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

Network Keşif Taramaları (cont)

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	–traceroute
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	-oN [tarama.txt] [hedef]
Xml	-oX [tarama.xml] [hedef]
Grep	-oG [tarama.txt] [hedef]
Herhangi	-oA [yeri/adı] [hedef]

Çıktı Seçenekleri (cont)

Zaman ayarlı	–stats-every [time] [hedef]

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 192.168.1.1
Ping	-sP	nmap -sP 10.0.0.1
UDP	-sU	nmap -sU 10.0.0.1
Window	-sW	nmap -sW 10.0.0.1
FIN/ACK	-sM	nmap -sM 10.0.0.1
Ftp B. Attack	-b	nmap -b 10.0.0.1

Hedef Belirtme

Tek hedef	[hedef]
Birden fazla	[h1,h2,h3]
Liste içi	-iL [liste.txt]
IP bloğu tarama	10.0.0.1-28
Tüm subnet	10.0.0.1/24
Belirli hedefi taramadan çıkar	-exclude [hedefler]
Belirli hedefi liste ile çıkar	[hedefler] –excludefile [liste.txt]
Rastgele host	-iR [sayı]

Tespit Örnekleri

İşletim sistemi ve servis tespiti	nmap -sV -O <hedef>
Web Server tespiti	nmap -sV --script http-title <hedef>
Broadcast pingleriyle host tespiti	nmap --script broadcast-ping
DNS Kaydı Brute Force	nmap --script dns-brute <hedef>
Büyük Ağlar için hızlı tarama	nmap -T4 -n -Pn -p- <hedef>

Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com