

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		Liste içi -iL
Hızlı aggressive 4	ICMP -PP		[liste.txt]
En hızlı insane 5	Timestamp		IP bloğu 10.0.0.1-28
	ICMP mask -PM		tarama
	ping		Tüm subnet 10.0.0.1/24
	Keşif yapma -Pn		Belirli -exclude
	IP protocol -PO		hedefi [hedefler]
	ping		taramadan
	ARP ping -PR		çıkarmak
	Traceroute -traceroute		Belirli [hedefler] -
	Hostları -sL		hedefi excludefile
	listele		liste ile [liste.txt]
	Tersine DNS -R		çıkarmak
	çöz		Rastgele -iR [sayı]
	DNS çözmeden -n		host
	OS DNS -system-dns		
	lookup		
	Elle DNS -dns-		
	sunucusu servers[adı]		
	Belirli nmap -p80		
	port <hed.>		
	Port devre -sn		
	dışı		
	Ping devre -p0		
	dışı		
Tespit Teknikleri	Çıktı Seçenekleri		Tespit Örnekleri
İşletim sistemi -O	Txt -oN[tarama.txt]		İşletim nmap -sV -O
İşletim sistemi -O -v <hedef>	[hedef]		sistemi ve <hedef>
(Verb.)	Xml -oX[tarama.xml]		servis
Tahmin yürütme -O -	[hedef]		tespiti
osscan-guess	Grep -oG[tarama.txt]		Web Server nmap -sV -
Servis versiyonu -sV	[hedef]		tespiti script http-
Hata tespiti -sV -	Herhangi -oA[yeri/adı]		title
version-trace	[hedef]		<hedef>
RPC tarama -sR			Broadcast nmap -
Port listeleme nmap -sO			pingleriyle script
<hedef>			host broadcast-pi
			tespiti ng
			DNS Kaydı nmap -
			Brute Force script dns-
			brute
			<hedef>
			Büyük Ağlar nmap -T4 -n
			için hızlı -Pn -p-
			tarama <hedef>

