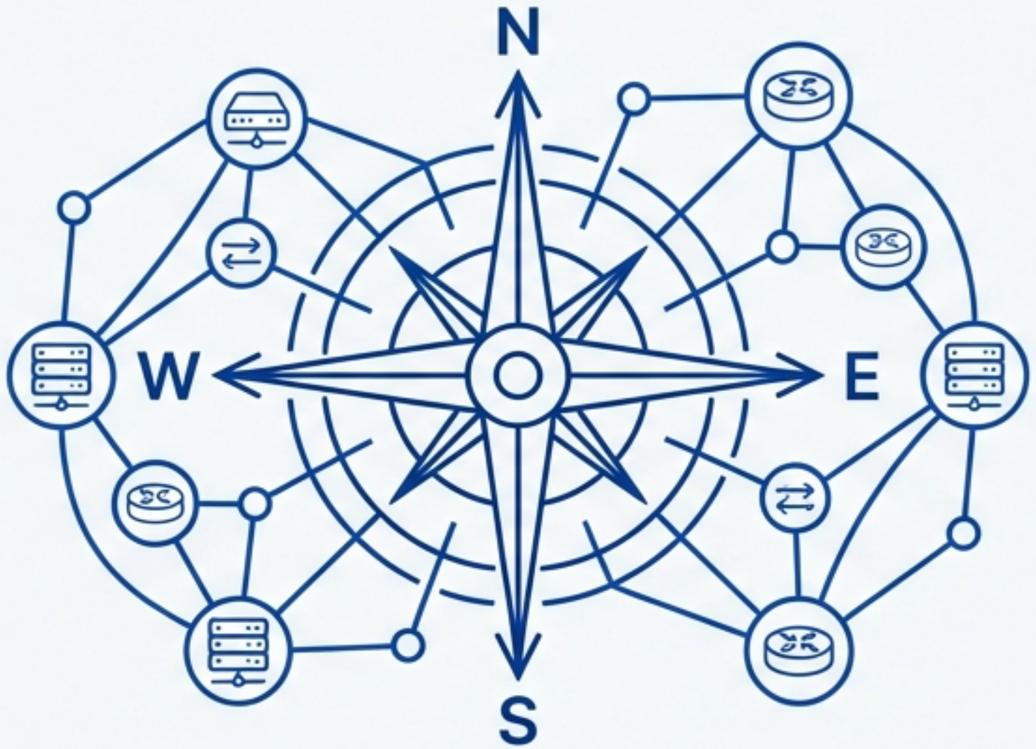
From Explorer to Cartographer
Mastering Network Visibility with Nmap



A practical guide to discovering, auditing,
and mapping network landscapes.

Vaithee

Your Essential Toolkit: What is Nmap?

Nmap (Network Mapper) is a free and open-source utility for network discovery and security auditing. It is one of the most widely used network scanning tools worldwide.

Created by Gordon Lyon ("Fyodor") and first released in *Phrack* magazine on 1 September 1997.

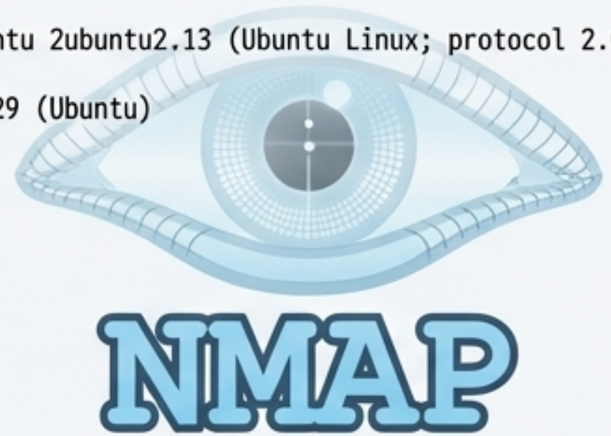
Core Capabilities

- **Host Discovery:** Finding active devices on a network.
- **Port Scanning:** Identifying open TCP/UDP ports.
- **Service & Version Detection:** Determining what software is running on open ports.
- **OS Fingerprinting:** Identifying the operating system of a target.
- **Nmap Scripting Engine (NSE):** Extending functionality with custom scripts for tasks like vulnerability detection.

```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-10 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not shown): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports

PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.6p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http    Apache httpd 2.4.29 (Ubuntu)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap
1068/tcp filtered instl_bootc
4444/tcp filtered krb524
4444/tcp filtered
5800/tcp filtered vnc-http
5900/tcp filtered vnc
9929/tcp  open    nping-echo Nping echo
31337/tcp open    tcpwrapped
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: 1 IP address (1 host up) scanned in 39.35 seconds
```



Vaithee

The Cartographer's Code: A Note on Ethical Use

Always use Nmap ethically and legally. Only scan networks you own or have explicit permission to test.

Why It Matters

- **Legality:** Unauthorised scanning can be a criminal offence.
- **Network Stability:** Aggressive scans can disrupt services.
- **Professional Integrity:** Upholding trust and responsibility is paramount in security work.

Common Legitimate Uses

- Network inventory and monitoring.
- Security assessments and penetration testing.
- Detecting unauthorised devices or open ports.

Chapter 1: Your First Landmark

Pinpointing and Analysing a Single Host

We begin by learning how to perform a detailed scan on a single target.
This is the foundational skill for all network mapping.

The Basic Scan: Identifying a Single Host

Objective: To perform a default scan against a single IP address or hostname, checking the 1,000 most common TCP ports.

Input: The Command

```
# By IP Address
nmap 192.168.1.100

# By Hostname
nmap example.com
```

Output: Understanding the Results

The port number and protocol (e.g., 22/tcp).

The current status of the port (e.g., open, closed, filtered).

The application or service likely running on the port.

```
Nmap scan report for 192.168.19.12
Host is up (0.0028s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1801/tcp  open   msmq
2103/tcp  open   zephyr-clt
2105/tcp  open   eklogin
2107/tcp  open   msmq-mgmt
3389/tcp  open   ms-wbt-server
5357/tcp  open   wsdapi
8000/tcp  open   http-alt
8089/tcp  open   unknown
MAC Address: 00:0C:29:D5:10:B1 (VMware)

Host script results:
|_ipidseq: Incremental!

Nmap done: 1 IP address (1 host up) scanned in 2.14 seconds
```

The Aggressive Scan: Uncovering Deeper Detail

To gather comprehensive information from a host, including OS, services, versions, and more.
This is the recommended scan for detailed reconnaissance.

```
nmap -T4 -A -v 192.168.1.100
```

nmap
The command to execute the Nmap program.

-T4
Timing Template. Sets timing to 'aggressive' (faster). A good balance between speed and reliability.

-A
Aggressive Scan. A powerful shortcut that enables OS detection (**-O**), version detection (**-sV**), script scanning (**-sC**), and traceroute (**--traceroute**).

-v
Verbose Output. Provides more detail about the scan as it progresses.

192.168.1.100
The Target. The IP address of the host you are scanning.

```
Starting Nmap 7.96 ( https://nmap.org ) at 2025-05-07 12:17 CDT
Nmap scan report for 192.168.1.100
Host is up (0.001s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|  ssh-hostkey: 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:20:34:97:6b:75 (DSA) ...
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
|_http-server-header: Apache/2.4.7 (Ubuntu)
3306/tcp  open  mysql   MySQL 5.5.62-0ubuntu0.14.04.1
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP  RTT     ADDRESS
 1   0.11 ms 192.168.1.100

Nmap done: 1 IP address (1 host up) scanned in 24.89 seconds
    Raw packets sent: 1004 (44.188KB) | Rcvd: 1004 (40.216KB)
```

Vaithee

Chapter 2: Charting the Territory

Discovering and **Scanning Entire Network Subnets**

From a single landmark, we now zoom out to **map the entire area**, identifying **all active hosts** within a network range.

Mapping the Subnet: From Discovery to Deep Scan

To scan an entire network, use CIDR notation (e.g., `192.168.1.0/24`) to specify the IP address range.

Scan Type 1: Quick Discovery (Ping Scan)

Objective

Quickly find all live hosts on the network without port scanning them. Ideal for initial inventory.

```
nmap -sn 192.168.1.0/24
```

Explanation

The `-sn` flag tells Nmap to perform a 'ping scan'—disabling port scanning and only reporting on which hosts responded.

Scan Type 2: Aggressive Network Scan

Objective

Perform a detailed, aggressive scan on every live host found in the subnet.

```
nmap -T4 -A 192.168.1.0/24
```

Explanation

This applies the same powerful `-A` flag from the single-host scan to the entire network.

Important Note:

Scanning a full network, especially with `-A`, can generate significant traffic. Always be mindful of network load.

Vaithee

Chapter 3: Refining the Map

Focusing Your Scans on Specific Ports

A true cartographer knows what to look for. Here, we learn to focus our scans on specific ports to quickly verify services or investigate points of interest.

The Art of Precision: Targeting Ports

Objective: To scan only specific ports or port ranges, making scans faster and more focused.

The `-p` flag is your primary tool for defining which ports Nmap will scan.

Example 1: A Single Port

Check if a web server is running.

```
nmap -p 80 example.com
```

Example 2: A Range of Ports

Scan the first 1024 “well-known" ports.

```
nmap -p 1-1024 192.168.1.100
```

Example 3: Multiple Specific Ports

Check for common administrative services.

```
nmap -p 22,80,443,3389 192.168.1.100
```

```
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  closed https
3389/tcp closed ms-wbt-server
```

Example 4: All Ports

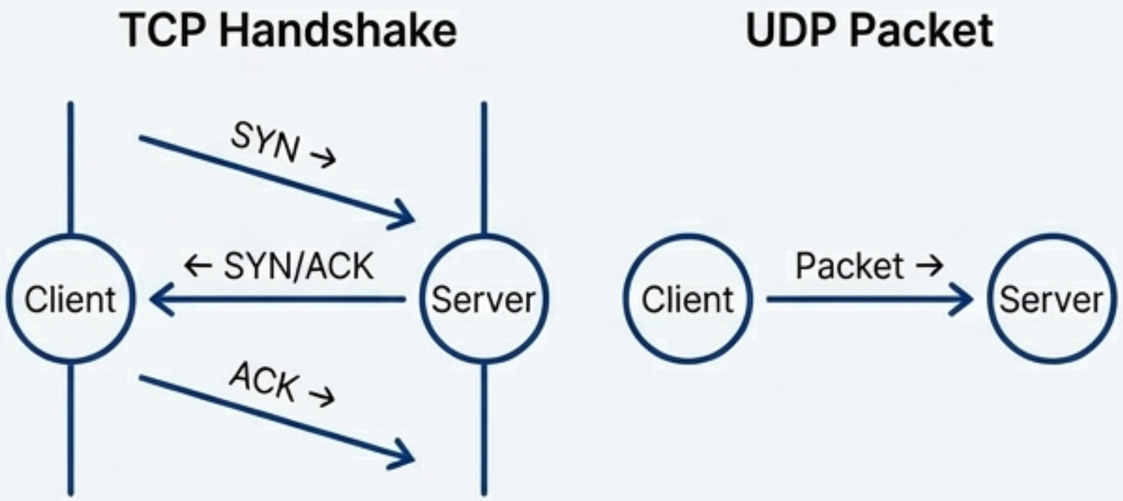
A very thorough but slow scan of all 65,535 TCP ports.

```
nmap -p- 192.168.1.100
```

Vaithee

Beyond TCP: Scanning for UDP Services

Key concept: While most common services use TCP, some critical services (like DNS and DHCP) use UDP. Scanning for them requires a specific flag and is often slower.



The `-sU` Flag: Enabling UDP Scan

Single UDP Port

Check for a DNS server.

```
nmap -sU -p 53 192.168.1.100
```

Multiple UDP Ports

Check for common SNMP ports.

```
nmap -sU -p 161,162 192.168.1.100
```

Pro Tip

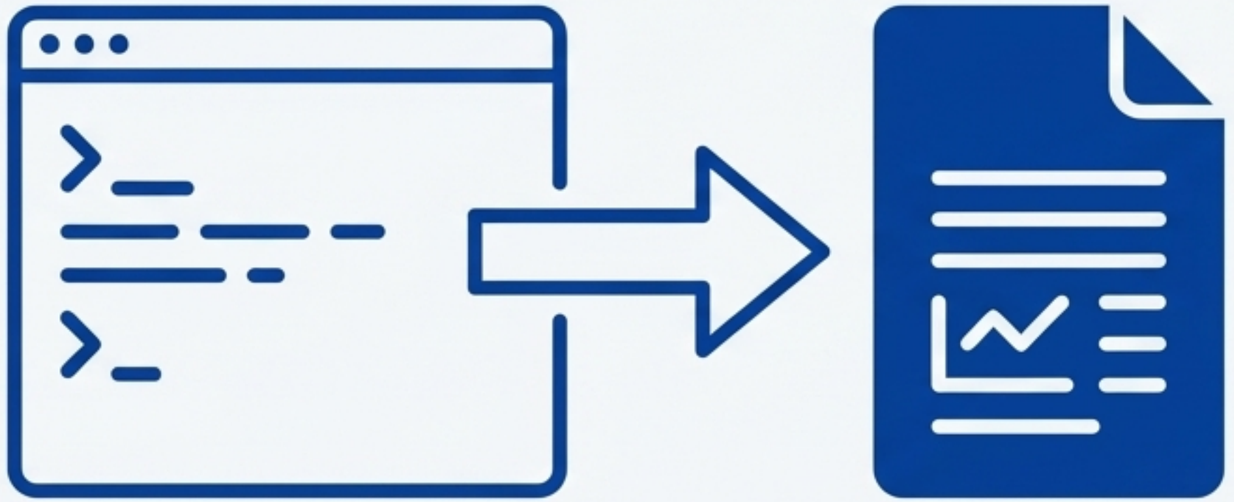
For best results, especially with SYN scans (the default TCP scan) or UDP scans, run Nmap with root privileges (`sudo nmap ...`).

Vaithee

Chapter 4: Publishing Your Atlas

Saving and Exporting Scan Results for Reporting

A map is only useful if it can be shared and understood. We'll now learn how to save scan data and convert it into a professional report.



The Professional Workflow: From XML to PDF Report

Nmap does not export directly to PDF. The recommended method is to save the results in the versatile XML format, convert to HTML, and then print the HTML to PDF from a browser.

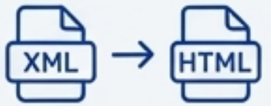
1 Save Scan Output as XML

Use the **-oX** flag to create a structured XML file containing all scan results.


```
nmap -A scanme.nmap.org -oX scan_results.xml
```

2 Convert XML to HTML

Use the **xsltproc** utility with Nmap's built-in stylesheet to generate a well-formatted HTML report.




```
xsltproc scan_results.xml -o scan_report.html
```

3 Print HTML to PDF

Open **scan_report.html** in any web browser and use the built-in print function (Ctrl+P) to 'Save as PDF'.

Pro Tip

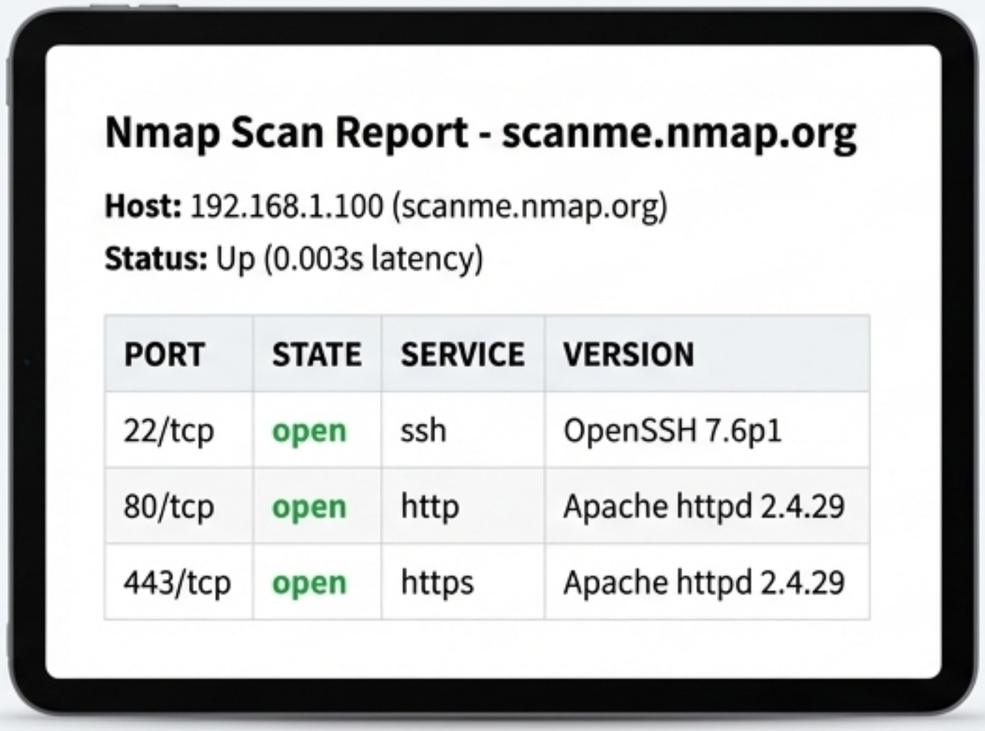
Use the **-oA <basename>** flag to save in all three major formats at once: Normal (.nmap), Grepable (.gnmap), and XML (.xml).

```
nmap -A 192.168.1.100 -oA scan_results
```

Vaithee

Your Network, Mapped and Understood

You have progressed from a simple explorer to a skilled network cartographer. With Nmap, you can transform the unknown complexity of a network into a clear, detailed, and actionable map.



Nmap Scan Report - scanme.nmap.org

Host: 192.168.1.100 (scanme.nmap.org)

Status: Up (0.003s latency)

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.6p1
80/tcp	open	http	Apache httpd 2.4.29
443/tcp	open	https	Apache httpd 2.4.29

Continuing the Journey

This guide covers the fundamentals. For advanced techniques, explore the Nmap Scripting Engine (NSE) and graphical front-ends like Zenmap.

The official documentation at **nmap.org** is the definitive resource for every command and option.

A good map is the foundation of all strategy.

Vaithee