Cheatography

nmap Cheat Sheet

by aragow via cheatography.com/24054/cs/8078/

Grundlegende Einstellungen

nmap Scantechnik *Option*

-v	*verbose*, mehr Ausgabeinformationen
-vv	maximale Informationen
-iL *datei*	IP-Liste
-n	keine DNS-Auflösung (schneller)
-oG *[-/file]*	Lesbares Format
open/filtered/closed	Status des Ports
-R	DNS-Auflösung (langsamer)
-T[1-5]	Timing-Template (höher ist schneller)
--version	Version
--excludefile *file*	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 *IP*	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 *ports*	Portangabe
-F	schneller Scan (nur 100 Ports)
--top-ports *zahl*	Die *zahl* Top Ports durchsuchen

Scantechniken

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

Hosterkennung

-PS *portlist*	TCP SYN Ping (gut für stateful Firewall)
-PA *portlist*	TCP ACK Ping (gut gegen stateless Firewall)
-PU *portlist*	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.

By **aragow**
cheatography.com/aragow/

Not published yet.
Last updated 13th May, 2016.