

# Kurzanleitung zur Installation und Verwendung des Portscanners nmap

**Achtung: Das Scannen fremder Rechner mit Werkzeugen wie nmap ist rechtlich umstritten und wird von vielen Netzbetreibern bereits als (illegaler) Hackingversuch aufgefasst und entsprechend verfolgt. Die Anwendung in eigenen Netzen (wie im Schulbuch beschrieben) ist unproblematisch; fremde im Internet erreichbare Rechner bzw. Netze dürfen mit nmap jedoch nicht gescannt werden! Dabei sollte auch beachtet werden, dass bereits ein einfacher Tippfehler bei der Eingabe des Zielnetzes zu einem rechtlich problematischen Scan fremder Netze führen kann. Hier muss also mit besonderer Sorgfalt gearbeitet werden!**

## 1. Installation

nmap ist ein Open-Source-Werkzeug und für verschiedene Betriebssysteme kostenlos aus dem Internet herunterladbar. Zu beachten ist, dass für die Installation und zum Teil auch die anschließende Nutzung unter allen drei im folgenden genannten Betriebssystemen in der Regel Administratorrechte benötigt werden.

### Windows

Für Windows bietet sich der Download der Installer-Version an, welche einen Installationsassistenten enthält, um nmap auf dem System einzurichten. Dabei werden neben nmap selbst ggf. auch noch weitere Hilfsprogramme/Treiber installiert, die für den vollen Funktionsumfang von nmap benötigt werden.

Das direkte Ausführen der nmap-Anwendung ohne vorherige Installation ist ebenfalls möglich, bietet aus den eben genannten Gründen aber nur einen sehr eingeschränkten Funktionsumfang.

Um die unter 2. vorgeschlagenen Scanoperationen auszuführen, muss im Terminal zunächst in das Verzeichnis gewechselt werden, in welchem nmap installiert ist (oder nmap muss zur sog. PATH-Umgebungsvariable hinzugefügt werden → siehe Anleitung auf der nmap-Webseite).

### MacOS

Auch für MacOS wird ein fertiges Installationspaket zum Download angeboten. Je nach Betriebssystemversion kann es bei der Installation ggf. notwendig sein die Ausführung des Installationspakets in den Systemeinstellungen unter „Datenschutz und Sicherheit“ explizit zu erlauben. Nach erfolgreicher Installation steht nmap im Terminal unmittelbar zur Verfügung

### Linux

Bei den meisten Linux-Distributionen ist die Installation leicht über die jeweiligen Paketmanager möglich. Auch hier werden ggf. benötigte Abhängigkeiten automatisch mit installiert und der Befehl nmap steht nach der Installation direkt im Terminal zur Verfügung.

## 2. Beispiele zur Durchführung einfacher Portscans

Hinweis: Windowsnutzer müssen bei den folgenden Beispielbefehlen je nach Systemkonfiguration ggf. „nmap.exe“ statt „nmap“ verwenden.

### 2.1 Einen einfachen Portscan durchführen

Im einfachsten Fall, kann ein Portscan mit den Standardeinstellungen gestartet werden. Neben der Angabe des Ziels sind dann keine weiteren Parameter erforderlich.

Als Ziel kann entweder ein einzelner Rechner oder ein Subnetz (in CIDR-Notation) angegeben werden:

nmap 192.168.0.1	Scannt nur den Host 192.168.0.1
nmap 192.168.0.0/24	Scannt den IP-Bereich 192.168.0.0 – 192.168.0.255

Nach Abschluss des Scans gibt nmap einen Bericht nach folgendem Schema aus:

*Starting Nmap 7.97 ( <https://nmap.org> ) at 2025-06-12 09:29 +0200*

*Nmap scan report for 192.168.0.1*

*Host is up (0.023s latency).*

*Not shown: 999 closed tcp ports (conn-refused)*

*PORT STATE SERVICE*

*22/tcp open ssh*

*Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds*

Die Ausgabe besteht aus einem Header mit Metadaten zum durchgeführten Scan (hier rot hervorgehoben), je einem Bericht pro Host (hier blau), sowie einer Zusammenfassung (hier grün). Im gezeigten Beispiel ist der Host 192.168.0.1 erreichbar („Host is up“) und besitzt einen offenen Port, hier Port 22 („22/tcp open ssh“) Die Angabe, dass an Port 22 ein SSH-Dienst verfügbar ist, ist dabei lediglich eine Vermutung basierend auf der standardisierten Verwendung von Portnummern.

### 2.2 Scannen ohne Portscan (Ping-Scan)

Möchte man lediglich herausfinden, welche IP-Adressen in einem Subnetz aktiv von Rechnern genutzt werden, kann der Portscan, also das ermitteln der offenen Ports pro Rechner mittels des Parameters -sn übersprungen werden.

nmap -sn 192.168.0.0/24

Die Ausgabe erfolgt dann entsprechend verkürzt:

*Starting Nmap 7.97 ( <https://nmap.org> ) at 2025-06-12 09:29 +0200*

*Nmap scan report for 192.168.0.1*

*Host is up (0.024s latency).*

*Nmap done: 256 IP addresses (1 host up) scanned in 12.25 seconds*

### 2.3 Scannen bestimmter Portbereiche

Mit den Standardeinstellungen (siehe 2.1) scannt nmap nur 1000 der 65535 möglichen Ports. Soll ein bestimmter Port oder Portbereich gescannt werden, muss dies mittels des Parameters -p angegeben werden:

nmap -p 1337 192.168.0.1	Scannt den Port 1337
nmap -p 42,1335-1337 192.168.0.1	Scannt den Port 42 sowie den Portbereich 1335-1337

## 2.4 Scannen von Hosts, die nicht auf ICMP-Pings antworten

Vor einem weitergehenden Portscan prüft nmap in der Regel, ob der jeweilige Zielhost erreichbar ist. Manche Rechner (z. B. viele Windows-Rechner) sind aus Sicherheitsgründen jedoch so konfiguriert, dass die auf derartige Ping bzw. Echoanfragen nicht reagieren. Mit dem Parameter -Pn kann ein weitergehender Scan dennoch erzwungen werden.

```
nmap -Pn 192.168.0.1
```

## 2.5 Intensivscan durchführen

Sollen möglichst viele Informationen in einem Scandurchlauf zu sammeln kann der Parameter -A verwendet werden. Dies aktiviert unter anderem die Betriebssystem- und Versionserkennung und führt so zu einer detaillierteren Ausgabe. Ggf. kann es hier zudem hilfreich sein, den Scanbefehl als Administrator (bei Linux z. B. mit sudo) auszuführen. Trotz der teils sehr umfangreichen Ausgabe muss auch hier bedacht werden, dass die gewonnenen Informationen teilweise auf Schätzungen und Vermutungen beruhen und nicht zwingend der Realität entsprechen müssen.

```
nmap -A 192.168.0.1
```

*Neben den gezeigten Beispielen bietet nmap noch eine ganze Reihe weiterer Optionen und Parameter. Viele davon („Stealth-Scan“, „Xmas-Scan“, usw.) haben dabei explizit zum Ziel Firewalls zu umgehen oder eine Detektion des Scans zu vermeiden und sind damit für den im Schulbuch beschriebenen Anwendungsfall nicht relevant.*