NMAP COMMANDS

Hier ist die textbasierte Umsetzung der Nmap-Befehlsübersicht aus dem bereitgestellten Bild. Die Liste wurde für eine bessere Lesbarkeit strukturiert und ein kleiner Typo aus dem Original-Infografik-Design korrigiert (die Option `-iL` für den Listen-Input verwendet im Original ein kleines "l").

Scan-Typen & Erkennung (Scan Types & Detection)

- `nmap -sP`
  Ping Scan *(Hinweis: In neueren Nmap-Versionen entspricht dies `-sn`)*
- `nmap -sS`
  TCP SYN Scan *(Stealth Scan / Halboffener Scan)*
- `nmap -sU`
  UDP Scan
- `nmap -sV`
  Version Detection *(Dienste- und Versionserkennung)*
- `nmap -O`
  OS Detection *(Betriebssystem-Erkennung)*
- `nmap -A`
  Aggressive Scan *(Aktiviert OS-Erkennung, Versionserkennung, Skript-Scans und Traceroute)*
- `nmap -sX`
  XMAS Scan *(Setzt FIN-, PSH- und URG-Flags)*
- `nmap -sF`
  FIN Scan *(Setzt nur das FIN-Flag)*
- `nmap -sT`
  TCP Connect Scan *(Vollständiger Drei-Wege-Handschlag)*
- `nmap -sN`
  TCP Null Scan *(Setzt überhaupt keine Flags)*
- `nmap -sA`
  TCP ACK Scan *(Wird primär zum Erkennen von Firewall-Regeln genutzt)*

⚙ Scan-Konfiguration & Performance

- `nmap -T4`
  Timing Template *(Setzt das Geschwindigkeits- und Aggressivitätsprofil; Stufe 4 von 5 für schnellere Scans)*
- `nmap -iL`
  Input from List *(Liest die Ziel-IPs/Hosts aus einer Textdatei ein)*
- `nmap -sn`
  No Port Scan *(Reine Host-Erkennung ohne anschließenden Port-Scan)*
- `nmap --top-ports <number>`
  Scan most common ports *(Scant nur die X am häufigsten genutzten Ports)*

□ Skript-Scans (Nmap Scripting Engine - NSE)

- `nmap -sC`
  Script Scan using default scripts *(Führt Standard-Testskripte auf den gefundenen Ports aus)*
- `nmap --script <script>`
  Run specific NSE script *(Führt ein ganz gezieltes Nmap-Skript oder eine Skript-Kategorie aus)*

Revision #1
Created 2026-10-20 12:21:32 UTC by Oliver Schönemann
Updated 2026-10-20 12:21:32 UTC by Oliver Schönemann