Cheatography

Nmap Komutları Cheat Sheet

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

Tarama Hızları -T		Network Keşif Taramaları (cont)		Çıktı Seçenekleri (cont)			Hedef Belirtme	
En yavaş	paranoid 0	SCTP Init	- PY	Zaman	-stats	-every	Tek hedef	[hedef]
Yavaş	sneaky 1	Ping		ayarlı	[time]	[hedef]	Birden	[h1,h2,h3]
Normalden yavaş polite 2		ICMP echo -PE					fazla	
Normal normal 3		ping		Tarama Türleri		Liste içi	-iL	
Hızlı	aggressive 4	ICMP	- PP	Tarama	Komut	Örnek		[liste.txt]
En hızlı	insane 5	Timestamp		Conn	-sT	nmap -sT	IP bloğu	10.0.0.1-28
Açık hostları bulmak		ICMP mask	- PM			10.0.0.1	tarama	
		ping		SYN	-sS	nmap -ss	Tüm subnet	10.0.0.1/24
Default Ping Scan	-sP <hedef></hedef>	Keşif yapı	na - Pn			10.0.0.1	Belirli hedefi	-exclude
	-sP -PS <hedef></hedef>	IP protoco	1 - PO	ACK	-sA	nmap -sA		[hedefler]
Ping	Si i o (nedel)	ping	g			10.0.0.1	taramadan	
'	-sP -PS80 <hedef></hedef>	ARP ping	- PR	FIN	-sF	nmap -sF 10.0.0.1	çıkar	
		Traceroute	e -traceroute				Belirli	[hedefler] -
ARP Scan	-sP -PR <hedef></hedef>	Hostları	-sL	Null	-sN	nmap -sN 10.0.0.1	hedefi liste ile	excludefile [liste.txt]
	-sP -PO <hedef></hedef>	listele		Vmogg	- CV		çıkar	[IISCE.CAC]
	-sPsend-ip <hedef></hedef>	Tersine DN	S -R	Xmass (FIN, PSH,	-sX	nmap -sX 10.0.0.1	Rastgele	-iR [sayı]
		çöz					host	IN [Say1]
		DNS çözmeden -n		URG)				
Tespit Teknikleri		OS DNS	-system-dns	Idle	-sI	nmap -sI	Tespit Örnekler	
İşletim sistemi	-O	lookup				Zombi:Port	İşletim	nmap -sV -O
İşletim sistemi	-O -v <hedef></hedef>	Elle DNS	-dns-			192.168.1.	sistemi ve	<hedef></hedef>
(Verb.)		sunucusu	servers[ad1]			1	servis	
Tahmin yürütme	-O – osscan-guess	Belirli port	nmap -p80	Ping	-sP	nmap -sP	tespiti Web Server	
Servis versiyonu	•		<hed.></hed.>			10.0.0.1		nmap -sV
Hata tespiti			-sn	UDP	-sU	nmap -sU	tespiti	script http- title
	version-trace	dışı				10.0.0.1		<hedef></hedef>
RPC tarama	-sR	Ping devre	- P0	Window	-sW	nmap -sW	Broadcast	nmap
Port listeleme	nmap -sO <hedef></hedef>	dışı		,		10.0.0.1	pingleriyle	script
		Çıktı Seçenekleri		FIN/ACK	-sM	nmap -sM	host	broadcast-pi
Network Keşif Taramaları		Txt	-oN[tarama.txt]	Eta D	b		tespiti	ng
		1	[hedef]	Ftp B. Attack	-b	nmap -b 10.0.0.1	DNS Kaydı	nmap
Ping ile	-sP	Xml	-oX[tarama.xml]	11004011			Brute Force	script dns-
Ping atmadan	- PN	111111	[hedef]					brute
TCP SYN Ping	-PS	Grep	-oG[tarama.txt]					<hedef></hedef>
TCP ACK ping	- PA	Ţ	[hedef]				Büyük Ağlar	nmap -T4 -n
UDP ping	- PU	Herhangi	-oA[yeri/adı]				için hızlı tarama	-Pn -p- <hedef></hedef>
		-	[hedef]					



By **codeluu** (codeluu) cheatography.com/codeluu/ code0day.wordpress.com Published 17th February, 2016. Last updated 17th February, 2016. Page 1 of 1. Sponsored by **Readability-Score.com**Measure your website readability!
https://readability-score.com