

Grundlegende Einstellungen

nmap Scantechnik *Option*

-v	verbose, mehr Ausgabeinformationen
-vv	maximale Informationen
-iL <i>datei</i>	IP-Liste
-n	keine DNS-Auflösung (schneller)
-oG <i>[-/file]</i>	Lesbares Format
open/filtered/closed	Status des Ports
-R	DNS-Auflösung (langsamer)
-T[1-5]	Timing-Template (höher ist schneller)
--version	Version
--excludefile <i>file</i>	Adressliste ausschließen

Dienstidentifizierung und OS-Erkennung

-sV	Dienstidentifizierung offene Ports
-O	OS-Detection
-A	Versions-/OS-Erkennung komplett

Testscans

-oG - 192.168.0.1-255 -p22 -vv

Ausführliche Anzeige in lesbarer Form des Portscans

-sP -PS80 -n Adresse	Test gegen Firewall (PA analog)
--exclude <i>IP</i>	IP-Adressen ausschließen

scanme.nmap.org zum Testen von Scans. Zenmap ist ein grafisches Interface von nmap. Die Techniken sind kombinierbar einsetzbar im selben Befehl.

Portangabe

-p <i>ports</i>	Portangabe
-F	schneller Scan (nur 100 Ports)
--top-ports <i>zahl</i>	Die <i>zahl</i> Top Ports durchsuchen

Scantechniken

-sT <i>ports</i>	TCP-Connect Scan (komplette Verbindung aufgebaut)
-sS <i>ports</i>	SYN-STEALTH Scan (kein kompletter Aufbau Verbindung)
-sU <i>ports</i>	UDP Portscan
-sP <i>ports</i>	Ping ICMP-Echo Request
-sN; -sF; -sX	TCP-NUL-,FIN-,XMAS-Scan (RST-Packet erzwungen -> Ports geschlossen))
-sA	TCP-ACK-Scan (Firewall-Zustand bestimmen)
-sW	TCP-WInow-Scan (minimaler Erfolg, ähnlich ACK-Scan)
--scanflags <i>flags</i>	Eigene Flags setzen (Reihenfolge egal) URG, ACK, PSH, RST, SYN, FIN

Hosterkennung

-PS <i>portlist</i>	TCP SYN Ping (gut für stateful Firewall)
-PA <i>portlist</i>	TCP ACK Ping (gut gegen stateless Firewall)
-PU <i>portlist</i>	UDP Host Discovery
-PE, -PM, -PP	ICMP Host Discovery (Echo REquest und eine der beiden anderen)
-PR	Arp-Ping

scanme.nmap.org zum Testen von Scans. Zenmap ist ein grafisches Interface von nmap. Die Techniken sind kombinierbar einsetzbar im selben Befehl.

Zusätzliche Informationen

curl ipinfo.io/ipadresse	IP-Adressinfos
https://www.exploit-db.com/	Exploit-Datenbank
https://nmap.org/nsedoc/categories/vuln.html	Nmap-Skripte

scanme.nmap.org zum Testen von Scans. Zenmap ist ein grafisches Interface von nmap. Die Techniken sind kombinierbar einsetzbar im selben Befehl.

