İSTANBUL GELİŞİM ÜNİVERSİTESİ

İSTKA- SİBER AKADEMİ

T-POT KURULUM VE KONFİGÜRASYONU

- **HAZIRLAYAN**
  HAYRUNNİSA ÜSTÜN

- **PROJE DANIŞMANLARI**

  SERKAN GÖNEN
  UĞUR KAYA
  GÖKÇE KARACAYILMAZ

İÇİNDEKİLER

1. GİRİŞ

Bu projenin temel amacı, T-Pot honeypot platformunun kurulumu ve etkin bir şekilde kullanılarak siber güvenlik tehditlerinin tespiti ve analizi konusunda derinlemesine bilgi edinmektir. Proje, şirketler, kurumlar veya bireylerin, ağlarını hedef alan siber saldırıları anlamalarına ve buna uygun savunma stratejileri geliştirmelerine yardımcı olmayı hedeflemektedir. Ayrıca, farklı honeypot teknolojilerinin uygulanabilirliğini araştırarak, ağ güvenliği seviyelerini optimize edecek bir altyapı oluşturulmasını sağlamak da projenin önemli bir parçasıdır.

2. T-POT NEDİR?

T-Pot, siber tehditlerin tespiti, analizi ve izlenmesi için geliştirilmiş bir honeypot platformudur. Deutsche Telekom Security tarafından açık kaynak olarak sunulan bu platform, çeşitli honeypot servislerini Docker tabanlı bir sistemde bir araya getirerek kullanıcıların siber saldırılara karşı daha iyi savunma mekanizmaları geliştirmesine olanak tanır. T-Pot, saldırgan davranışlarını yakından izlemek ve bu davranışlardan elde edilen verilerle savunma stratejilerini güçlendirmek için kullanılan etkili bir araçtır.

Avantajlar:

- **Kapsamlı Tehdit Analizi:** Birden fazla honeypot teknolojisi sayesinde çok yönlü tehdit algılama.
- **Kolay Görselleştirme:** Toplanan verilerin Kibana gibi araçlarla anlık olarak analiz edilmesi ve raporlanması.
- **Esneklik:** T-Pot, farklı servislerin birleştirilmesine olanak tanıyan modüler bir yapıya sahiptir.
- **Açık Kaynak:** Geliştirmeye ve özelleştirmeye uygun bir yapıda sunulur.
- **Farkındalık ve Eğitim:** Siber güvenlik uzmanları ve araştırmacılar için bir öğrenme platformu olarak kullanılabilir.

Dezavantajlar:

- **Yüksek Kaynak Tüketimi:** Birden fazla honeypot bileşeni çalıştırdığı için güçlü donanım gerektirebilir.
- **Saldırgan Tespiti:** Bazı saldırganlar honeypot kullanıldığını fark ederek yanıltıcı veri sağlayabilir.
- **Kurulum Zorluğu:** Teknik bilgi ve deneyim gerektiren bir süreçtir.
- **Gerçek Etki Analizi Eksikliği:** Honeypot ortamı, gerçek üretim sistemlerinden farklı olduğu için saldırıların gerçek etkilerini her zaman doğru yansıtamayabilir.

Bu özellikler göz önünde bulundurulduğunda, T-Pot, siber güvenlik stratejilerini güçlendirmek ve tehditleri anlamak için güçlü bir araçtır, ancak sınırlamalarıyla birlikte dikkatli bir şekilde kullanılmalıdır.

2.1. T-Pot'un Amacı

- Siber saldırganların yöntemlerini ve araçlarını anlamak.
- Tehdit analizi yaparak zararlı yazılımlar ve saldırı teknikleri hakkında bilgi toplamak.
- Ağ ve sistem güvenliğini artırmak için uygun savunma stratejileri geliştirmek.
- Çeşitli honeypot teknolojilerinin etkinliğini test etmek ve karşılaştırmak.
- Eğitim ve farkındalık yaratmak amacıyla siber güvenlik uzmanlarına gerçekçi saldırı senaryoları sağlamak.

2.2. Kullanım Alanları

- **Tespit İstihbaratı:** Yeni saldırı yöntemlerini öğrenmek
- **Siber Akademi Eğitimi:** Gerçek saldırılara pratik yapmak
- **Ağ Güvenliği:** Şirket ağlarının savunmasını güçlendirmek

T-Pot, özellikle araştırmacılar ve güvenlik uzmanları için kapsamlı bir honeypot çözümüdür.

2.3. Bal Küpü (Honeypot)

Bal küpü, diğer adıyla **honeypot**, siber güvenlikte kullanılan bir tuzak teknolojisidir. Amaç, saldırganların dikkatini gerçek sistemlerden uzaklaştırarak onları yanıltmak, saldırı yöntemlerini anlamak ve güvenlik açıklarını analiz etmektir. Honeypot, genellikle tehdit istihbaratı toplamak, ağ güvenliğini artırmak ve saldırganların motivasyonlarını anlamak için kullanılır.

2.4. T-Pot ve Bal Küpü (Honeypot) Arasındaki Farklar

Özellik	Honeypot	T-Pot
Tanım	Belirli bir saldırıyı yakalamak için tasarlanmış sistem.	Farklı honeypotları bir araya getiren bir platform.
Teknoloji Desteği	Tek bir protokol veya hizmet için çalışabilir.	Birden fazla honeypot hizmetini entegre eder.
Kapsam	Sadece belirli bir saldırı türünü izlemek için kullanılır.	Tüm ağ saldırı türlerini izleyebilecek bir sistem sunar.
Kullanım Kolaylığı	Genelde manuel yapılandırma gerektirir.	Önceden yapılandırılmış, Docker tabanlı kolay kurulum.
Veri Görselleştirme	Veri analizi ve görselleştirme genelde ek araç gerektirir.	Kibana ve Elasticsearch ile görselleştirme sağlar.
Hedef	Tek bir tehdit türüne odaklanır.	Geniş bir saldırı türü yelpazesini kapsar.

3. SİSTEM GEREKSİNİMLERİ

3.1 Donanım Gereksinimleri

- Minimum 8 GB RAM
- 4 Çekirdekli işlemci
- 128 GB depolama alanı

3.2 Yazılım Gereksinimleri

- Linux tabanlı bir sunucu işletim sistemi (Ubuntu 20.04 LTS önerilir)
- Docker ve Docker Compose

4.KURULUM

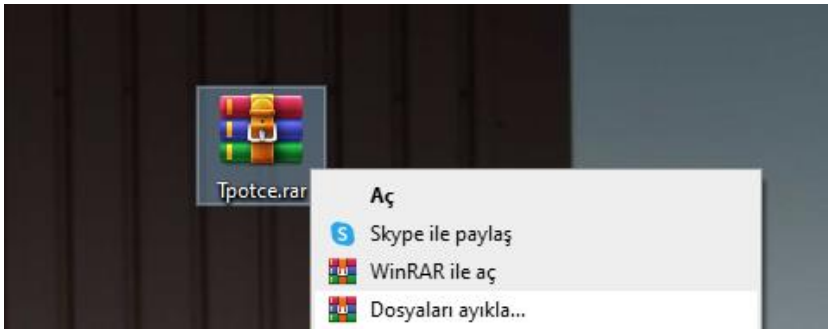
4.1. Hazırlık Aşaması

- Sistemin donanım gereksinimlerine uygunluğunu kontrol edin.
- İnternet bağlantısını sağlayın.

4.2. T-Pot Dosyasının İndirilmesi

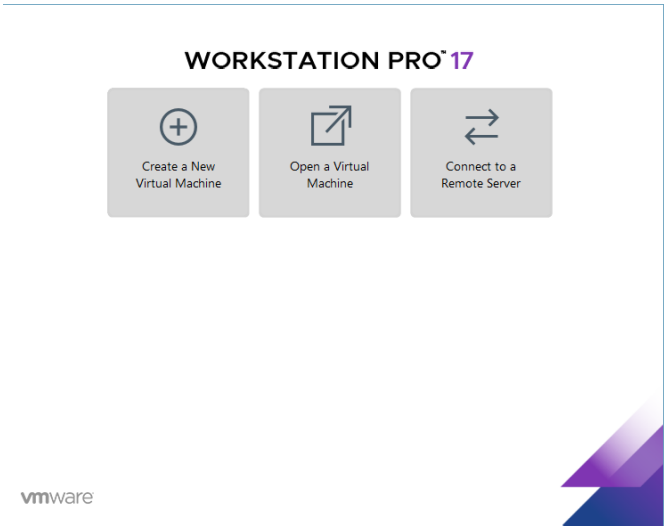
Kurulum **VMware Workstation Pro** üzerinden gerçekleştirilmektedir.
Öncelikle buraya tıklayarak indirme işlemini gerçekleştirin.

İndirilen uzantıyı **"dosyaları ayıkla"** yaparak dosya haline getirin.*(Fotoğraf 1.1)*



(Fotoğraf 1.1)

Dosyayı VMware üzerinden**"Open a Virtual Machine"** kısmından açarak kurulumu başlatın. *(Fotoğraf 1.2)*



(*Fotoğraf 1.2)*

Yükleme tamamlandıktan sonra ekrana gelen komut satırına "**cd tpotce**" yazıp tpot dizinine geçmesini sağlayın. Sonrasında " **./install.sh**" komutu ile indirmeye başlayın. *(Fotoğraf 1.3)*

(*Fotoğraf 1.3)*

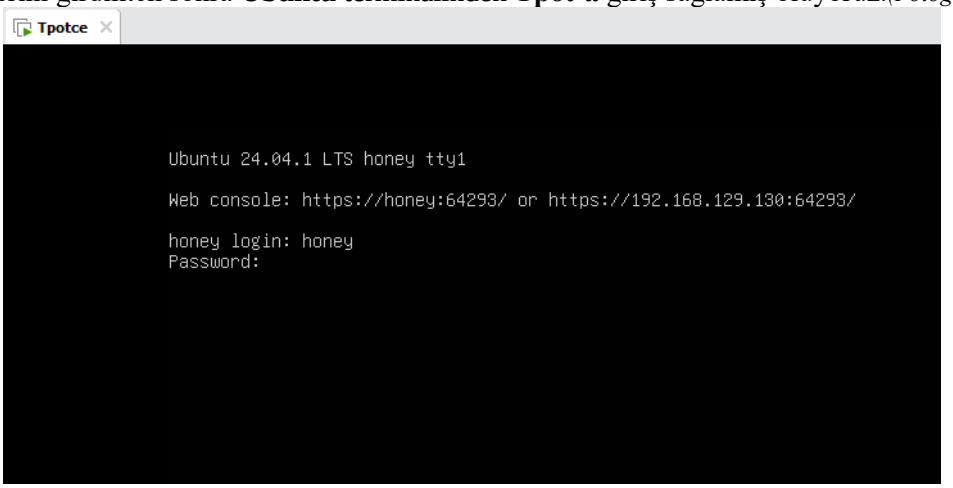
Gelen ekrandan indirme türünü **"s" (sensor)** olarak seçip indirme işlemini tamamlıyoruz. *(Fotoğraf 1.4)*

(*Fotoğraf 1.4)*

Ardından indirme işlemimiz tamamlanmış olup;

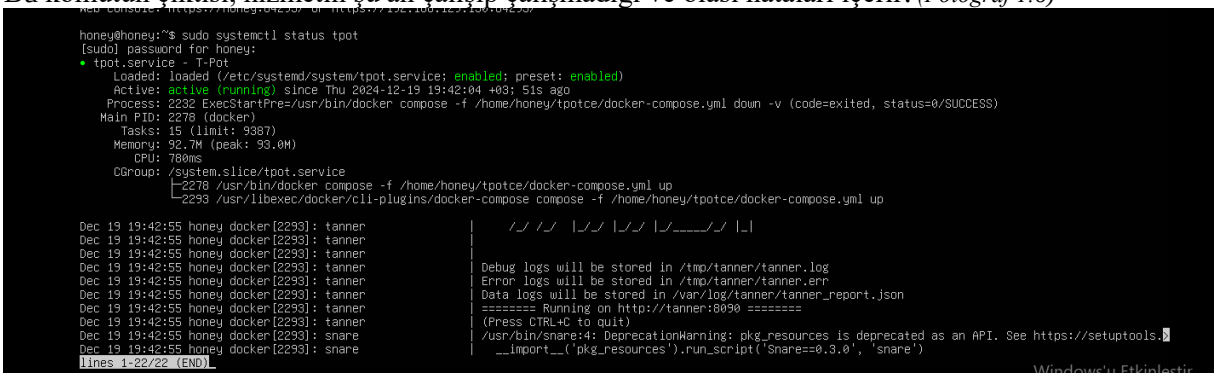
- ✧ **Honey login :** honey
- ✧ **Password :** honey

Giriş bilgilerini girdikten sonra **Ubuntu** terminalinden **Tpot'a** giriş sağlamış oluyoruz.*(Fotoğraf 1.5)*



(*Fotoğraf 1.5)*

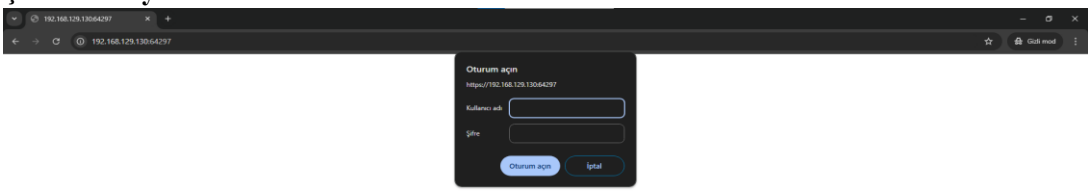
Eğer bir T-Pot Serverında "**sudo systemctl status tpot**" komutunu çalıştırırsanız, T-Pot hizmetinin durumunu görüntülersiniz.
Bu komutun çıktısı, hizmetin şu an çalışıp çalışmadığı ve olası hataları içerir. *(Fotoğraf 1.6)*



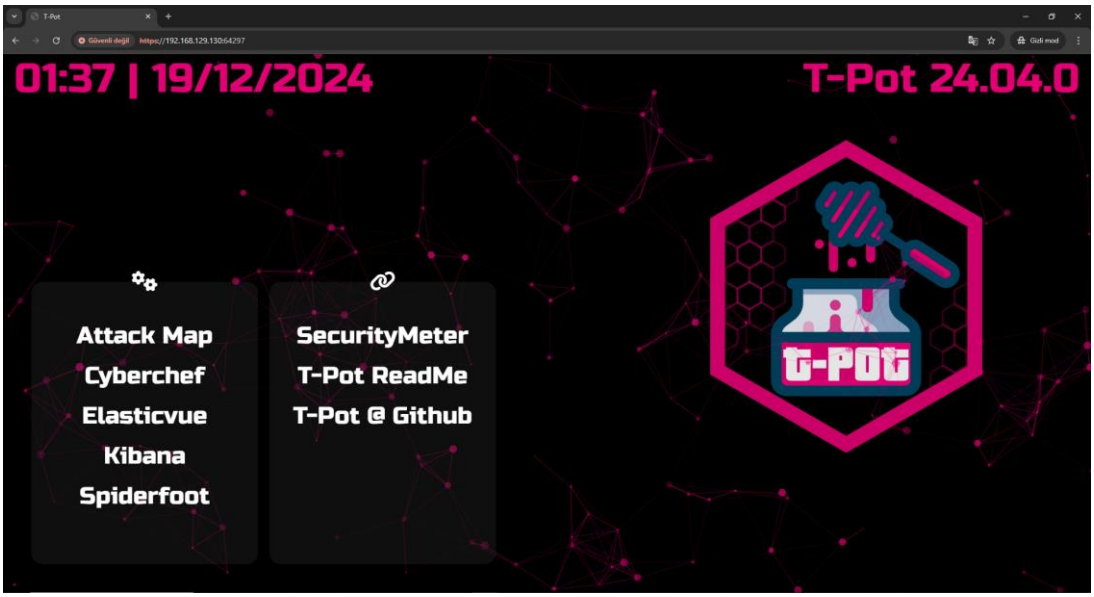
(*Fotoğraf 1.6)*

5.T-POT KULLANIMI

T-Pot'u VMware Workstation Pro üzerinden açıp, tarayıcı üzerinden (**Chrome, Firefox, Opera vb.**) erişim sağlamak için domain kısmına "https://<hedef ip>:64297" yazın.
Ardından karşınıza gelecek olan "Kullanıcı adı" ve "Şifre" kısmına;
Kullanıcı Adı: honey
Şifre: honey



yazarak **T-Pot** platformuna erişiyoruz.



5.1 Arayüz Tanıtım:

T-Pot Arayüzünde Attack Map

T-Pot arayüzünde bulunan Attack Map, bir honeypot ortamındaki saldırıların coğrafi ve görsel olarak analiz edilmesine olanak sağlar. Bu harita, sisteme yapılan kötü niyetli girişimlerin kaynaklandığı IP adreslerinin coğrafi konumlarını ve bu saldırıların hedeflerini görsel bir şekilde sunar.

T-Pot Arayüzünde CyberChef

T-Pot arayüzünde bulunan CyberChef, bir çeşit 'siber mutfak' olarak düşünülebilir. CyberChef, veri işleme ve analiz için bir araçtır ve çeşitli şifreleme, kodlama, dönüştürme ve veri analiz işlemlerini kolayca yapmanıza olanak tanır. T-Pot ortamında bu araç, özellikle saldırı verilerini analiz etmek ve hızlıca işlem yapmak için kullanışlıdır

CyberChef, T-Pot gibi bir honeypot sisteminde, saldırıların analizi ve hızlı veri işleme için ideal bir araçtır. Özellikle tehdit istihbaratı ya da veri temizleme işlemleriyle uğraşanlar için oldukça kullanışlıdır.

T-Pot Arayüzünde Elasticvue

T-Pot arayüzünde bulunan Elasticvue, bir **Elasticsearch** veritabanını yönetmek ve analiz etmek için kullanılan web tabanlı bir kullanıcı arayüzüdür. Elasticsearch, büyük miktarda veri depolamak ve aramak için kullanılan güçlü bir platformdur; Elasticvue ise bu verileri kolayca incelemenizi ve yönetmenizi sağlar.

Elasticvue, T-Pot tarafından toplanan saldırı günlüklerini ve veritabanını daha iyi anlamak, analiz etmek ve yönetmek için oldukça kullanışlıdır.

T-Pot Arayüzünde Spider Foot

T-Pot arayüzünde bulunan SpiderFoot, otomatik bir siber tehdit istihbaratı ve keşif aracıdır. Bu araç, hedef sistemler veya alan adları hakkında bilgi toplamak için tasarlanmıştır. SpiderFoot, özellikle saldırganların potansiyel hedefler hakkında nasıl bilgi topladığını anlamak veya kendi altyapınızın açıklarını keşfetmek için kullanılabilir.

SpiderFoot, tehdit istihbaratı, risk değerlendirmesi ve saldırı yüzeyinizi analiz etmek için güçlü bir araçtır.

T-Pot Arayüzünde Kibana

T-Pot arayüzünde Kibana, Elasticsearch tarafından depolanan verileri görselleştirmek, analiz etmek ve yönetmek için kullanılan güçlü bir açık kaynaklı analiz ve görselleştirme platformudur. Honeypot verilerinin izlenmesi, analiz edilmesi ve görsel raporlar oluşturulması gibi işlemler için T-Pot'un ayrılmaz bir parçasıdır.

Kibana'nın Özellikleri

1. **Görselleştirme:**
   - Grafikler ve Panolar (Dashboards): Bar grafikleri, pasta grafikleri, çizgi grafikleri ve coğrafi haritalar gibi görselleştirmelerle verilerinizi anlamlı hale getirir.
   - Gerçek Zamanlı İzleme: Veriler gerçek zamanlı olarak güncellenir ve anlık tehditleri analiz etmenizi sağlar.
2. **Log Analizi**:
   - Toplanan saldırı günlüklerini (logs) inceleyerek saldırıların detaylarını keşfetmenize yardımcı olur.
   - Örnek: Kaynak IP adresleri, kullanılan saldırı teknikleri, hedeflenen portlar ve protokoller gibi detayları kolayca analiz edebilirsiniz.
3. **Arama ve Filtreleme:**
   - Elasticsearch'ün güçlü sorgu dilini kullanarak karmaşık aramalar yapabilirsiniz.
   - Filtreleme: Belirli bir zaman aralığına, saldırı türüne, IP adresine veya diğer kriterlere göre verileri daraltabilirsiniz.

4. **Gelişmiş Analitik:**
   - Zaman içindeki saldırı trendlerini ve tehdit modellerini analiz ederek gelecekteki saldırılara hazırlanmanıza olanak tanır.
   - Örnek: Belirli bir saldırı türünün hangi zaman diliminde yoğunlaştığını keşfedebilirsiniz.

5. **Coğrafi Harita Desteği:**
   - IP adreslerinden elde edilen konum verilerini harita üzerinde görselleştirir.
   - Saldırıların kaynaklandığı bölgeleri ve hedeflenen coğrafyaları bir harita üzerinde analiz etmenizi sağlar.

6. **Kullanıcı Dostu Arayüz:**
   - Sürükle-bırak yöntemiyle kolayca görselleştirmeler ve panolar oluşturabilirsiniz.
   - Teknik bilgi gereksinimini en aza indirir, böylece farklı uzmanlık düzeylerindeki kullanıcılar da kolayca kullanabilir.

Kibana ile T-Pot Kullanım Senaryoları

1. **Saldırı Tespit ve Analizi:**
   - Sisteme yapılan saldırıların türünü, sıklığını ve hangi sistemleri hedeflediğini anlamak.
   - Örneğin, hangi portların en çok tarandığını ya da hangi ülkelerden saldırıların geldiğini analiz etmek.
2. **Güvenlik Durumunu İzleme:**
   - Honeypot sisteminin performansını ve güvenlik durumunu düzenli olarak kontrol etmek.
3. **Saldırı Yüzeyi Görselleştirme:**
   - Saldırganların sisteminiz üzerinde ne tür girişimler yaptığını görsel olarak anlamlandırmak.
4. **Raporlama ve Paylaşım:**
   - Otomatik olarak oluşturulan raporlarla yönetim ya da güvenlik ekiplerine düzenli bilgi sağlamak.

Kibana'nın Avantajları

- ✧ **Esneklik:** Farklı veri setlerini analiz etme ve özelleştirilmiş görselleştirmeler oluşturma imkanı sunar.
- ✧ **Hız:** Elasticsearch ile doğrudan entegre olduğu için büyük veri setlerini hızla işler.
- ✧ **Gerçek Zamanlı Güncellemeler:** Yeni gelen veriler otomatik olarak panolara yansır.
- ✧ **Özelleştirme:** Kendi panolarınızı, görsellerinizi ve sorgularınızı oluşturabilirsiniz.

6.SALDIRILAR

6.1 Nmap Nedir? Nmap Saldırısı Nedir?

Nmap (Network Mapper), ağ güvenliği denetimleri ve keşif amacıyla kullanılan açık kaynaklı bir yazılımdır. Temelde, bir ağda bulunan cihazları tarayarak onların durumunu incelemeye ve güvenlik açıklarını belirlemeye yarar. Nmap, ağdaki aktif cihazları, bu cihazların hangi portlarının açık olduğunu, hangi hizmetlerin çalıştığını, bu hizmetlerin hangi versiyonlarını kullandığını ve cihazların hangi işletim sistemlerini çalıştırdığını tespit edebilir. Nmap, genellikle güvenlik uzmanları tarafından ağ güvenliği testleri yapmak, ağdaki zayıf noktaları keşfetmek ya da ağ trafiğini izlemek amacıyla kullanılır.
Nmap saldırısı genellikle, Nmap aracını kullanarak yapılan bir ağ tarama ve keşif işlemidir. Nmap saldırıları, genellikle ağın savunmasız noktalarını belirleyerek, bu noktalara daha sonra yapılacak saldırıları kolaylaştırmak için kullanılır. Bu tür taramalar genellikle dikkatli yapılmalıdır, çünkü izinsiz taramalar yasal olmayan faaliyetler olarak kabul edilebilir ve ağ savunma sistemleri tarafından tespit edilip engellenebilir.

6.2 Brute Force Saldırısı Nedir?

Brute Force saldırısı, bir sistemin güvenliğini kırmak için yapılan ve deneme-yanılma yöntemine dayanan bir saldırı türüdür. Bu tür saldırılarda, saldırgan, hedefin şifresini veya erişim anahtarını bulana kadar tüm olası kombinasyonları tek tek deneyerek sistemin güvenliğini aşmaya çalışır. Bu tür saldırılar, güçlü şifreler kullanmayan sistemlere karşı oldukça etkili olabilir. Şifrelerin uzunluğu ve karmaşıklığı arttıkça, Brute Force saldırısının başarılı olması da daha zor hale gelir, çünkü denenecek kombinasyon sayısı hızla artar. Modern sistemler genellikle Brute Force saldırılarını tespit etmek ve engellemek için güvenlik önlemleri alır, örneğin çok sayıda başarısız girişimden sonra hesapları geçici olarak kilitlemek gibi.

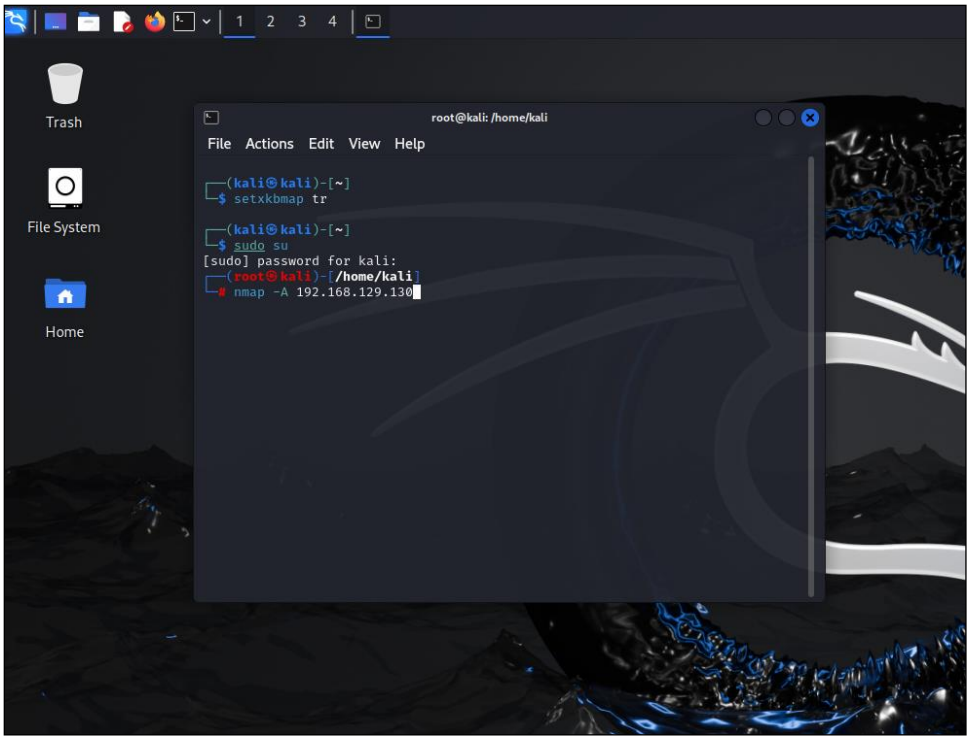
6.3 DDoS Saldırısı Nedir?

DDoS (Distributed Denial of Service) saldırısı, bir hedefi (genellikle bir web sitesi ya da ağ servisi) aşırı yükleyerek çalışamaz hale getirmeyi amaçlayan kötü niyetli bir saldırıdır. Bu tür saldırılar, birden fazla bilgisayar ve cihazdan gelen devasa trafikle gerçekleştirilir, bu da hedefin sunucusunun ya da ağına hizmet veremez duruma gelmesine yol açar. DDoS saldırısının hedefi, sunucunun kapasitesinin çok ötesinde bir trafik akışı yaratmak, bu sayede gerçek kullanıcıların erişimini engellemektir. Bu tür saldırılar, birçok şirket için büyük zararlara yol açabilir, çünkü ağ kaynaklarını tükettikleri ve hedef sistemin hizmet veremez duruma gelmesine neden oldukları için ciddi iş kesintilerine sebep olabilirler.

7.SALDIRI ANALİZLERİ

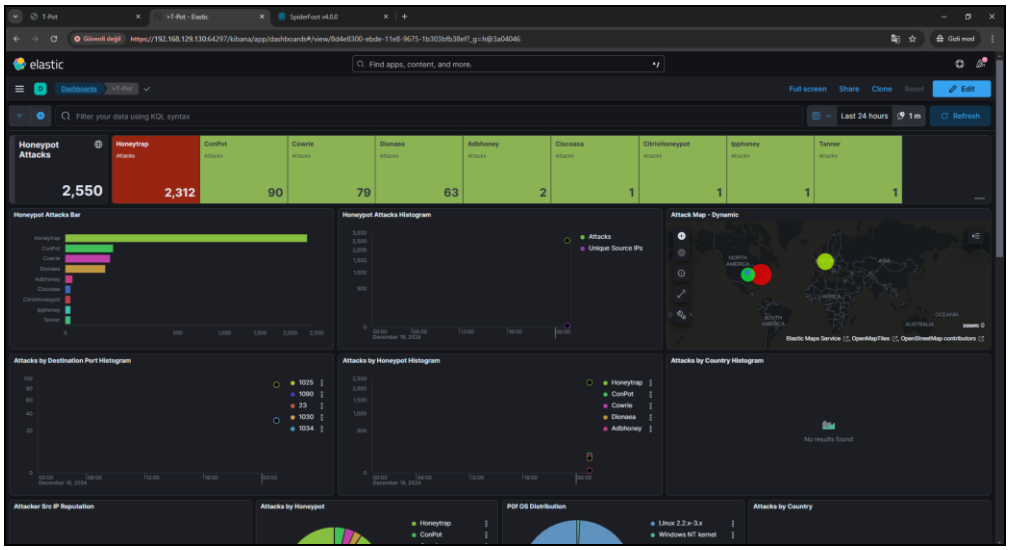
7.1 NMap Taraması:

Tarama yapmak için **Kali Terminaline** giriş yapıyoruz.
Komutumuzun doğru çalışması için "sudo su" yazdıktan sonra çıkan password kısmına "**kali**" yazıp, **Root**'umuzu (yani yetkimizi) alıyoruz.
Ardından "**nmap –A xxx.xxx.xxx.xxx (hedef ip'niz)**" komutunu çalıştırıyoruz.



7.1.1 NMap Tarama Analizi:

Yaptığımız taramayı **Kibana** üzerinden bu şekilde analiz ediyoruz.



7.2 Brute Force Saldırısı:

Hydra: Hydra, bir brute-force (kaba kuvvet) sızdırma aracıdır ve oturum açma bilgilerini test etmek için kullanılır. Bu komut ile hedef sistemde çalışan bir servise, özellikle şifre denemeleri yapılır**.**

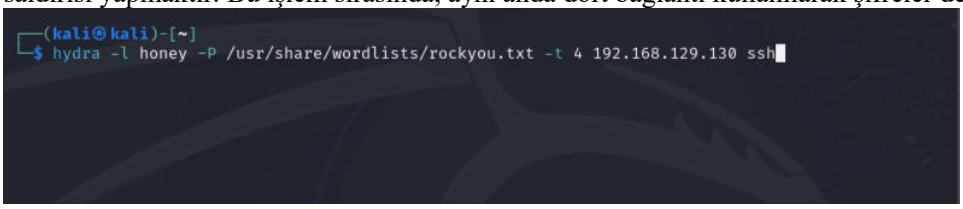
-l honey: -l bayrağı, hedefte test edilmek üzere kullanıcı adını belirtir. Bu örnekte, hedef sistemdeki kullanıcı adı "honey" olarak belirlenmiştir. Hydra, şifreleri sadece bu kullanıcı adı için deneyecektir.

-P /usr/share/wordlists/rockyou.txt: -P bayrağı, brute-force işlemi için şifrelerin bulunduğu bir kelime listesini belirtir. Burada kullanılan kelime listesi, yaygın şifreleri içeren ünlü bir liste olan **rockyou.txt** dosyasıdır.

-t 4: -t bayrağı, Hydra'nın aynı anda kaç paralel işlem (thread) yürüteceğini belirler. Bu komut için paralel işlem sayısı dört olarak ayarlanır. Bu, işlem hızını artırmakla birlikte algılanma riskini de arttırabilir.

192.168.129.130: Bu IP adresi, hedef sistemin adresini ifade eder. Komut, bu adresteki bir servisi hedef alarak oturum açma bilgilerini test eder.
ssh: Bu parametre, hedef sistemde test edilecek servisin protokolünü belirtir. Bu komut örneğinde hedef servis SSH (Secure Shell) protokolüdür. Hydra, belirtilen kullanıcı adı ve şifre kombinasyonlarını SSH portu üzerinden test edecektir.

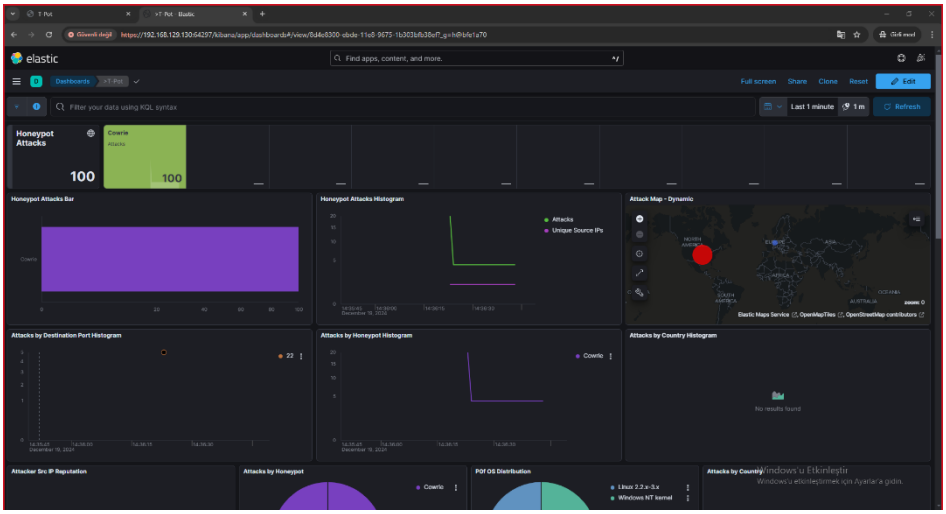
****Komutun Amacı**, 192.168.129.130 IP adresindeki bir SSH servisine yönelik olarak, "**honey**" kullanıcı adını hedef alıp **rockyou.txt** kelime listesindeki şifre kombinasyonlarıyla brute-force (kaba kuvvet) saldırısı yapmaktır. Bu işlem sırasında, aynı anda dört bağlantı kullanılarak şifreler denenir.*(Resim.b-f*s)*



(Resim.b-f*s)

7.2.1 Brute Force Saldırı Analizi:

Yaptığımız taramayı **Kibana** üzerinden bu şekilde analiz ediyoruz.***(Resim.b-f*a)***



(Resim.b-f*a)

7.3 DDoS Saldırısı

hping3: hping3, bir ağ analiz ve paket oluşturma aracıdır. Çeşitli protokoller (TCP, UDP, ICMP) kullanarak özel paketler oluşturabilir ve gönderebilir. Araç, genellikle ağ güvenliği testleri, trafiğini analiz etmek ve saldırı simülasyonları yapmak için kullanılır.

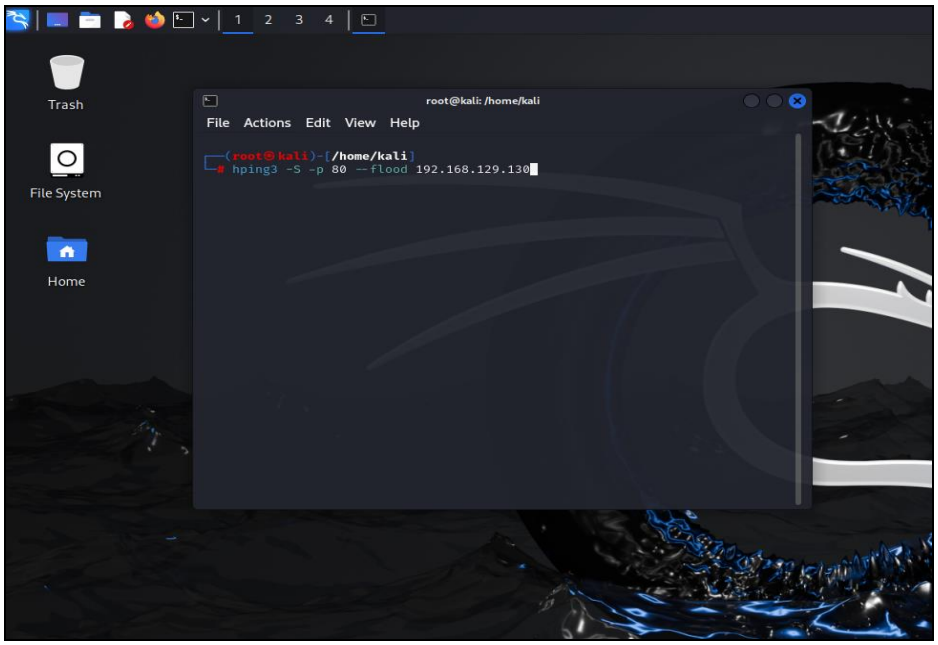
-S (SYN bayrağı): Bu parametre, TCP protokolü üzerinden gönderilecek paketlerde SYN (synchronize) bayrağını etkinleştirir. SYN bayrakları, bir TCP el sıkışmasının (handshake) başlangıç aşamasını temsil eder ve genellikle hedef sistemi yeni bir TCP bağlantısı başlatmaya zorlar.

-p 80 (Port 80): Bu parametre, hedef portu belirtir. Bu örnekte, hedef sistemdeki **80 numaralı port** hedeflenmiştir. Port 80, web sunucuları tarafından yaygın olarak HTTP trafiği için kullanılır.

--flood (Flood Modu): Bu parametre, hping3 aracının hedef sisteme maksimum hızda ve durmaksızın paketler göndermesini sağlar. Bu, ağ üzerinde çok yoğun trafik oluşturarak hedef sistemin kaynaklarını t t\u00fketmeye çalışan bir Denial of Service (DoS) saldırısının simülasyonudur.

192.168.129.130 (Hedef IP Adresi): Bu, hping3 tarafından paketlerin gönderileceği hedef IP adresidir. Bu komutta, hedef olarak yerel ağda bulunan **192.168.129.130** IP adresi belirlenmiştir.

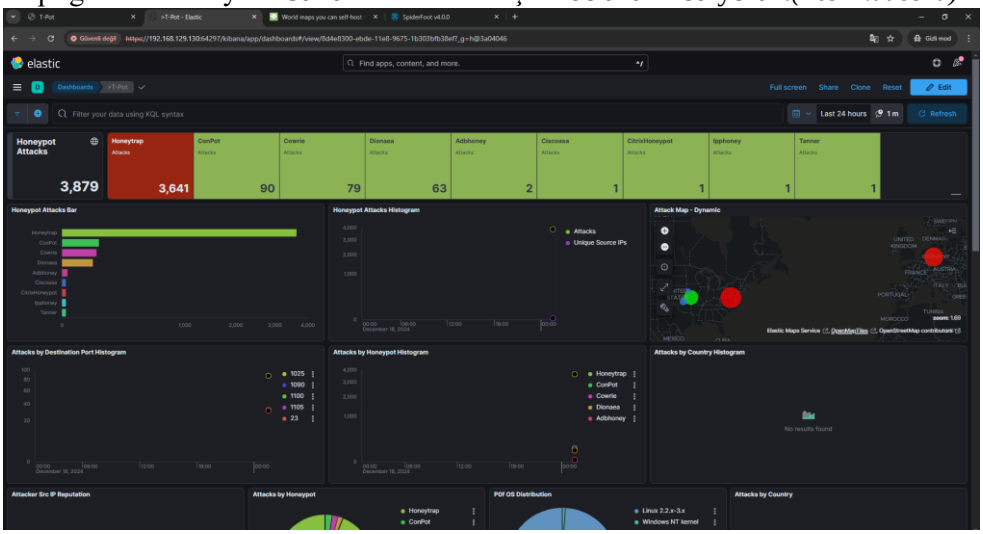
****Komutun Amacı**, **192.168.129.130** IP adresindeki bir sisteme TCP protokolü üzerinden SYN bayraklı paketler göndererek hedefin **80 numaralı portunu** yoğun bir şekilde trafiğe boğar. Bu işlem, hedef sistemin hizmet verememesine neden olabilecek bir DoS (Denial of Service) saldırısı simülasyonudur. *(Resim.ddos*s)*



(Resim.ddos*s)

7.3.1 DDoS Saldırı Analizi

Yaptığımız taramayı **Kibana** üzerinden bu şekilde analiz ediyoruz.*(Resim.ddos*a)*



(Resim.ddos*a)

8. API KEY

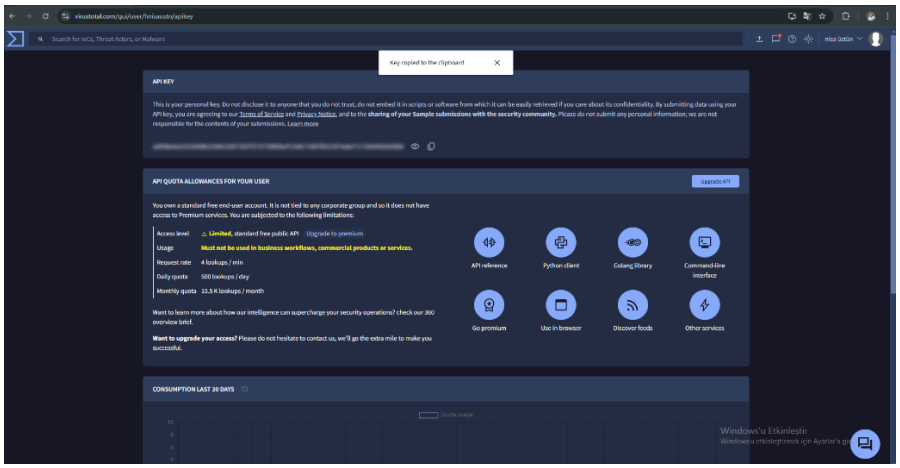
API Key (Uygulama Programlama Arayüzü Anahtarı), bir uygulamanın veya kullanıcının bir API'ye (Uygulama Programlama Arayüzü) erişim yetkisini doğrulamak için kullanılan benzersiz bir kimlik doğrulama kodudur.
Düşün ki, bir API kullanmak bir kulüp etkinliğine katılmak gibi. API Key de senin o etkinliğe giriş bileti! Bu anahtar sayesinde:

1. API sağlayıcısı, kim olduğunuzu bilir.
2. Verilere veya servislere ne kadar erişim hakkınız olduğunu kontrol eder.
3. Güvenliği sağlamak için kötüye kullanımları ve yetkisiz erişimleri engeller.

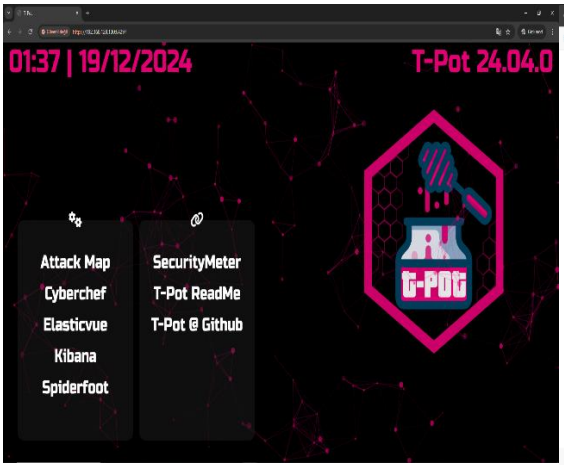
Özetle, API Key, bir uygulamanın doğru bir şekilde ve güvenle bir API ile iletişim kurmasını sağlar.

8.1 API Key Etkinleştirme

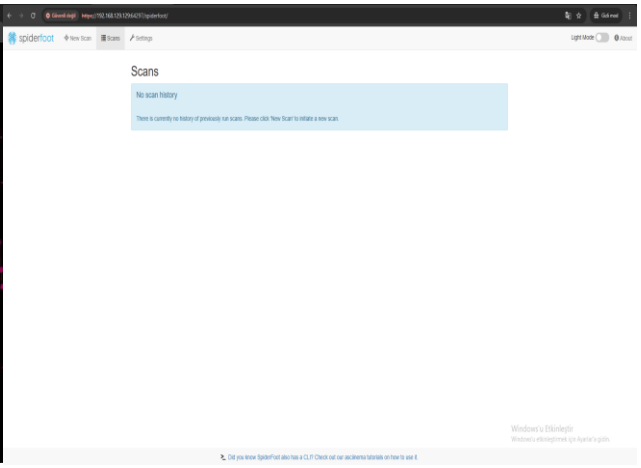
API Key almak için öncelikle **Virüs Total** sitesine kayıt oluyoruz. Ardından profil sekmemiz ya da E-Postamıza bize ait **API Key**'imiz gelmiş oluyor ve bunu kopyalıyoruz.



Kopyaladıktan sonra tarayıcı üzerinden **T-Pot** arayüzüne giriyoruz ve **SpiderFoot**'a erişim sağlıyoruz.

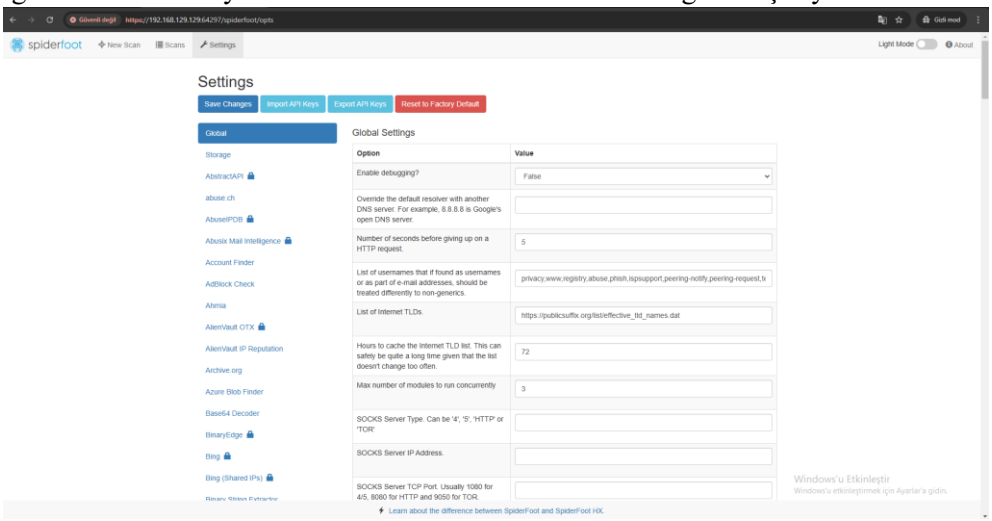


T-Pot Arayüz Ekranı

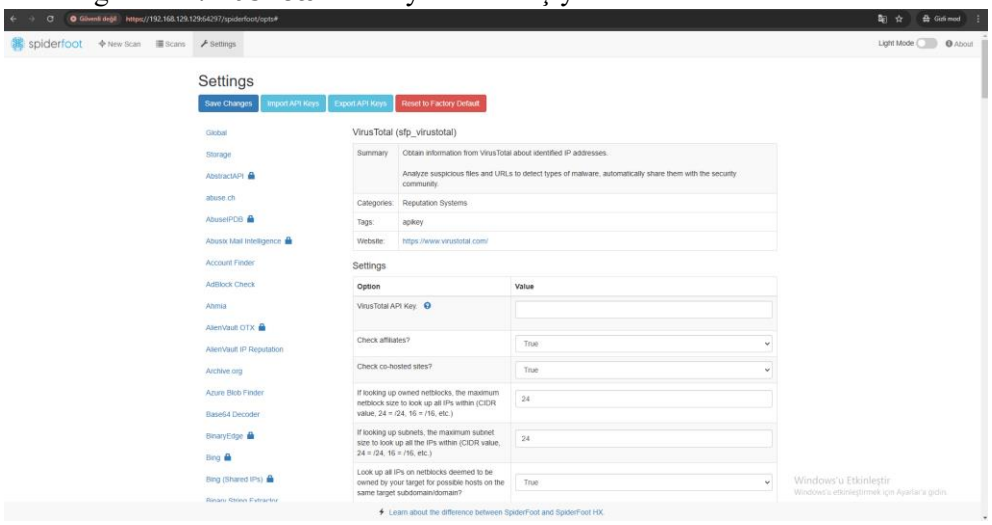


SpiderFoot Arayüz Ekranı

SpiderFoot'a erişim sağladıktan sonra karşımıza "No Scan History" adında mavi bir uyarı çıkıyor. "Settings"e basarak ilerliyoruz ve ekranımızın sol tarafında kategoriler çıkıyor.

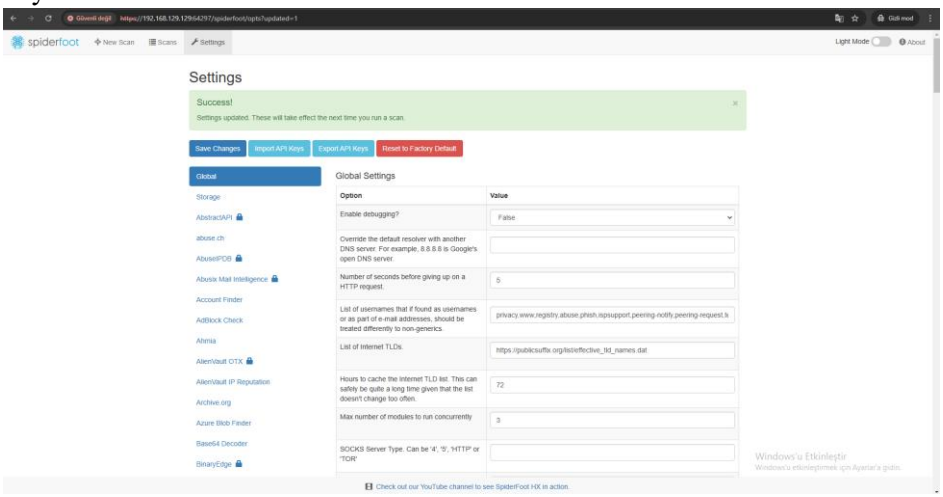


Şimdi bu kategoriden **VirusTotal**'i buluyoruz ve seçiyoruz.

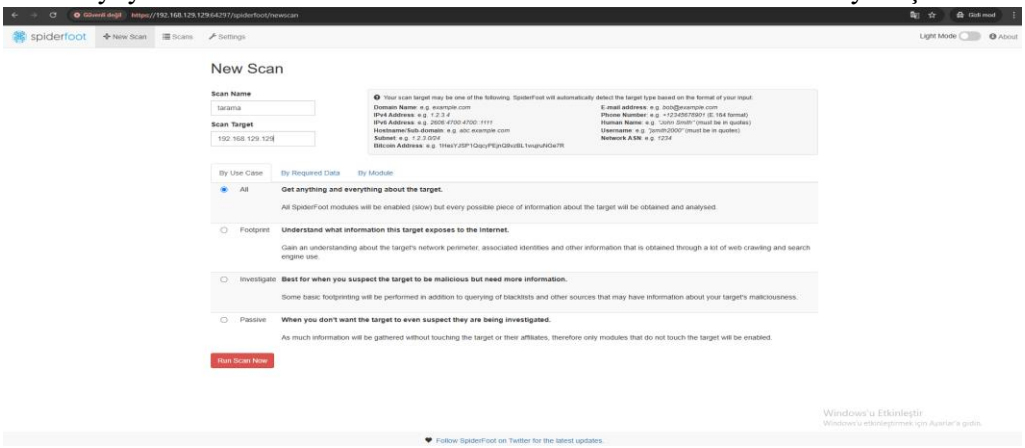


Seçtikten sonra orta kısımda bulunan "**VirusTotal API Key**" kutucuğuna kopyaladığımız API Key'imizi yapıştırıyoruz.

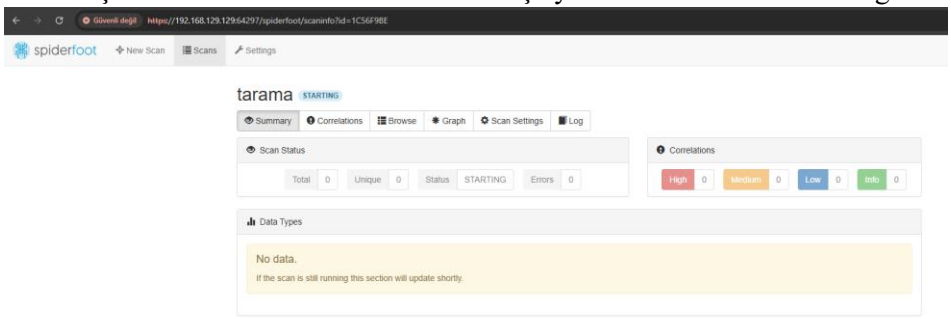
Ardından "**Save Changes**" butonuna basıyoruz. "**Success**" uyarısı geldiğinde **API Key**'imizi aktif etmiş oluyoruz.



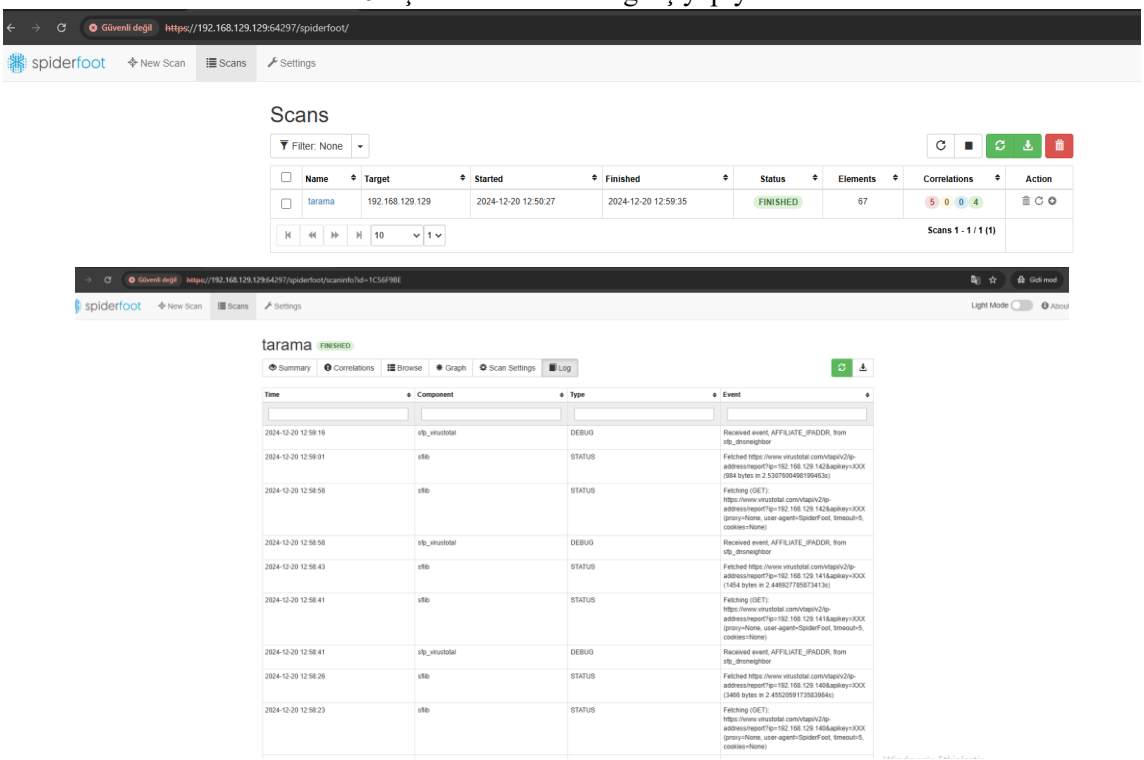
Şimdi "**New Scan**" butonuna basarak **Scan Name** ve **Scan Target** kutucuklarımızı dolduralım. **Scan Name** kısımına istediğiniz adı vererek **Scan Target** kısmına geçelim ve **T-Pot**'umuzun IP'si neresi ise o IP'yi yazalım ardından "**Run Scan Now**" butonuna basarak taramayı başlatalım.



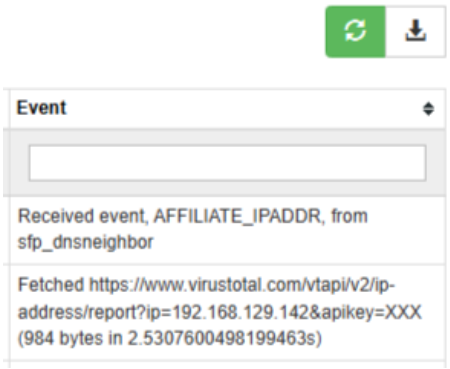
Tarama başladıktan sonra scans bölümünde başlayan ve biten taramalarımız gözükür.



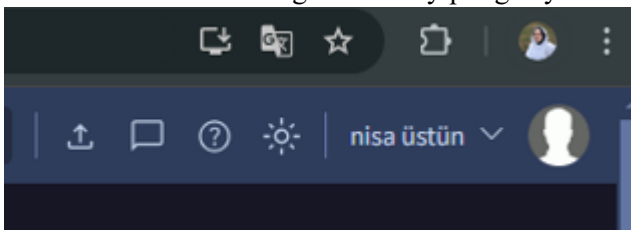
Bitmiş olan taramamıza giriş yapıyoruz.



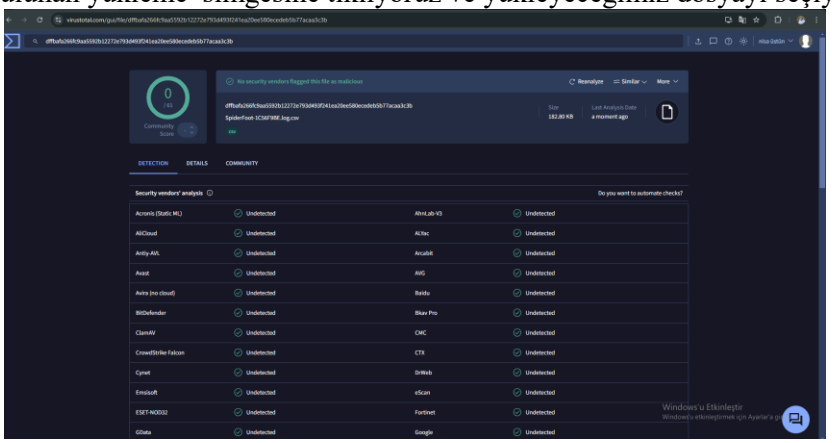
Açılan sayfadan üst menüdeki log kısmına tıklıyoruz.



Sağ üst tarafta bulunan indirme imgesine tıklayıp log kaydını indiriyoruz.



İndirdikten sonra **VirusTotal** web sitesine giriyoruz.
Sağ üst tarafta bulunan yükleme simgesine tıklıyoruz ve yükleyeceğimiz dosyayı seçiyoruz.



Yüklediğimiz log kayıdının analizini virus total sitesinde api key ile yapmış bulunmaktayız.

9.KAYNAKLAR

- ChatGPT
- Linkedin
- Medium
- GitHup
- Siber Akademi Ders Notları