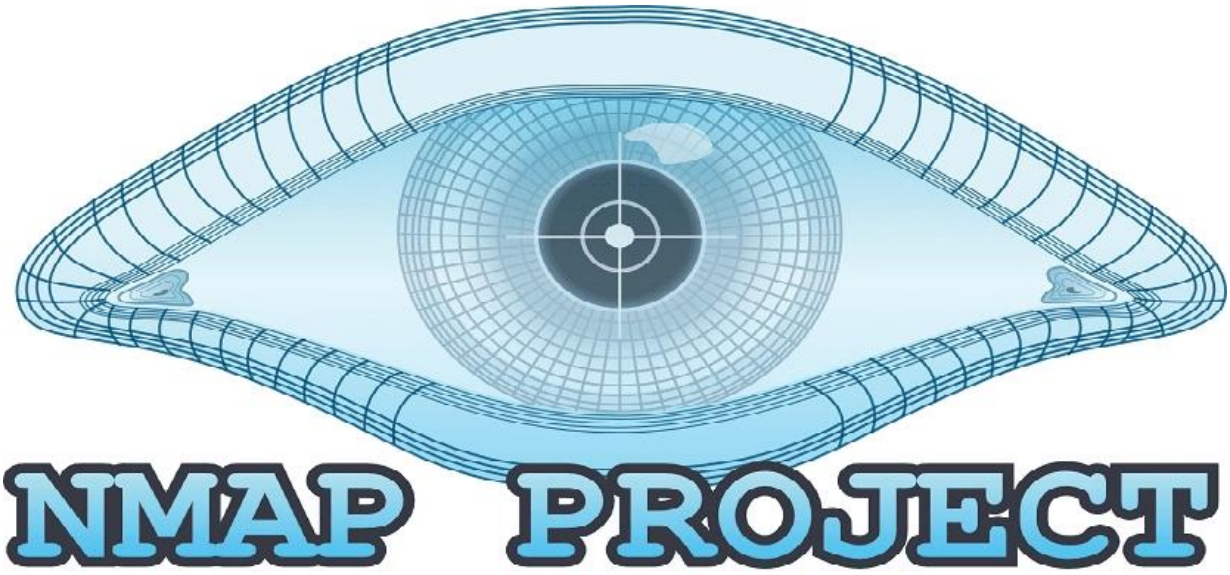
Nmap und Zenmap



Inhaltsverzeichnis

Nmap (Network Mapper) - Überblick

Nmap ist ein leistungsstarker, kostenloser Netzwerkscanner, der von Gordon Lyon (bekannt als Fyodor Vaskovich) entwickelt wurde. Als eines der wichtigsten Tools für Netzwerkadministratoren und Cybersecurity-Experten bietet Nmap vielseitige Funktionen zur Netzwerkanalyse und Sicherheitsbewertung.[1]

Kernfunktionen von Nmap

Host-Erkennung (Host Discovery)

Nmap identifiziert aktive Geräte im Netzwerk durch verschiedene Probentechniken:[2]

- ICMP-Pakete (Echo-Requests, Zeitstempel)
- ARP/ND-Requests für lokale Netzwerke
- TCP SYN/ACK-Pakete an ausgewählte Ports
- UDP-"Pings"
- SCTP INIT-Requests

Port-Scanning

Das Herzstück von Nmap ermittelt den Status von Ports auf Zielgeräten:[3][2]

- **Offene Ports**: Dienste nehmen Verbindungen an
- **Geschlossene Ports**: Keine aktiven Dienste
- **Gefilterte Ports**: Durch Firewalls blockiert

Service- und Versionserkennung

Nmap analysiert offene Ports und identifiziert:[2][1]

- Laufende Anwendungen und deren Versionen
- Spezifische Dienstinformationen
- Banner-Grabbing für detaillierte Service-Analyse

Betriebssystem-Erkennung

Durch TCP/IP-Stack-Fingerprinting ermittelt Nmap:[1][2]

- Betriebssystem-Typ und Version
- Hardware-Charakteristika
- Netzwerkgerät-Details

Nmap Scan-Techniken

TCP SYN Scan (-sS)

- Stealth-Scan ohne vollständige TCP-Verbindung
- Sendet SYN-Pakete und analysiert Antworten
- Standard-Scan-Methode für Privilegierte[4][3]

TCP Connect Scan (-sT)

- Vollständige TCP-Verbindung (3-Way-Handshake)
- Zuverlässig, aber weniger diskret
- Für unprivilegierte Benutzer[5][3]

UDP Scan (-sU)

- Erkennt UDP-Services
- Langsamer als TCP-Scans
- Kombinierbar mit TCP-Scans[6][7]

Spezielle Scan-Techniken:[8][5]

- **NULL Scan (-sN)**: Keine Flags gesetzt
- **FIN Scan (-sF)**: Nur FIN-Flag gesetzt
- **XMAS Scan (-sX)**: FIN, PSH, URG-Flags gesetzt
- **ACK Scan (-sA)**: Firewall-Regeln testen
- **Idle Scan (-sI)**: Stealth-Scan über "Zombie"-Host

Nmap Scripting Engine (NSE)

Die **NSE** erweitert Nmaps Grundfunktionen erheblich durch Lua-Skripte:[9][10][2]

NSE-Kategorien:[11][12][10]

- **auth**: Authentifizierungs-Tests
- **broadcast**: Broadcast-Requests im Netzwerk
- **brute**: Brute-Force-Angriffe
- **default**: Standard-Skript-Set
- **discovery**: Host- und Service-Erkennung
- **dos**: Denial-of-Service-Tests
- **exploit**: Exploit-Skripte

- **external**: Externe Services nutzen
- **fuzzer**: Fuzzing-Tests
- **intrusive**: Potentiell störende Tests
- **malware**: Malware-Erkennung
- **safe**: Sichere, nicht-störende Tests
- **version**: Erweiterte Versionserkennung
- **vuln**: Vulnerability-Scanner

NSE-Beispiele:[13][14][15]

```
# Vulnerability-Scans
nmap --script=vuln target.com

# SMB-Enumeration
nmap --script=smb-enum-shares 192.168.1.1

# Web-Vulnerability-Tests
nmap --script=http-vuln-* example.com

# Brute-Force-Tests
nmap --script=snmp-brute 192.168.1.1
```

Erweiterte Nmap-Commands für Penetration Testing:[16][7][17]

```
# Aggressive Scan mit OS-Detection
nmap -A -T4 192.168.1.0/24

# Stealth-Scan mit Service-Detection
nmap -sS -sV -O target.com

# Alle TCP-Ports scannen
nmap -p 1-65535 target.com

# Firewall-Evasion
nmap -f -D RND:10 --source-port 53 target.com

# Script-Scan mit Vulnerability-Detection
nmap -sC --script=vuln target.com
```

Zenmap - Grafische Benutzeroberfläche

Zenmap ist die offizielle grafische Benutzeroberfläche für Nmap. Es macht Nmap für Anfänger zugänglich und bietet erfahrenen Nutzern erweiterte Funktionen.[18][19][20]

Hauptfunktionen von Zenmap

Benutzerfreundliche GUI:[21][22][18]

- Interaktive Scan-Erstellung ohne Kommandozeile
- Dropdown-Menüs für Scan-Optionen
- Echtzeit-Anzeige der generierten Nmap-Befehle
- Plattformübergreifend (Windows, Linux, macOS)

Scan-Profile:[23][24]

- Vordefinierte Scan-Templates
- Quick Scan, Regular Scan, Intense Scan
- Custom Profile-Erstellung
- Profile-Export und -Import zwischen Benutzern

Ergebnisvisualisierung:[25][24][18]

- **Ports/Hosts-Tabs**: Übersichtliche Port- und Service-Anzeige
- **Host Details**: Detaillierte Informationen pro Host
- **Scan-History**: Verlauf aller durchgeführten Scans
- **Services-Ansicht**: Gruppierung nach Services

Netzwerk-Topologie:[24][18][25]

- Grafische Netzwerkkarten
- Zoom-Funktionen für bessere Übersicht
- Farbcodierung nach Host-Status:
    - Grün: Weniger als 3 offene Ports
    - Gelb/Orange: Moderate Anzahl Ports
    - Rot: Viele offene Ports

Erweiterte Zenmap-Features

Scan-Vergleich:[22][18][23]

- Vergleich zwischen verschiedenen Scans

- Erkennung von Änderungen im Netzwerk
- Neue oder verschwundene Hosts/Services
- Zeitbasierte Netzwerküberwachung

Suchfunktionen:[18][25]

- Durchsuchbare Scan-Datenbank
- Filter nach Hosts, Ports, Services
- Pattern-Matching für spezielle Suchen
- Ergebnisexport in verschiedene Formate

Import/Export-Funktionen:[24][18]

- XML-Import von Nmap-Scans
- Scan-Ergebnisse speichern und laden
- Profile-Sharing zwischen Benutzern
- Integration in andere Security-Tools

Installation und Grundlegende Nutzung

Nmap Installation:[26]

```
# Linux (Debian/Ubuntu)
sudo apt update
sudo apt install nmap

# Arch Linux
sudo pacman -S nmap

# CentOS/RHEL
sudo yum install nmap
```

Zenmap Installation:[27][28]

```
# Kali Linux (moderne Versionen)
sudo apt update
sudo apt install zenmap

# Ältere Systeme - über RPM conversion
wget [zenmap-rpm-url]
sudo alien zenmap-*.rpm
```

```
sudo dpkg -i zenmap-*.deb
```

Grundlegende Zenmap-Bedienung:[29][25][23]

1. **Target eingeben**: IP-Adresse oder Hostname
2. **Profile auswählen**: Quick Scan, Regular Scan, etc.
3. **Scan starten**: Button "Scan" klicken
4. **Ergebnisse analysieren**: Ports/Hosts-Tabs verwenden
5. **Topologie betrachten**: Netzwerk-Visualisierung nutzen

Nmap vs. Zenmap - Vergleich:[30][21][22]

Aspekt	Nmap	Zenmap
Interface	Kommandozeile	Grafische Oberfläche
Lernkurve	Steiler für Anfänger	Anfängerfreundlich
Flexibilität	Maximale Kontrolle	Guided Interface
Performance	Ressourcenschonend	Höherer Speicherbedarf
Automation	Skript-Integration	GUI-basierte Profiles
Portabilität	Minimal Dependencies	GUI-Dependencies
Netzwerk-Visualisierung	Keine	Topologie-Karten
Ergebnisvergleich	Manuell	Integrierte Funktion

Best Practices und Sicherheitshinweise

Rechtliche Aspekte:[16][1]

- Nur auf eigenen Netzwerken verwenden
- Schriftliche Genehmigung für Penetration Tests
- Compliance mit lokalen Gesetzen beachten
- Dokumentation aller Aktivitäten

Ethische Nutzung:

- White-Hat-Hacking für Sicherheitsverbesserungen
- Responsible Disclosure bei gefundenen Schwachstellen

- Keine unauthorisierten Scans auf fremden Systemen
- Respektierung von Netzwerk-Policies

Performance-Optimierung:[31][6]

```
# Timing-Templates für verschiedene Szenarien
nmap -T1  # Paranoid (sehr langsam)
nmap -T2  # Sneaky (langsam)
nmap -T3  # Normal (Standard)
nmap -T4  # Aggressive (schnell)
nmap -T5  # Insane (sehr schnell)
```

Firewall-Evasion:[8][31]

```
# Fragment-Pakete
nmap -f target.com

# Decoy-Scans
nmap -D RND:10 target.com

# Source-Port-Spoofing
nmap --source-port 53 target.com
```

Sowohl Nmap als auch Zenmap sind unverzichtbare Tools für Netzwerkadministration und Cybersecurity. Während Nmap maximale Kontrolle und Effizienz bietet, erleichtert Zenmap den Einstieg und bietet wertvolle Visualisierungsfunktionen für komplexe Netzwerkanalysen.

Syntaxliste mit Beispielanwendungen

Grundlegende Ziel-Spezifikation

Einzelziele und Zielbereiche

Syntax	Beispiel	Beschreibung
nmap [Ziel]	nmap 192.168.1.1	Einzelnes Ziel scannen
nmap [Ziel1,Ziel2]	nmap 192.168.1.1,192.168.1.5	Mehrere spezifische Ziele
nmap [IP-Bereich]	nmap 192.168.1.1-10	IP-Bereich scannen
nmap [CIDR]	nmap 192.168.1.0/24	Gesamtes Subnetz scannen
nmap -iL [Datei]	nmap -iL targets.txt	Zielliste aus Datei laden
nmap -iR [Anzahl]	nmap -iR 100	Zufällige Hosts scannen
nmap --exclude [Ziele]	nmap 192.168.1.0/24 --exclude 192.168.1.1	Bestimmte Hosts ausschließen
nmap --excludefile [Datei]	nmap 192.168.1.0/24 --excludefile exclude.txt	Ausschluss-Hosts aus Datei

Port-Spezifikation

Port-Auswahl

Syntax	Beispiel	Beschreibung
nmap -p [Port]	nmap -p 80 192.168.1.1	Einzelnen Port scannen
nmap -p [Start]-[Ende]	nmap -p 80-443 192.168.1.1	Port-Bereich scannen
nmap -p-	nmap -p- 192.168.1.1	Alle 65535 Ports scannen

nmap -p [Protokoll]:[Ports]	nmap -p T:80,U:53 192.168.1.1	TCP- und UDP-Ports spezifizieren
nmap --top-ports [Anzahl]	nmap --top-ports 1000 192.168.1.1	Die häufigsten N Ports scannen
nmap -F	nmap -F 192.168.1.1	Fast-Scan (100 häufigste Ports)

Beispiel-Anwendung:

Webserver-Ports auf mehreren Hosts scannen
nmap -p 80,443,8080,8443 192.168.1.1-50

Alle TCP- und UDP-Ports auf kritischem Server
nmap -p T:1-65535,U:1-1000 192.168.1.10

Scan-Techniken

TCP-Scans

Syntax	Beispiel	Beschreibung
nmap -sS	nmap -sS 192.168.1.1	**SYN-Scan** (Stealth, Standard)
nmap -sT	nmap -sT 192.168.1.1	**TCP Connect-Scan** (vollständige Verbindung)
nmap -sA	nmap -sA 192.168.1.1	**ACK-Scan** (Firewall-Erkennung)
nmap -sW	nmap -sW 192.168.1.1	**Window-Scan** (Firewall-Analyse)
nmap -sF	nmap -sF 192.168.1.1	**FIN-Scan** (Stealth-Technik)
nmap -sN	nmap -sN 192.168.1.1	**NULL-Scan** (keine Flags gesetzt)
nmap -sX	nmap -sX 192.168.1.1	**Xmas-Scan** (FIN, PSH, URG)

UDP und andere Scans

Syntax	Beispiel	Beschreibung
nmap -sU	nmap -sU 192.168.1.1	**UDP-Scan**
nmap -sO	nmap -sO 192.168.1.1	**IP-Protokoll-Scan**
nmap -sI [Zombie]	nmap -sI 192.168.1.5 192.168.1.1	**Idle-Scan** (über Zombie-Host)

Beispiel-Anwendung:

Stealth-Scan für Firewall-Umgehung
nmap -sF -T1 192.168.1.1

Kombinierter TCP/UDP-Scan für DNS-Server

```
nmap -sS -sU -p T:53,U:53 192.168.1.10
```

Host-Erkennung (Discovery)

Ping-Techniken

Syntax	Beispiel	Beschreibung
nmap -sn	nmap -sn 192.168.1.0/24	**Ping-Scan** (nur Host-Erkennung)
nmap -Pn	nmap -Pn 192.168.1.1	**Kein Ping** (Host als online behandeln)
nmap -PS [Ports]	nmap -PS80,443 192.168.1.1	**TCP SYN-Ping**
nmap -PA [Ports]	nmap -PA80,443 192.168.1.1	**TCP ACK-Ping**
nmap -PU [Ports]	nmap -PU53,123 192.168.1.1	**UDP-Ping**
nmap -PE	nmap -PE 192.168.1.1	**ICMP Echo-Ping**
nmap -PP	nmap -PP 192.168.1.1	**ICMP Timestamp-Ping**
nmap -PM	nmap -PM 192.168.1.1	**ICMP Address Mask-Ping**
nmap -PR	nmap -PR 192.168.1.0/24	**ARP-Ping** (nur lokales Netzwerk)

Beispiel-Anwendung:

```
# Schnelle Netzwerk-Inventarisierung
nmap -sn -PR 192.168.1.0/24

# Host-Discovery hinter Firewall
nmap -PS21,22,23,25,53,80,110,443,993,995 192.168.1.0/24
```

Service- und Version-Erkennung

Detaillierte Analyse

Syntax	Beispiel	Beschreibung
nmap -sV	nmap -sV 192.168.1.1	**Service-Version-Erkennung**
nmap -O	nmap -O 192.168.1.1	**Betriebssystem-Erkennung**
nmap -A	nmap -A 192.168.1.1	**Aggressive Erkennung** (OS, Service, Scripts, Traceroute)
nmap --osscan-guess	nmap -O --osscan-guess 192.168.1.1	OS-Erkennung mit Schätzung
nmap --version-intensity [0-9]	nmap -sV --version-intensity 9 192.168.1.1	Intensität der Version-Erkennung
nmap --version-light	nmap -sV --version-light 192.168.1.1	Leichte Version-Erkennung
nmap --version-all	nmap -sV --version-all 192.168.1.1	Alle Probes für Version-Erkennung

Beispiel-Anwendung:

Vollständige Systemanalyse
nmap -A -T4 192.168.1.10

Detaillierte Service-Fingerprinting
nmap -sV --version-intensity 9 -p- 192.168.1.5

NSE Scripts (Nmap Scripting Engine)

Script-Kategorien

Syntax	Beispiel	Beschreibung
nmap --script default	nmap --script default 192.168.1.1	Standard-Scripts ausführen
nmap --script vuln	nmap --script vuln 192.168.1.1	**Vulnerability-Scripts**
nmap --script exploit	nmap --script exploit 192.168.1.1	**Exploit-Scripts**
nmap --script auth	nmap --script auth 192.168.1.1	**Authentifizierung-Scripts**
nmap --script brute	nmap --script brute 192.168.1.1	**Brute-Force-Scripts**
nmap --script discovery	nmap --script discovery 192.168.1.1	**Discovery-Scripts**
nmap --script safe	nmap --script safe 192.168.1.1	**Sichere Scripts** (nicht-intrusiv)
nmap --script intrusive	nmap --script intrusive 192.168.1.1	**Intrusive Scripts**

Spezifische Scripts

Syntax	Beispiel	Beschreibung
nmap --script [Script-Name]	nmap --script http-title 192.168.1.1	Einzelnes Script ausführen
nmap --script "vuln,exploit"	nmap --script "vuln,exploit" 192.168.1.1	Mehrere Kategorien kombinieren
nmap --script vulners	nmap --script vulners 192.168.1.1	**CVE-Erkennung** über Vulners.com API

nmap --script smb-vuln-*	nmap --script smb-vuln-* 192.168.1.1	Alle SMB-Vulnerability-Scripts
nmap --script ssl-*	nmap --script ssl-* -p 443 192.168.1.1	SSL/TLS-Analyse Scripts

Beispiel-Anwendung:

```
# Umfassende Vulnerability-Analyse
nmap -sV --script "vuln,exploit,auth" 192.168.1.10

# Web-Anwendung Sicherheitsprüfung
nmap --script "http-*" -p 80,443 192.168.1.5

# SMB-Schwachstellen prüfen (EternalBlue etc.)
nmap --script smb-vuln-* -p 445 192.168.1.1-50
```

Timing und Performance

Timing-Templates

Syntax	Beispiel	Beschreibung
nmap -T0	nmap -T0 192.168.1.1	**Paranoid** (sehr langsam, IDS-Umgehung)
nmap -T1	nmap -T1 192.168.1.1	**Sneaky** (langsam, IDS-Umgehung)
nmap -T2	nmap -T2 192.168.1.1	**Polite** (weniger Bandbreite)
nmap -T3	nmap -T3 192.168.1.1	**Normal** (Standard)
nmap -T4	nmap -T4 192.168.1.1	**Aggressive** (schnell, zuverlässiges Netzwerk)
nmap -T5	nmap -T5 192.168.1.1	**Insane** (sehr schnell, kann ungenau sein)

Erweiterte Performance-Optionen

Syntax	Beispiel	Beschreibung
nmap --min-parallelism [n]	nmap --min-parallelism 100 192.168.1.0/24	Mindestanzahl paralleler Probes
nmap --max-parallelism [n]	nmap --max-parallelism 10 192.168.1.1	Maximale Anzahl paralleler Probes
nmap --scan-delay [Zeit]	nmap --scan-delay 1s 192.168.1.1	Verzögerung zwischen Probes
nmap --max-scan-delay [Zeit]	nmap --max-scan-delay 2s 192.168.1.1	Maximale Scan-Verzögerung

Beispiel-Anwendung:

```
# Langsamer Stealth-Scan
nmap -sS -T1 --scan-delay 5s 192.168.1.1

# Schneller Netzwerk-Scan
nmap -T4 --min-parallelism 50 192.168.1.0/24
```

Firewall- und IDS-Umgehung

Fragmentierung und Spoofing

Syntax	Beispiel	Beschreibung
nmap -f	nmap -f 192.168.1.1	**Paket-Fragmentierung**
nmap --mtu [Größe]	nmap --mtu 16 192.168.1.1	Spezifische MTU-Größe
nmap -D [Decoys]	nmap -D 8.8.8.8,8.8.4.4,ME 192.168.1.1	**Decoy-Scan** (Köder-IPs)
nmap -D RND:[Anzahl]	nmap -D RND:10 192.168.1.1	Zufällige Decoy-IPs
nmap --source-port [Port]	nmap --source-port 53 192.168.1.1	Quell-Port spezifizieren
nmap --data-length [Bytes]	nmap --data-length 25 192.168.1.1	Zufällige Daten anhängen
nmap --spoof-mac [MAC]	nmap --spoof-mac 0 192.168.1.1	MAC-Adresse spoofing
nmap --badsum	nmap --badsum 192.168.1.1	Fehlerhafte Checksummen senden

Kombinierte Evasion-Techniken

Syntax	Beispiel	Beschreibung
nmap --randomize-hosts	nmap --randomize-hosts 192.168.1.1-50	Zufällige Host-Reihenfolge
nmap --packet-trace	nmap --packet-trace 192.168.1.1	Paket-Details anzeigen

Beispiel-Anwendung:

```
# Maximale Stealth-Konfiguration
nmap -f -T1 -D RND:10 --source-port 53 --data-length 25 192.168.1.1

# Firewall-Bypass mit Fragmentierung
nmap -f --mtu 8 -sF 192.168.1.1
```

Output-Formate

Standard-Output-Optionen

Syntax	Beispiel	Beschreibung
nmap -oN [Datei]	nmap -oN scan.txt 192.168.1.1	**Normal-Output** (lesbar)
nmap -oX [Datei]	nmap -oX scan.xml 192.168.1.1	**XML-Output** (strukturiert)
nmap -oG [Datei]	nmap -oG scan.grep 192.168.1.1	**Grepable-Output** (für Scripts)
nmap -oS [Datei]	nmap -oS scan.skid 192.168.1.1	Script-Kiddie-Output
nmap -oA [Basis]	nmap -oA scan 192.168.1.1	**Alle Formate** (scan.nmap, scan.xml, scan.gnmap)

Erweiterte Output-Optionen

Syntax	Beispiel	Beschreibung
nmap -v	nmap -v 192.168.1.1	**Verbose** (mehr Details)
nmap -vv	nmap -vv 192.168.1.1	Sehr verbose
nmap -d	nmap -d 192.168.1.1	**Debug-Modus**
nmap --reason	nmap --reason 192.168.1.1	Begründung für Port-Status
nmap --open	nmap --open 192.168.1.1	Nur offene Ports anzeigen

nmap --append-output	nmap --append-output -oN scan.txt 192.168.1.1	An Datei anhängen

Beispiel-Anwendung:

Vollständige Dokumentation
nmap -A -oA complete-scan --reason --open 192.168.1.0/24

Detaillierter Verbose-Scan
nmap -sS -sV -vv --reason -oN verbose-scan.txt 192.168.1.1

DNS und Reverse-Lookup

DNS-Optionen

Syntax	Beispiel	Beschreibung
nmap -n	nmap -n 192.168.1.1	**Keine DNS-Auflösung**
nmap -R	nmap -R 192.168.1.1	**Reverse DNS erzwingen**
nmap --dns-servers [Server]	nmap --dns-servers 8.8.8.8 192.168.1.1	DNS-Server spezifizieren
nmap --system-dns	nmap --system-dns 192.168.1.1	System-DNS verwenden
nmap -sL	nmap -sL 192.168.1.0/24	**List-Scan** (nur DNS-Auflösung)

Beispiel-Anwendung:

```
# Schneller Scan ohne DNS-Verzögerung
nmap -n -T4 192.168.1.0/24

# Host-Liste mit DNS-Namen erstellen
nmap -sL -R 192.168.1.0/24 | grep "Nmap scan report"
```

IPv6-Unterstützung

IPv6-Scans

Syntax	Beispiel	Beschreibung
nmap -6	nmap -6 2001:db8::1	IPv6-Scan aktivieren
nmap -6 --script ipv6-*	nmap -6 --script ipv6-* 2001:db8::1	IPv6-spezifische Scripts

Praktische Scan-Kombinationen

Häufig verwendete Kombinationen

```
# 1. Schneller Netzwerk-Überblick
nmap -T4 -F 192.168.1.0/24

# 2. Detaillierte Einzelhost-Analyse
nmap -A -T4 -oA target-analysis 192.168.1.10

# 3. Stealth-Vulnerability-Scan
nmap -sS -T2 --script vuln --script-timeout 10m 192.168.1.5

# 4. Web-Service Analyse
nmap -sS -sV --script "http-*" -p 80,443,8080,8443 192.168.1.1-50

# 5. Umfassender Sicherheits-Scan
nmap -sS -sU -T4 --script "vuln,exploit,auth,brute" --script-timeout 5m -oA security-scan 192.168.1.10

# 6. Firewall-Analyse
nmap -sA -T4 192.168.1.0/24

# 7. Service-Discovery für große Netzwerke
nmap -sS -T4 --top-ports 1000 --open -oG services.txt 10.0.0.0/8

# 8. Stealth-Reconnaissance
nmap -sF -T1 -f --source-port 53 -D RND:10 192.168.1.1

# 9. Vulnerability-Assessment mit externer DB
nmap -sV --script vulners --script-args mincvss=7.0 192.168.1.1-50

# 10. UDP-Service Discovery
nmap -sU --top-ports 100 -T4 192.168.1.0/24
```

Spezielle Use Cases

Netzwerk-Inventarisierung

```
# Aktive Hosts identifizieren
nmap -sn 192.168.1.0/24 | grep "Nmap scan report" | awk '{print $5}'

# Service-Matrix erstellen
nmap -sS --top-ports 1000 --open 192.168.1.0/24 -oG - | grep "Ports:"
```

Sicherheits-Assessment

```
# CVE-Analyse mit Severity-Filter
nmap -sV --script vulners --script-args mincvss=8.0 192.168.1.0/24

# SMB-Schwachstellen (EternalBlue, etc.)
nmap --script smb-vuln-* -p 445 192.168.1.0/24

# Web-Vulnerabilities
nmap --script "http-vuln-*" -p 80,443 192.168.1.0/24
```

Performance-Optimierung

```
# Schnellstmöglicher Scan
nmap -T5 --min-parallelism 100 --max-retries 2 192.168.1.0/24

# Bandwidth-freundlicher Scan
nmap -T2 --scan-delay 1s --max-parallelism 5 192.168.1.0/24
```

Troubleshooting und Debug

Debug-Optionen

Syntax	Beispiel	Beschreibung
nmap --packet-trace	nmap --packet-trace 192.168.1.1	Alle gesendeten/empfangenen Pakete anzeigen
nmap --iflist	nmap --iflist	Netzwerk-Interfaces und Routen anzeigen
nmap --version	nmap --version	Nmap-Version anzeigen
nmap --help	nmap --help	Hilfe anzeigen

Script-Integration Beispiele

Mit externen Tools kombinieren

```
# Nmap + Metasploit Integration
nmap -sS -sV -oX metascan.xml 192.168.1.1
# Dann in Metasploit: db_import metascan.xml

# Nmap + Nessus Workflow
nmap -sS --top-ports 1000 --open 192.168.1.0/24 -oG - | \
  awk '/Up$/{print $2}' > live_hosts.txt

# Automatisierte CVE-Reports
nmap -sV --script vulners 192.168.1.0/24 -oN vulns.txt
grep -E "(CVE-|CVSS)" vulns.txt > cve_summary.txt
```

1. https://en.wikipedia.org/wiki/Nmap
2. https://www.wiz.io/academy/nmap-overview
3. https://www.geeksforgeeks.org/ethical-hacking/port-scanning-techniques-by-using-nmap/
4. https://www.techtarget.com/searchnetworking/tip/Types-of-Nmap-scans-and-best-practices
5. https://www.hackercoolmagazine.com/port-scanning-techniques-for-beginners/
6. https://www.centron.de/en/tutorial/switches-and-scan-types-in-nmap/
7. https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/nmap-commands
8. https://levelblue.com/blogs/security-essentials/advanced-nmap-scanning-techniques
9. https://nmap.org/book/nse-example-scripts.html
10. https://nmap.org/book/man-nse.html
11. https://nmap.org/book/nse-usage.html
12. https://subscription.packtpub.com/book/cloud-&-networking/9781782168317/1/ch01lvl1sec11/script-categories
13. https://routezero.security/2024/12/07/nmap-exploring-nse-scripts-for-pentesters/
14. https://www.redhat.com/en/blog/nmap-scripting-engine
15. https://www.stationx.net/nmap-scripts/
16. https://www.youtube.com/watch?v=wlqUO09J-nw
17. https://www.cbtnuggets.com/blog/certifications/security/7-absolutely-essential-nmap-commands-for-pen-testing
18. https://nmap.org/book/zenmap.html
19. https://nmap.org/zenmap/
20. https://nmap.org/zenmap/man.html
21. https://nextdoorsec.com/zenmap-vs-nmap/
22. https://www.stationx.net/zenmap-vs-nmap/

23. https://www.youtube.com/watch?v=Xqj12-03vlg

24. https://secviz.org/content/new-zenmap-adds-feature-does-topology-mapping.html

25. https://www.hackercoolmagazine.com/beginners-guide-to-zenmap-2/

26. https://www.varonis.com/de/blog/nmap-commands

27. https://www.meinetestumgebung.de/index.php/2020/03/09/zenmap-auf-kali-linux-nachinstallieren/

28. https://www.linkedin.com/pulse/zenmap-installation-kali-linux-quick-guide-halil-ibrahim-deniz-0amcf

29. https://www.youtube.com/watch?v=3julVr6qFo4

30. https://www.youtube.com/watch?v=aly4WjXL2RY

31. https://www.stationx.net/nmap-cheat-sheet/

32. https://github.com/daniel-cues/NMapGUI

33. https://nmap.org/book/toc.html

34. https://www.youtube.com/watch?v=0uGyMpUdKpU

35. https://nmap.org/book/man-briefoptions.html

36. https://nmap.org/book/man-port-scanning-techniques.html

37. https://nmap.org/book/osdetect-usage.html

38. https://nmap.org/book/inst-windows.html

39. https://nmap.org/book/scan-methods.html

40. https://www.vaadata.com/blog/nmap-the-tool-for-mapping-and-assessing-network-security/

41. https://www.eikoon.de/wiki-single/nmap-zenmap-wiki/

42. https://www.secopsolution.com/blog/nmap-vs-z-map-a-comparative-analysis-of-network-scanning-tools

43. https://www.easy-network.de/nmap-tutorial-howto.html

44. https://www.secureideas.com/blog/introduction-to-writing-nmap-scripting-engine-nse-scripts

45. https://www.youtube.com/watch?v=DMNbz-fnTAw

46. https://www.reddit.com/r/nmap/comments/1gtx3oh/nmap_results_differ_from_zenmap/

47. https://www.geeksforgeeks.org/linux-unix/how-to-use-nmap-script-engine-nse-scripts-in-linux/

48. https://www.youtube.com/watch?v=EU8JT_bT-xM

49. https://nmap.org/nsedoc/categories/default.html

50. https://nmap.org/nsedoc/scripts/

51. https://github.com/ekol-x9/nmap-cheatsheet

52. https://www.helpnetsecurity.com/2007/12/14/zenmap-nmap-official-gui-screenshots/

53. https://nmap.org/book/man-examples.html

54. https://supportcommunity.milestonesys.com/s/article/using-Zenmap-and-netstat