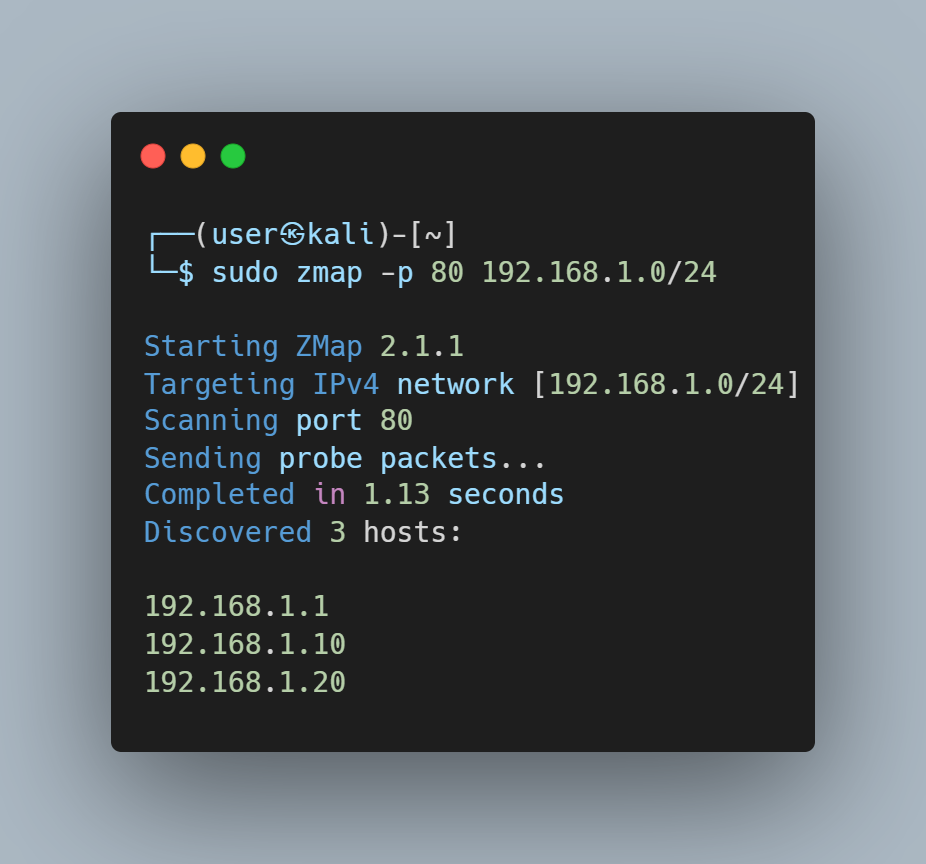
**ZMap Nedir?**

ZMap, büyük ağlarda (örneğin tüm internet blokları) hızlı port taraması yapmak için geliştirilmiş, açık kaynak kodlu ve son derece hızlı bir tarama aracıdır. Özellikle araştırma, sızma testi ve güvenlik analizlerinde milyonlarca IP’yi çok kısa sürede taramak isteyen uzmanlar tarafından kullanılır.

ZMap, geleneksel tarayıcılar olan Nmap’e göre daha az ayrıntı verir, ancak çok daha hızlı çalışır. Bu nedenle, “ön keşif” ya da “IP üzerinde servis var mı yok mu” gibi hızlı cevaplar alınması gereken durumlarda tercih edilir.

****

* Starting ZMap 2.1.1: Kullanılan ZMap sürümüdür.
* Targeting IPv4 network: Hedeflenen IP aralığını belirtir.
* Discovered X hosts: Belirtilen portta açık bulunan cihazlar listelenir.
* ZMap yalnızca açık port bilgisi verir; ayrıntılı banner bilgisi vermez (nmap’ten farklı olarak).

**ZMap Ne İşe Yarar?**

* Milyonlarca IP adresini birkaç dakikada tarayabilir.
* İnternete açık portları tespit etmek için kullanılır (örneğin 80, 443, 22).
* Açık kaynak internet taramaları için kullanılır (örn: üniversitelerin güvenlik araştırmaları).
* Büyük çaplı port taramaları yapmak isteyen kırmızı ekipler için idealdir.

Temel Kullanım: **sudo zmap -p 80 192.168.1.0/24**

Bu komut, 192.168.1.0/24 ağı üzerinde **80. port** (HTTP) açık olan IP adreslerini tarar.

İleri Seviye Örnek: **sudo zmap -B 10M -p 443 --output-file=https\_hosts.txt 0.0.0.0/0**

**Bu örnekte:**

* **-B 10M:** Bant genişliğini 10 Mbps ile sınırlar.
* **-p 443:** HTTPS portu taranır.
* **--output-file=https\_hosts.txt:** Sonuçlar belirtilen dosyaya yazılır**.**
* **0.0.0.0/0:** Tüm internet IP aralığı taranır (gerçek hayatta dikkatli kullanılmalıdır!).

**ZMap’in Özellikleri**

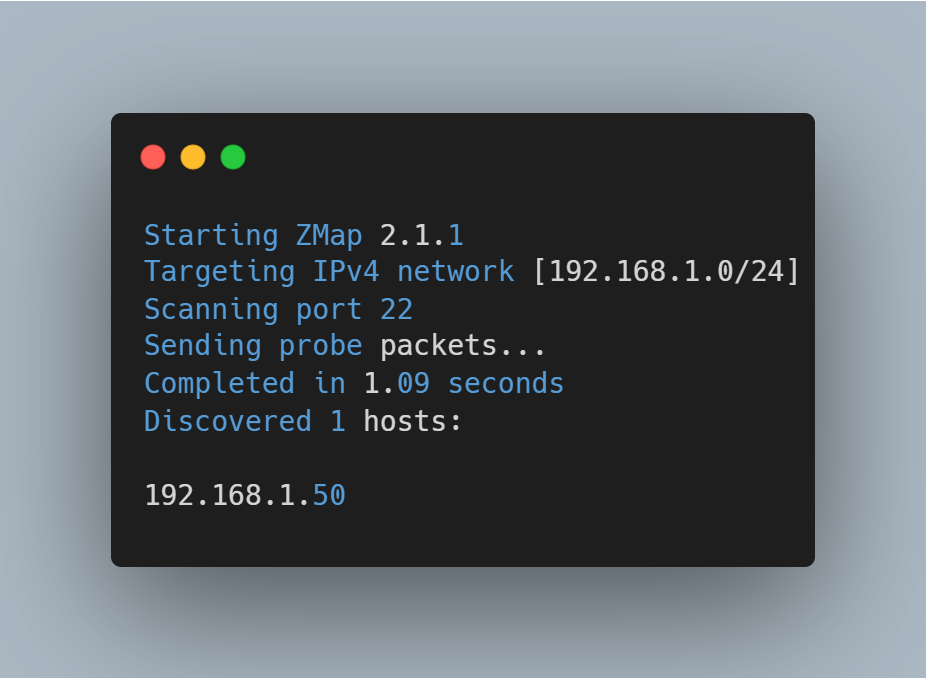
| **Özellik** | **Açıklama** |
| --- | --- |
| **Yüksek Hız** | **Milyonlarca IP'yi dakikalar içinde tarar.** |
| **Basit Arayüz** | **Komut satırı üzerinden kolay kullanım.** |
| **Eklenti Desteği** | **Modüler yapısı ile gelişmiş analiz yapılabilir.** |
| **JSON/CSV Çıktı** | **Kolayca dışa aktarım yapılabilir.** |

ZMap, her taramada yalnızca bir port tarayabildiği için çoklu port taramaları için port başına ayrı komutlar çalıştırılır.

Örnek: Port 22 (SSH), 443 (HTTPS)

Port 22;





Alternatif: Çıktılar TXT Dosyasına Yazılsın

***sudo zmap -p 443 192.168.1.0/24 -o https\_hosts.txt***

Bu komut, bulduğu IP adreslerini https\_hosts.txt adlı dosyaya yazacaktır.

Port 443

