**Masscan**, dünyanın en hızlı port tarayıcısı olarak bilinen açık kaynaklı bir araçtır. Özellikle büyük ağları (örneğin tüm interneti) çok kısa sürede taramak için tasarlanmıştır. Nmap’e benzer şekilde çalışır fakat **asenkron** motoru sayesinde çok daha yüksek hızda tarama yapabilir.

**Bu Aracın Özellikleri Nelerdir?**

* **Milyonlarca IP’yi saniyeler içinde tarayabilir**
* **Nmap benzeri sonuç formatı** sunar
* **TCP SYN taraması (stateless)** ile çalışır
* **Port aralığı ve hız özelleştirilebilir**
* **Çıktılar XML, JSON, grepable formatlarda alınabilir**
* **Firewall ve IDS sistemlerini zorlayacak kadar hızlı**

**Bu Aracı Kali Linux Üzerinde Kullanma ve Test Etme Adımları**

**Adım 1: Masscan’in Kurulu Olduğunu Kontrol Et / Kurulum**

**“**which masscan” **ile kontrol et**

**Eğer kurulu değil ise :**

“sudo apt update

sudo apt install masscan -y”

**Adım 2: Temel Port Taraması (TCP 80)**

“sudo masscan 192.168.1.0/24 -p80”

**metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Adım 3: Hız Limitini Ayarlayarak Tarama**

“sudo masscan 192.168.1.0/24 -p22 --rate=100”



**Adım 4: Belirli IP ve Çoklu Portları Tarama**

“sudo masscan 192.168.1.5 -p21,22,80,443”

metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu

**Adım 5: Sonuçları Dosyaya Kaydetme**

“sudo masscan 192.168.1.0/24 -p80 -oG masscan\_results.txt”

**Adım 6: Tüm İnterneti Tarama**

“sudo masscan 0.0.0.0/0 -p80 --rate=1000”

Bu komut **internetin tamamına** SYN paketi gönderir. Sadece özel lab ortamında test edilmelidir. Gerçek dünyada yasal risk doğurur!