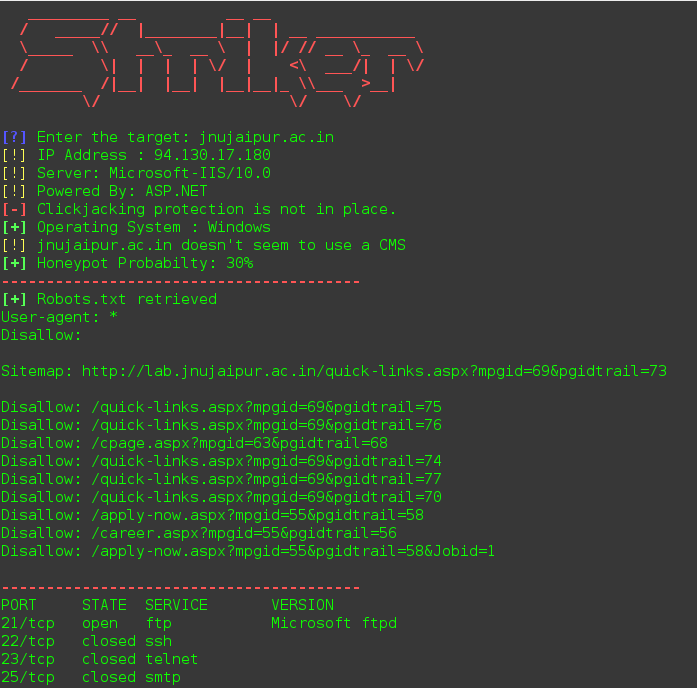
**1. Striker Nedir?**

**Striker**, hedef bir web sitesini analiz ederek onunla ilgili zafiyetleri, güvenlik yapılandırmalarını ve eksiklikleri otomatik olarak tarayan bir **bilgi toplama (recon) ve zafiyet analiz** aracıdır. Python ile yazılmıştır.



**2. Ne İşe Yarar?**

Striker, bir hedef web sitesine dair şu analizleri yapar:

* Güvenlik başlıklarını kontrol eder (HTTP security headers)
* Clickjacking zafiyeti olup olmadığını denetler
* SSL sertifika durumunu ve güvenliğini kontrol eder
* Açık portları ve kullanılan teknolojileri tespit eder
* WHOIS, DNS ve geolocation (coğrafi konum) bilgilerini çeker
* CORS (Cross-Origin Resource Sharing) yapılandırmasını denetler

Yani bir web sitesinin güvenliğine dair **birçok temel testi** otomatik şekilde tek araçla yapar.

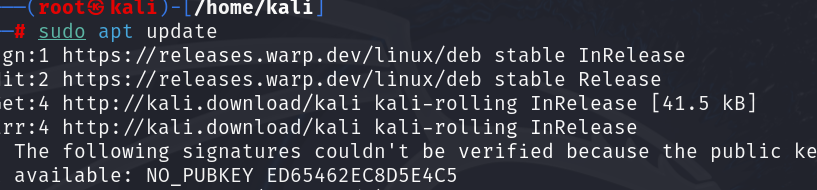
**3. Neden Önemlidir?**

* **Hızlı bir ilk analiz** yaparak güvenlik açıklarını gözler önüne serer.
* Pentester’lar ve güvenlik araştırmacıları için zaman kazandırır.
* Özellikle CORS, güvenlik başlıkları ve clickjacking gibi ihmal edilen alanları kontrol eder.
* Zafiyetleri düzeltmeden önce sistem sahipleri için rehber niteliğindedir.
* Otomatik ve sade çıktıları sayesinde hem yeni başlayanlar hem de uzmanlar için kullanışlıdır.

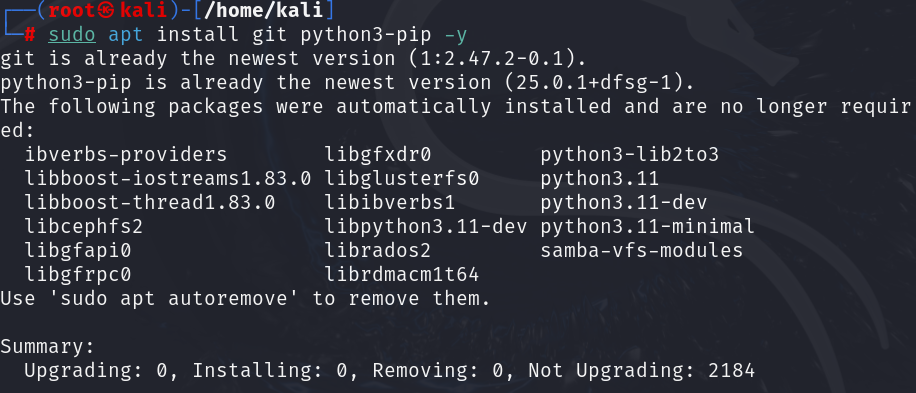
**4. Nasıl Kurulur?**

**Kali Linux / Debian tabanlı sistemler için:**

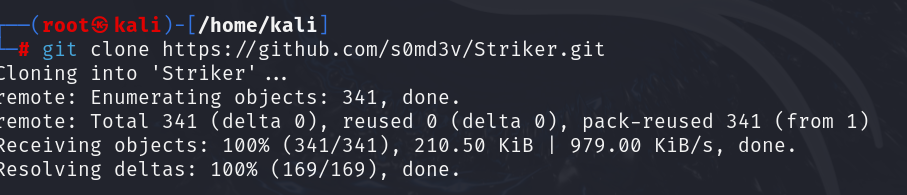
***1 - sudo apt update***

******

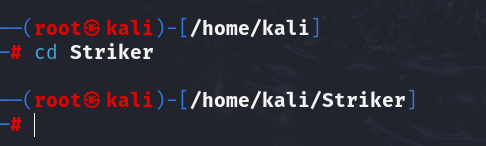
***2 - sudo apt install git python3-pip –y***



***3 - git clone https://github.com/s0md3v/Striker.git***

******

***4 - cd Striker***

******

***5 - pip3 install -r requirements.txt***

******

Eğer pip3 yüklü değilse:

***sudo apt install python3-pip***

**5. Örnek Bir Adım (Kullanım)**

***python3 striker.py -u*** [***http://example.com***](http://example.com)

******

Bu komut example.com sitesine karşı tarama yapar ve aşağıdakiler gibi bilgiler verir:

* Site HTTPS mi kullanıyor?
* Güvenlik başlıkları mevcut mu?
* CORS açık mı?
* Clickjacking yapılabilir mi?
* Kullanılan teknolojiler neler?