**Dijital Dünyanın Kapılarını Aralayan Anahtar: Naabu**

Siber güvenlik okyanusunda, hedef sistemlerin zayıf noktalarını bulmak için atılan ilk adım genellikle keşif ve bilgi toplamadır. Bu sürecin en temel yapı taşlarından biri de port taramasıdır. Bir sistemin dış dünyaya açık olan "kapılarını", yani portlarını bilmek, o sisteme nasıl yaklaşılabileceği konusunda paha biçilmez bilgiler sunar. Geleneksel araçlar bu işi yapsa da, hız ve verimliliğin her şey demek olduğu günümüzde, Project Discovery ekibinin geliştirdiği **Naabu** adlı araç, modern bir süperstar olarak parlıyor. Bu yazıda, Naabu'nun ne olduğunu, neden bu kadar popüler olduğunu, nasıl kurulup kullanılacağını ve en önemlisi, bu aracı bir profesyonel gibi kullanmanızı sağlayacak etkili örnekleri A'dan Z'ye inceleyeceğiz.

**1. Naabu Aracı Nedir?**

**Naabu**, Go programlama dili ile yazılmış, son derece hızlı ve basit bir port tarama aracıdır. Temel amacı, bir veya daha fazla hedef sistem üzerinde hangi TCP ve UDP portlarının açık olduğunu olabildiğince hızlı bir şekilde tespit etmektir. Project Discovery tarafından geliştirilen diğer siber güvenlik araçlarıyla (Subfinder, Httpx, Nuclei vb.) mükemmel bir uyum içinde çalışacak şekilde tasarlanmıştır. Bu entegrasyon yeteneği, onu basit bir port tarayıcıdan çok daha fazlası haline getirir.

Özetle Naabu:

* **Hızlıdır:** Asenkron yapısı ve Go dilinin gücü sayesinde binlerce portu ve hedefi saniyeler içinde tarayabilir.
* **Basittir:** Karmaşık konfigürasyonlar gerektirmeyen, sade ve anlaşılır bir komut satırı arayüzüne sahiptir.
* **Esnektir:** Tek bir hedeften, on binlerce hedefin bulunduğu listelere kadar geniş bir yelpazede tarama yapabilir.
* **Entegredir:** Diğer araçlardan gelen veriyi (pipe) doğrudan işleyebilir ve kendi çıktısını başka araçlara yönlendirebilir.

**2. Neden Kullanılır?**

Piyasada Nmap gibi çok güçlü ve köklü port tarayıcılar varken neden Naabu'ya ihtiyaç duyalım? Cevap, kullanım amacında gizlidir.

* **Hız Odaklı Keşif:** Güvenlik araştırmacıları veya sızma testi uzmanları, genellikle binlerce alt alan adından (subdomain) oluşan listeleri taramak zorundadır. Nmap ile bu işlem saatler sürebilirken, Naabu aynı işi dakikalar içinde tamamlar. Amacı, derinlemesine analizden ziyade **hızlıca açık portları bulmaktır.**
* **Otomasyon ve "Pipelining":** Naabu'nun asıl gücü, "pipelining" yani komutları birbirine bağlama yeteneğidir. Örneğin, Subfinder ile bir şirketin alt alan adlarını bulup, bu listeyi doğrudan Naabu'ya göndererek açık portları tespit edebilir ve ardından bu portları Httpx'e yollayarak hangilerinde web sunucusu çalıştığını kontrol edebilirsiniz. Bu zincirleme işlem, manuel iş yükünü ortadan kaldırır.
* **Pasif Tarama:** Naabu, hedefe tek bir paket bile göndermeden port taraması yapabilir. Bunu, **Shodan** gibi internet çapında tarama yapan servislerin veritabanını sorgulayarak yapar. Bu sayede, tamamen gizli bir şekilde ön bilgi toplamak mümkün olur.
* **Kaynak Verimliliği:** Özellikle büyük ölçekli taramalarda sistem kaynaklarını (CPU, RAM) Nmap'a kıyasla daha verimli kullanır.

**3. Nasıl Kurulum Yapılır?**

Naabu'yu kurmanın birden fazla yolu vardır. Size en uygun olanı seçebilirsiniz.

**Yöntem 1: Go ile Kurulum (Önerilen)**

Bu yöntem için sisteminizde Go programlama dilinin kurulu olması gerekir.

1. Terminali açın ve aşağıdaki komutu çalıştırın:

go install -v github.com/projectdiscovery/naabu/v2/cmd/naabu@latest

1. Kurulum tamamlandığında, Naabu ~/go/bin/ dizinine yüklenecektir. Bu dizinin sisteminizin PATH değişkenine ekli olduğundan emin olun. Değilse, aşağıdaki komutu ~/.bashrc veya ~/.zshrc dosyanıza ekleyin:

export PATH=$PATH:$(go env GOPATH)/bin

**Yöntem 2: Binary (Hazır Derlenmiş) Dosya ile Kurulum**

Go ile uğraşmak istemiyorsanız, projenin GitHub sayfasından işletim sisteminize uygun hazır derlenmiş dosyayı indirebilirsiniz.

1. [Naabu GitHub Releases](https://www.google.com/url?sa=E&q=https%3A%2F%2Fgithub.com%2Fprojectdiscovery%2Fnaabu%2Freleases) sayfasına gidin.
2. İşletim sisteminize (Linux, Windows, macOS) uygun olan .zip dosyasını indirin.
3. İndirdiğiniz dosyayı arşivden çıkarın.
4. Çıkan naabu dosyasını sisteminizde komutların çalıştığı bir dizine (örneğin Linux için /usr/local/bin) taşıyın.

# Örnek Linux komutları

wget https://github.com/projectdiscovery/naabu/releases/download/v2.1.9/naabu\_2.1.9\_linux\_amd64.zip

unzip naabu\_2.1.9\_linux\_amd64.zip

sudo mv naabu /usr/local/bin/

**4. Kullanım Parametreleri**

Naabu'nun kullanımı oldukça basittir. İşte en sık kullanılan parametreler:

* -host: Tarama yapılacak tek bir hedefi veya virgülle ayrılmış birden fazla hedefi belirtir. (-host example.com,test.com)
* -l (list): İçinde satır satır hedeflerin bulunduğu bir dosyanın yolunu belirtir.
* -p (ports): Taranacak portları belirtir.
  + Tek port: -p 80
  + Aralık: -p 80-443
  + Virgülle ayrılmış: -p 80,443,8080
  + Tüm portlar: -p -
  + En popüler X port: -top-ports 100
* -o: Çıktıyı belirtilen dosyaya yazar.
* -v: Ayrıntılı (verbose) çıktı modunu açar.
* -silent: Sadece sonuçları (açık portları) gösterir, başlangıç banner'ını gizler.
* -rate: Saniye başına gönderilecek paket sayısını belirler (hız ayarı).
* -passive: Shodan API'sini kullanarak pasif tarama yapar. (API anahtarı gerekir)
* -nmap-cli: Naabu'nun bulduğu açık portları doğrudan Nmap'e göndererek daha detaylı bir tarama (versiyon, script vb.) başlatır.

**5. Etkili Kullanım Örnekleri ve Açıklamaları**

Teoriyi pratiğe dökme zamanı! İşte Naabu'yu etkili bir şekilde kullanmanızı sağlayacak 5 senaryo:

**Örnek 1: Temel ve Hızlı Web Portu Taraması**

En basit kullanım senaryosudur. Tek bir hedefin en yaygın web portlarının açık olup olmadığını hızlıca kontrol etmek için kullanılır.

* **Komut:**

naabu -host example.com -p 80,443,8080,8443 -v

* **Açıklama:**  
  Bu komut, example.com hedefi üzerinde 4 adet yaygın web portunu (80, 443, 8080, 8443) tarar. -v parametresi sayesinde, Naabu'nun taramaya başladığını ve ilerlemesini gösteren bilgileri de ekranda görürüz. Sonuç olarak sadece açık olan portlar listelenir.

**Örnek 2: Bir Hedef Listesindeki En Popüler 100 Portu Tarama ve Sonuçları Kaydetme**

Elinizde subfinder gibi bir araçla oluşturduğunuz yüzlerce alt alan adından oluşan bir liste olduğunu varsayalım. Bu listedeki tüm hedeflerin en sık kullanılan 100 portunu taramak isteyebilirsiniz.

* **Komut:**

naabu -l hedefler.txt -top-ports 100 -o acik\_portlar.txt

* **Açıklama:**  
  naabu, hedefler.txt dosyasındaki her bir hedefi alır (-l). Her hedef için en popüler 100 portu tarar (-top-ports 100). Bulduğu tüm hedef:port şeklindeki sonuçları acik\_portlar.txt dosyasına kaydeder (-o). Bu, geniş ölçekli ilk keşif için mükemmel bir yöntemdir.

**Örnek 3: Gücün Zirvesi: Subfinder, Naabu ve Httpx Zinciri (Pipelining)**

Bu, Naabu'nun ve Project Discovery ekosisteminin gerçek gücünü gösteren senaryodur. Tek bir komut satırıyla bir alan adının tüm web varlıklarını keşfederiz.

* **Komut:**

subfinder -d example.com -silent | naabu -silent | httpx -title -status-code

* **Açıklama:**
  1. subfinder -d example.com -silent: example.com'a ait tüm alt alan adlarını bulur ve -silent sayesinde sadece sonuçları ekrana basar.
  2. |: Pipe operatörü, Subfinder'ın çıktısını (alt alan adları listesini) bir sonraki komutun girdisi olarak gönderir.
  3. naabu -silent: Girdi olarak aldığı alt alan adlarının varsayılan portlarını (top 100) tarar ve sadece açık olan hedef:port çiftlerini bir sonraki komuta gönderir.
  4. |: İkinci pipe, Naabu'nun bulduğu açık portları Httpx'e gönderir.
  5. httpx -title -status-code: Girdi olarak aldığı hedef:port listesine HTTP/HTTPS isteği atarak hangilerinin web sunucusu olduğunu, HTTP durum kodunu (200 OK, 403 Forbidden vb.) ve sayfa başlığını (-title) tespit eder.  
     Sonuçta, tek bir satırla dakikalar içinde bir hedefin tüm aktif web sunucularının listesini elde etmiş olursunuz.

**Örnek 4: Gizli Keşif: Shodan ile Pasif Tarama**

Hedef sisteme hiçbir iz bırakmadan, güvenlik duvarlarına veya tespit sistemlerine yakalanmadan bilgi toplamak istediğinizde bu yöntem kullanılır.

* **Komut:**

naabu -host bugcrowd.com -passive

* **Açıklama:**  
  Bu komut, bugcrowd.com hedefine **hiçbir paket göndermez**. Bunun yerine, Naabu, Shodan'ın devasa veritabanına "Bugcrowd.com için daha önce hangi portları açık buldun?" diye sorar ve cevabı size gösterir. Bu özelliğin çalışması için Shodan API anahtarınızı ~/.config/projectdiscovery/config.yaml dosyasına eklemeniz gerekir.

**Örnek 5: Hızlı Keşif + Derin Analiz (Nmap Entegrasyonu)**

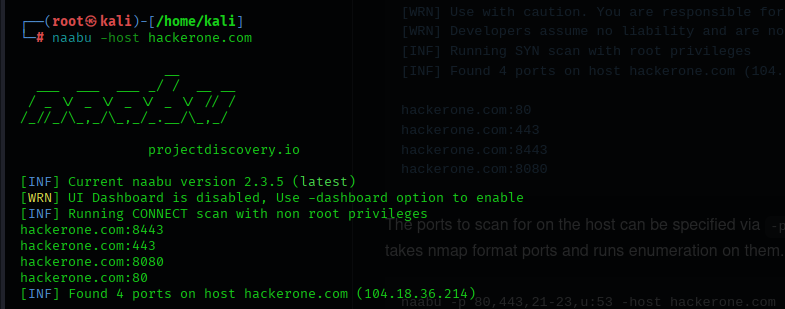
Naabu'nun hızını Nmap'in derin analiz yetenekleriyle birleştirmek, en verimli tarama yöntemlerinden biridir. Önce Naabu ile hızlıca açık portları bulur, sonra sadece o portları Nmap ile detaylıca inceleriz.

* **Komut:**

naabu -host scanme.nmap.org -top-ports 100 -nmap-cli "nmap -sV -sC"

* **Açıklama:**
  1. naabu -host scanme.nmap.org -top-ports 100: Naabu, hedefin en popüler 100 portunu çok hızlı bir şekilde tarar.
  2. -nmap-cli "nmap -sV -sC": Naabu, bulduğu açık portlar için otomatik olarak bir Nmap komutu oluşturur. Örneğin, 22 ve 80 portlarını açık bulursa, nmap -p 22,80 -sV -sC scanme.nmap.org komutunu çalıştırır. -sV ile servis versiyonlarını, -sC ile de varsayılan Nmap script'lerini çalıştırarak portta neyin çalıştığına dair detaylı bilgi toplar. Bu, "hızlıca bul, yavaşça analiz et" stratejisidir.

Örnek :



naabu aracı ile gerçekleştirilen port taraması sonucunda, *hackerone.com* alan adına ait 80, 443, 8080 ve 8443 portlarının açık olduğu tespit edilmiştir. Tarama işlemi non-root yetkileriyle gerçekleştirilmiş ve sonuçlar terminal çıktısı üzerinden alınmıştır. Bu tarama, hedef sistemde aktif servislerin belirlenmesine yönelik ön keşif adımının bir parçasıdır.

**Sonuç: Siber Güvenlik Cephaneliğinizin Yeni Gözdesi**

Naabu, modern siber güvenlik uzmanının ihtiyaç duyduğu hızı, basitliği ve entegrasyonu bir araya getiren güçlü bir araçtır. Tek başına etkili bir port tarayıcı olmasının ötesinde, Project Discovery ekosisteminin bir parçası olarak kullanıldığında potansiyelini tam anlamıyla ortaya koyar. Geniş ölçekli ağ keşiflerinden otomatize edilmiş güvenlik taramalarına kadar birçok alanda vazgeçilmez bir yardımcıdır. Eğer siz de keşif süreçlerinizi hızlandırmak ve daha verimli hale getirmek istiyorsanız, Naabu'yu siber güvenlik cephaneliğinize eklemenin tam zamanı.