use 5.x or 6.x kernels with critical security patches.

OS detection helps security analysts understand the **patch level and potential vulnerability exposure** of target systems, guiding remediation priorities.

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.196.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 1
Nmap scan report for 192.168.196.128
Host is up (0.00061s 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: 00:0C:29:95:37:AE (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect res
Nmap done: 1 IP address (1 host up) scanned in 14.60 se
```

Aggressive Scan: Full Reconnaissance

Comprehensive Detection Suite

```
sudo nmap -A 192.168.196.128
```

The `-A` flag enables **aggressive scanning**, combining OS detection, version detection, script scanning, and traceroute into one comprehensive reconnaissance operation.

Anonymous FTP Access

Unauthenticated access enabled - major security vulnerability

Insecure SSLv2 Protocol

Deprecated encryption protocol with known cryptographic weaknesses

Outdated Apache Server

Legacy web server version requiring immediate update

> **Critical Finding:** Bindshell discovered on port 1524 — this represents a severe security compromise allowing unauthorized remote access.

Aggressive scans provide the most detailed intelligence but generate significant network traffic and may trigger intrusion detection systems.

```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.196.128 -oN test.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-
Nmap scan report for 192.168.196.128
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.196.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubu
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-10-09T19:53:00+00:00; +4m27s from
| ssl-cert: Subject: commonName=ubuntu804-base.loca
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELI
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubu
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

Nmap Script Example: HTTP Enumeration

Script Execution

```
nmap --script=http-enum -p 80
192.168.196.128
```

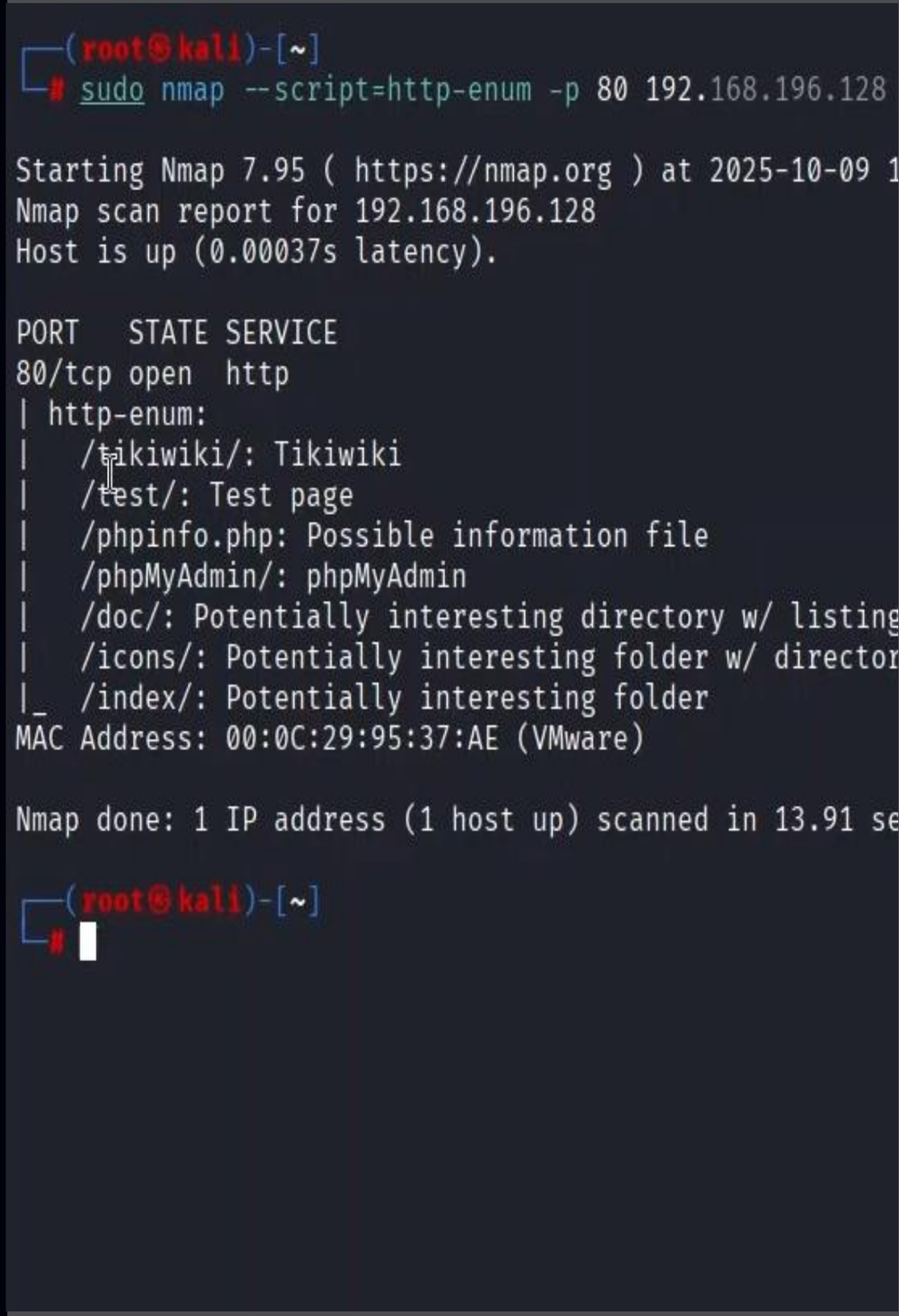
Nmap Scripting Engine (NSE) scripts extend functionality. The `http-enum` script discovers exposed web directories and files.

Discovered Paths

- `/icons/` - Server icon directory
- `/manual/` - Apache documentation
- `/phpmyadmin/` - Database admin panel

HTTP enumeration helps identify **sensitive paths and potential attack surfaces** on web servers. Exposed admin panels like phpMyAdmin represent significant security risks if not properly secured.

> **Key Takeaway:** Nmap is an indispensable tool for network security professionals. Master its various scan types, understand the intelligence each provides, and always scan responsibly with proper authorization.



Saving Reports

Proper documentation is essential for effective network security analysis. Saving Nmap scan results creates a permanent record for comprehensive review, trend analysis, and compliance reporting.

Command Syntax

```
nmap -A 192.168.196.128 -oN full_report.txt
```

The `-oN` flag exports results in normal format, creating a human-readable text file.

Key Benefits

- Maintain detailed audit trails for security assessments
- Compare scan results over time to track changes
- Share findings with team members and stakeholders
- Support incident response and forensic investigations

```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.196.128 -oN test.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-
Nmap scan report for 192.168.196.128
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.196.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubu
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-10-09T19:53:00+00:00; +4m27s from s
| ssl-cert: Subject: commonName=ubuntu804-base.local
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELIN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubu
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
```

Findings & Recommendations

Based on the network scan analysis, several critical vulnerabilities and security gaps require immediate attention to protect your infrastructure.

Update Services

Upgrade outdated FTP, Apache, and MySQL versions to patch known exploits and security vulnerabilities.

Disable Anonymous FTP

Remove anonymous FTP login capabilities immediately to prevent unauthorized file access and uploads.

Remove Backdoor

Eliminate the shell on port 1524 and conduct a forensic investigation to identify the compromise source.

01

Restrict phpMyAdmin access using IP whitelisting and strong authentication

02

Disable insecure SSLv2 protocol in SMTP configurations

03

Deploy firewall rules and implement strict access controls for sensitive ports

04

Perform verification scan after remediation to confirm successful mitigation

Zenmap GUI Overview

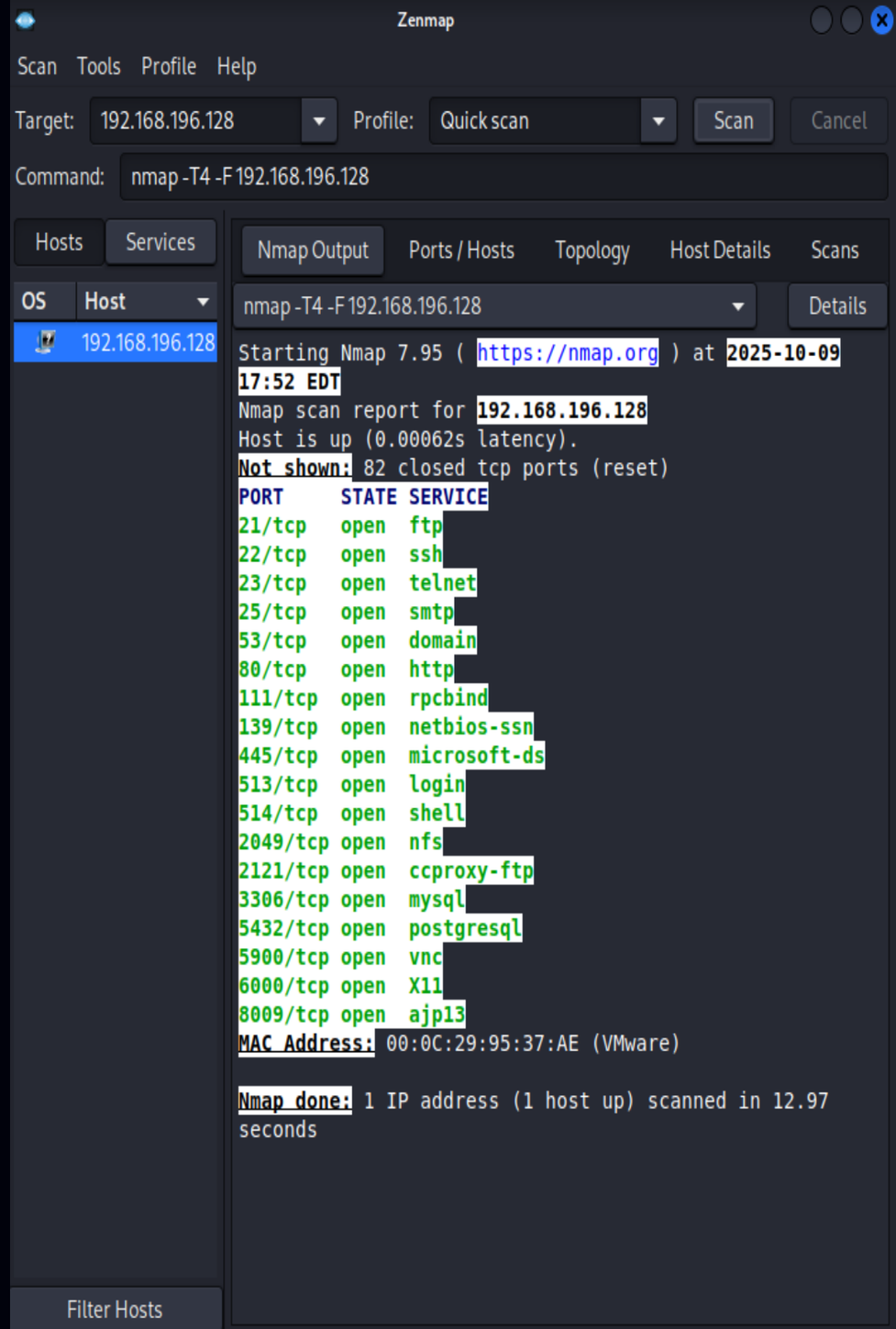
Zenmap provides an intuitive graphical interface for Nmap, making network scanning accessible to security professionals who prefer visual workflows over command-line operations.

Key Features

- Visual representation of scan results with interactive network topology maps
- Profile editor for saving custom scan configurations
- Comparison tool to track changes between multiple scans
- Search functionality to filter and analyze large datasets efficiently

Installation

```
sudo apt install zenmap
```



Results Summary

The comprehensive Nmap scan successfully mapped the target network infrastructure, revealing critical security insights and actionable intelligence for remediation.

Port & Service Discovery

Enumerated all open ports and identified running services, including FTP (21), SSH (22), HTTP (80), MySQL (3306), and suspicious backdoor on port 1524.

Vulnerability Detection

Discovered outdated software versions with known CVEs, anonymous FTP access, insecure SSLv2 protocol, and unrestricted phpMyAdmin exposure.

OS Fingerprinting

Successfully identified operating system details, kernel version, and network stack characteristics through advanced TCP/IP fingerprinting techniques.

Documentation & Reporting

Generated comprehensive reports with actionable security recommendations, ready for stakeholder review and remediation planning.

Conclusion

1

Nmap's Role in Security

Nmap remains the industry-standard tool for network discovery and security auditing, trusted by professionals worldwide for reconnaissance and vulnerability assessment.

2

Real-World Application

This project demonstrated practical usage of Nmap for identifying security weaknesses, mapping network topology, and generating actionable intelligence for defense teams.

3

Ongoing Vigilance

Regular network scans, timely security updates, and continuous monitoring are essential practices for maintaining robust defenses against evolving cyber threats.

Pro Tip: Schedule automated Nmap scans weekly to detect unauthorized changes and maintain a baseline of your network security posture.

THANK YOU