Cheatography

Nmap Komutları Cheat Sheet

by codeluu (codeluu) via cheatography.com/26083/cs/7196/

Tarama Hızları -T

En yavaş	paranoid|0
Yavaş	sneaky|1
Normalden yavaş	polite|2
Normal	normal|3
Hızlı	aggressive|4
En hızlı	insane|5

Açık hostları bulmak

Default Ping Scan	-sP <hedef>
TCP/SYN Ping	-sP -PS <hedef>
Spesifik Port	-sP -PS80 <hedef>
ARP Scan	-sP -PR <hedef>
ICMP, IP-in-IP	-sP -PO <hedef>
ARP devre dışı	-sP --send-ip <hedef>

Tespit Teknikleri

İşletim sistemi	-O
İşletim sistemi (Verb.)	-O -v <hedef>
Tahmin yürütme	-O –osscan--guess
Servis versiyonu	-sV
Hata tespiti	-sV –version-trace
RPC tarama	-sR
Port listeleme	nmap -sO <hedef>

Network Keşif Taramaları

Ping ile	-sP
Ping atmadan	-PN
TCP SYN Ping	-PS
TCP ACK ping	-PA
UDP ping	-PU
SCTP Init Ping	-PY
ICMP echo ping	-PE
ICMP Timestamp	-PP
ICMP mask ping	-PM
Keşif yapma	-Pn
IP protocol ping	-PO
ARP ping	-PR
Traceroute	–trace route
Hostları listele	-sL
Tersine DNS çöz	-R
DNS çözmeden	-n
OS DNS lookup	–system-dns
Elle DNS sunucusu	-dns-servers[adı]
Belirli port	nmap -p80 <hed.>
Port devre dışı	-sn
Ping devre dışı	-P0

Çıktı Seçenekleri

Txt	-sP	-oN[tam adı]
Xml	-PN	-oX[tam adı]
Grep	-PS	-oG[tam adı]
Herhangi	-PA	-oA[yeri/adı] [hedef]
Zaman ayarlı	-PU	-stats -every [time] [hedef]
	-PY	
	-PE	
	-PP	
	-PM	
	-Pn	
	-PO	
	-PR	
	-sL	
	-R	
	-n	
	-sP	
	-PU	
	-PW	

Tarama Türleri

Tarama	Komut	Örnek
Conn	-sT	nmap -sT 10.0.0.1
SYN	-sS	nmap -sS 10.0.0.1
ACK	-sA	nmap -sA 10.0.0.1
FIN	-sF	nmap -sF 10.0.0.1
Null	-sN	nmap -sN 10.0.0.1
Xmass (FIN, PSH, URG)	-sX	nmap -sX 10.0.0.1
Idle	-sI	nmap -sI Zombi:Port 192
Ping	-sP	nmap -sP 10.0.0.1
UDP	-sU	nmap -sU 10.0.0.1
Window	-sW	nmap -sW 10.0.0.1

Tarama Türleri (cont)

FIN/ACK	-sM	nmap
Ftp Bounce	-b	nmap

Hedef Belirtme

Tek hedef
Birden fazla
Liste içi
IP bloğu tarama
Tüm subnet
Belirli hedefi taramadan ç
Belirli hedefi liste ile ç
Rastgele host

Tespit Örnekleri

İşletim sistemi ve servis
Web Server tespiti
Broadcast pingle riyle hosi
DNS Kaydı Brute Force
Büyük Ağlar için hızlı tar

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com