

Forum:[Hack Forums](#)

Thread: [Nmap Usage Tutorial: A Comprehensive Guide for Network Scanning](#)

Imadmin - July 16, 2026, 8:34 pm

Abstract: Nmap (Network Mapper) is a free, open-source network exploration and security auditing tool widely used by network administrators, security professionals, and penetration testers. This report provides a detailed tutorial on Nmap, covering its basic introduction, installation, core scanning commands, advanced usage techniques, and safety precautions. By the end of this tutorial, readers will be able to use Nmap proficiently for network discovery, port scanning, service detection, and operating system identification, laying a solid foundation for network management and security testing.

Keywords: Nmap; Network Scanning; Port Detection; Security Auditing; Command Tutorial

1. Introduction to Nmap

Nmap was developed by Gordon Lyon (also known as Fyodor) and first released in 1997. It is designed to scan large networks efficiently while also being suitable for single-host scanning. Nmap works by sending raw IP packets to target hosts and analyzing the returned responses to gather detailed network information, including:

- Identifying live hosts on the network (host discovery)
- Detecting open ports on target hosts and the corresponding services running on those ports
- Determining the operating system (OS) and its version running on target hosts
- Detecting firewall and packet filter configurations on the network
- Performing vulnerability scanning with the help of Nmap Scripting Engine (NSE)

Nmap is cross-platform, supporting operating systems such as Linux, Windows, macOS, and BSD. It is widely used in network troubleshooting, security assessment, and penetration testing due to its flexibility, accuracy, and rich feature set.

2. Installation of Nmap

2.1 Installation on Linux

Nmap is pre-installed on most popular penetration testing distributions like Kali Linux, Parrot Security OS, and BackBox. For other Linux distributions, it can be installed via the package manager:

For Debian/Ubuntu-based systems:

```
sudo apt update && sudo apt install nmap
```

For Red Hat/CentOS/Fedora systems:

```
sudo yum install nmap
```

For Arch Linux:

```
sudo pacman -S nmap
```

2.2 Installation on Windows

1. Download the latest Windows installer from the official Nmap website .

2. Run the installer and follow the on-screen instructions. It is recommended to install the Nmap GUI (Zenmap) together for easier operation, especially for beginners.

3. After installation, add the Nmap installation directory (usually C:\Program Files (x86)\Nmap) to the system environment variables to run Nmap commands directly from the Command Prompt or PowerShell.

2.3 Installation on macOS

Nmap can be installed on macOS using Homebrew, a popular package manager:

```
brew install nmap
```

Alternatively, download the macOS installer from the official website and install it manually.

3. Basic Nmap Scanning Commands

Before using Nmap, it is important to note that unauthorized scanning of networks or hosts may

violate local laws and regulations. Always obtain proper permission from the network owner before performing any scanning operations.

3.1 Host Discovery

Host discovery is the process of identifying which hosts are active on the target network. The default Nmap scan includes host discovery, but users can also perform standalone host discovery with specific commands.

1. Basic host discovery for a single IP address:

```
nmap 192.168.1.1
```

This command sends ICMP echo requests, TCP SYN packets to port 443, TCP ACK packets to port 80, and ICMP timestamp requests to detect if the host 192.168.1.1 is active.

2. Host discovery for a network range:

```
nmap 192.168.1.0/24
```

This command scans all hosts in the 192.168.1.0/24 network segment to find active hosts.

3. Skip host discovery and scan all specified hosts (useful when the target host blocks ICMP requests):

```
nmap -Pn 192.168.1.1
```

3.2 Port Scanning

Port scanning is one of the core functions of Nmap, used to detect open ports on target hosts. Ports are divided into three states: open (a service is running and listening on the port), closed (no service is running on the port), and filtered (the port is blocked by a firewall or packet filter, and Nmap cannot determine its state).

1. Basic port scan (scans the 1000 most common ports):

```
nmap -p- 192.168.1.1
```

The "-p-" option scans all 65535 TCP ports, which is more comprehensive but takes longer. For a specific port range, use "-p 1-1000" to scan ports 1 to 1000.

2. Scan specific ports:

```
nmap -p 22,80,443,3306 192.168.1.1
```

This command scans only ports 22 (SSH), 80 (HTTP), 443 (HTTPS), and 3306 (MySQL) on the target host.

3. TCP SYN scan (the default scan type for privileged users, fast and stealthy):

```
nmap -sS 192.168.1.1
```

TCP SYN scan sends a SYN packet to the target port. If a SYN-ACK packet is returned, the port is open; if a RST packet is returned, the port is closed. This scan does not complete the TCP three-way handshake, making it less likely to be detected by intrusion detection systems (IDS).

4. TCP connect scan (suitable for non-privileged users, completes the TCP three-way handshake):

```
nmap -sT 192.168.1.1
```