**🧠 1. ZMap Nedir?**

**ZMap**, açık kaynak kodlu, **tek port taramasına odaklı** ve **aşırı hızlı** bir ağ tarama aracıdır.

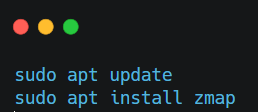
📌 Hedefi: Saniyede milyonlarca IP’ye SYN paketi göndererek belirli bir portta açık sistemleri bulmak  
📌 Geliştirici: University of Michigan  
📌 Kullanım Alanı: İnternet çapında port taraması (research, honeypot, saldırı analizi)

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🚀 Süper hızlı tarama | Milyonlarca IP’yi dakikalar içinde tarar |
| 🔎 Tek port odaklı | Her çalıştırmada yalnızca **1 port** taranır |
| 📊 Ham verileri kaydeder | Çıktılar JSON, CSV veya raw formatta alınabilir |
| 🧪 Network research | Honeypot analizi, saldırı yüzeyi haritalama |
| 📁 Büyük veri toplama | Geniş kapsamlı port/servis çalışmaları için kullanılır |

**⚙️ 3. Kurulum (Kali Linux / Debian)**

**✅ 1. Paket yöneticisiyle kur:**



**✅ 2. Kaynaktan kurmak istersen:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ Basit kullanım – 80. portu taramak:**

sudo zmap -p 80 192.168.1.0/24

**✅ Sonuçları dosyaya yazmak:**

sudo zmap -p 443 0.0.0.0/0 -o ssl\_hosts.txt

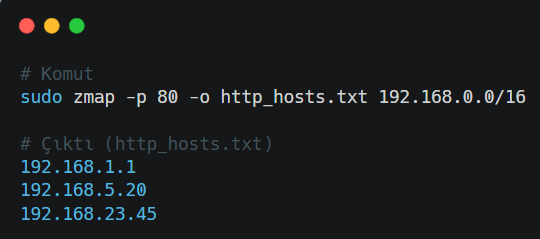
**✅ JSON formatında çıktı:**

sudo zmap -p 22 192.168.100.0/24 -f saddr -O json -o ssh\_result.json

**✅ Hedefleri özel bir IP listesi dosyasından almak:**

sudo zmap -p 8080 -w target\_ips.txt -o output.txt

**📋 5. Örnek Terminal Çıktısı**



| **Senaryo** | **Açıklama** |
| --- | --- |
| 🌍 Global port keşfi | Belirli bir portun (örneğin 22, 80, 445) dünya çapındaki dağılımı |
| 🔐 Savunma testleri | Hangi IP’lerin dış dünyaya açık olduğunu görmek |
| 🧪 Honeypot tespiti | Beklenmedik tepkilerle çalışan IP’leri analiz etmek |
| 🛰️ Siber tehdit yüzeyi analizi | Kurumsal IP bloklarında açık portları tespit etmek |

**⚠️ 7. Dikkat Edilmesi Gerekenler**

| **Durum** | **Açıklama** |
| --- | --- |
| ⚠️ Gürültülü | Çok hızlı tarama yaptığı için IDS/IPS sistemleri tarafından fark edilir |
| 🌐 Tüm interneti tarayabilir | Ancak etik ve hukuki sorumluluğu büyüktür |
| 📛 Abuse riski | Gerçek ağlara izinsiz gönderim yaparsan blacklist’e alınabilirsin |

**🎯 8. Öğrenim Kazanımları**

* Tek port taramanın hız ve etki analizini kavrama
* Büyük veri ile güvenlik keşfi yapmayı öğrenme
* Ağ tarama araçları arasında hız/fonksiyon farkını anlama
* Network araştırmalarında bilimsel araç kullanımını deneyimleme