



SİBER AKADEMİ PROJESİ

SANAL SUNUCU TABANLI SOC ÇALIŞMA ORTAMI

Gözde Yağızyılmaz

Sümeyye Erdoğan

20 ARALIK 2024

İSTKA-İGÜ

Siber Akademi



İÇERİK

Proje Kapsamı

Proje Yönetim Süreci / Trello

SCRUM

SOC Çalışma Ortamının Hazırlanması

T-POT Nedir? (Kurulum, Dashboard, İçerik)

Attack Map

Kibana Dashboard Tanıtımı

Saldırı Türleri

Saldırının Etkilediği Tpot Türleri

Splunk Nedir?

Splunk Analizleri

Spider Foot

Biz Kimiz?

Teşekkür

Proje Kapsamı

Bu proje, siber güvenlikte saldırganları tuzağa düşürmek ve onların yöntemlerini analiz etmek amacıyla oluşturulan Honeypot sisteminin sanal ortamda kurulması ve tptolara düşen saldırıların analizinin Splunk tarafından izlenmesini içeriyor.

Projenin amacı;

Gerçek bir hedefmiş gibi davranışan, güvenlik açıklarına sahip, ancak aslında izleme ve analiz amacıyla kullanılan bir sistemin sunucusu üzerinde kurulması,

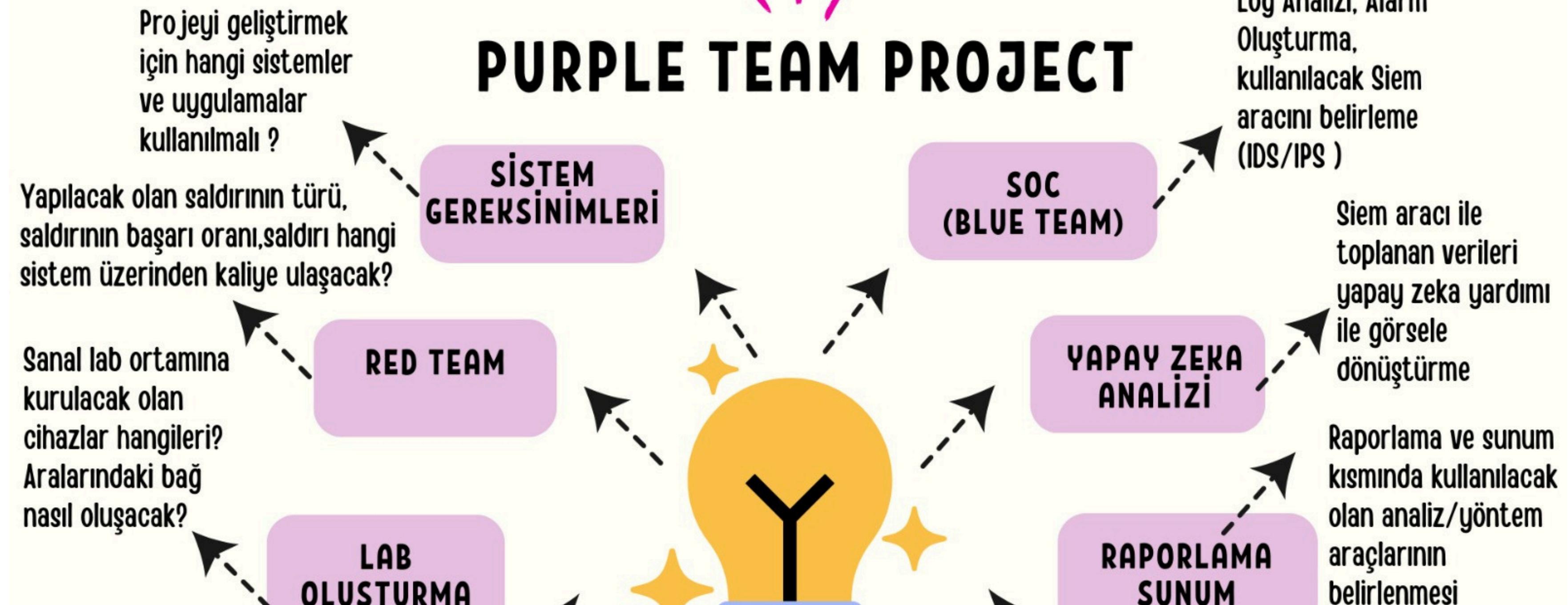
Saldırganlar bu sahte sisteme saldırdığında, onların davranışları ve saldırı tekniklerinin kaydedilmesi ve analizi,

Yapılan analizler sonucu elde edilen bilgilerin, güvenlik açıklarını kapatmak ve savunma stratejilerini geliştirmek için kullanılması.

Bu çalışmanın, siber güvenlik topluluğuna katkı sağlaması ve gelecekte daha güvenli bir dijital ekosistemin inşasına destek olması dileğiyle.



PURPLE TEAM PROJECT



Proje Yönetim

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 ettik.

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.



S

W

O

T

SWOT analizi, bir işletmenin, projenin veya organizasyonun mevcut durumunu ve gelecekteki potansiyelini anlamak için kullanılan stratejik bir planlama yöntemidir.

Güçlü Yönler

- Sanal Sunucu Ortamı
- Uygulama Çeşitliliği
- Analiz yapabilme
- Sektörde en çok kullanılan uygulamar
- Dashboard ekranı oluşturma
- Saldırı çeşitliliği
- Hibrit test ortamı
- Otomatik veri aktarımı

Zayıf Yönler

- Alt yapıdan kaynaklı oluşabilecek sorunlar
- Sunucu maliyeti

Fırsatlar

- İş imkanı
- Gerçek zamanlı tehdit izleme
- Hızlı aksiyon alma
- Projede yer almak isteyen kişi sayısının fazla olması

Tehditler

- Rakipler
- Dış Bağlantılı müdahale

SOC Çalışma Ortamının Hazırlanması

- Proje içeriği belirlendikten sonra Danışman hocalar ile yapılan görüşmelerin sonucunda topoloji oluşturuldu. İkinci aşamada kullanılacak olan uygulamalar belirlendi.

VMWARE

KALI LINUX

UBUNTU SERVER

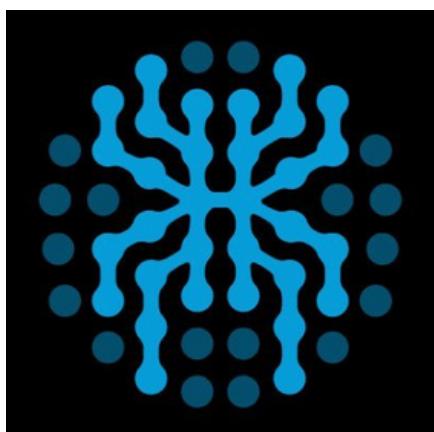
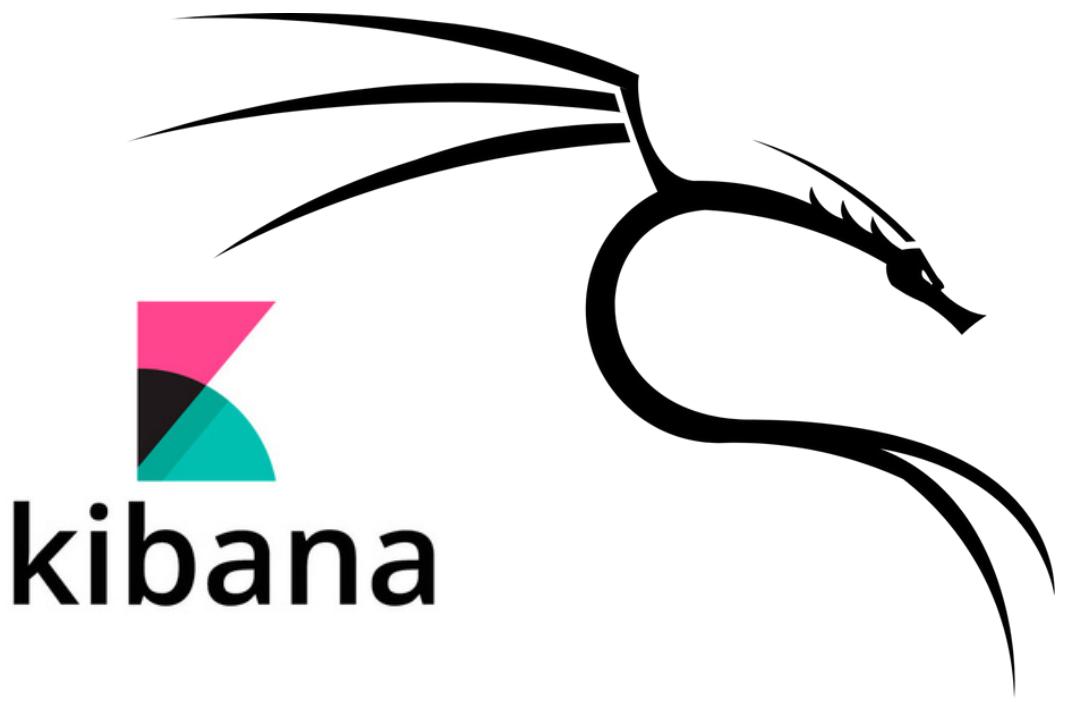
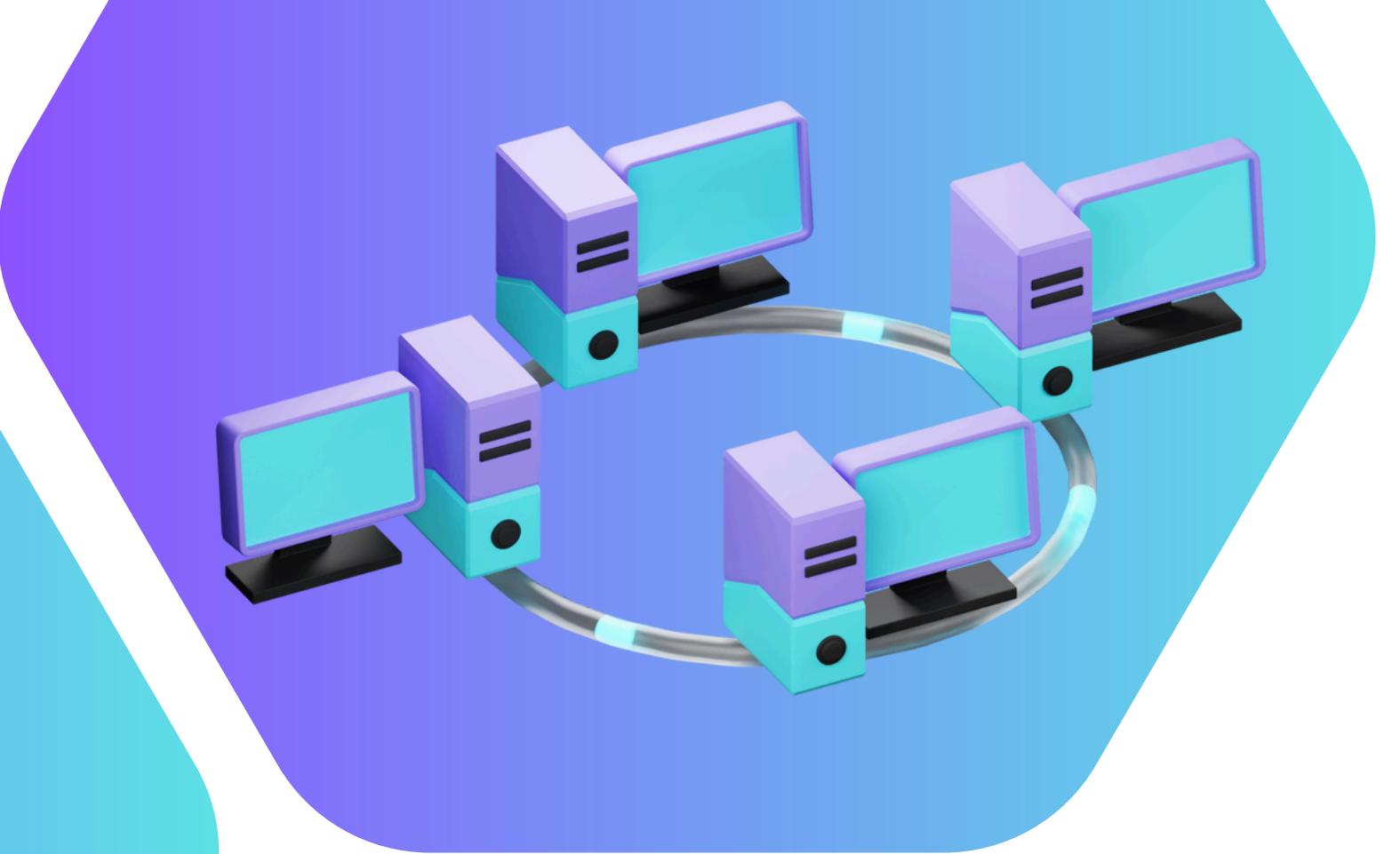
SPLUNK

T-POT

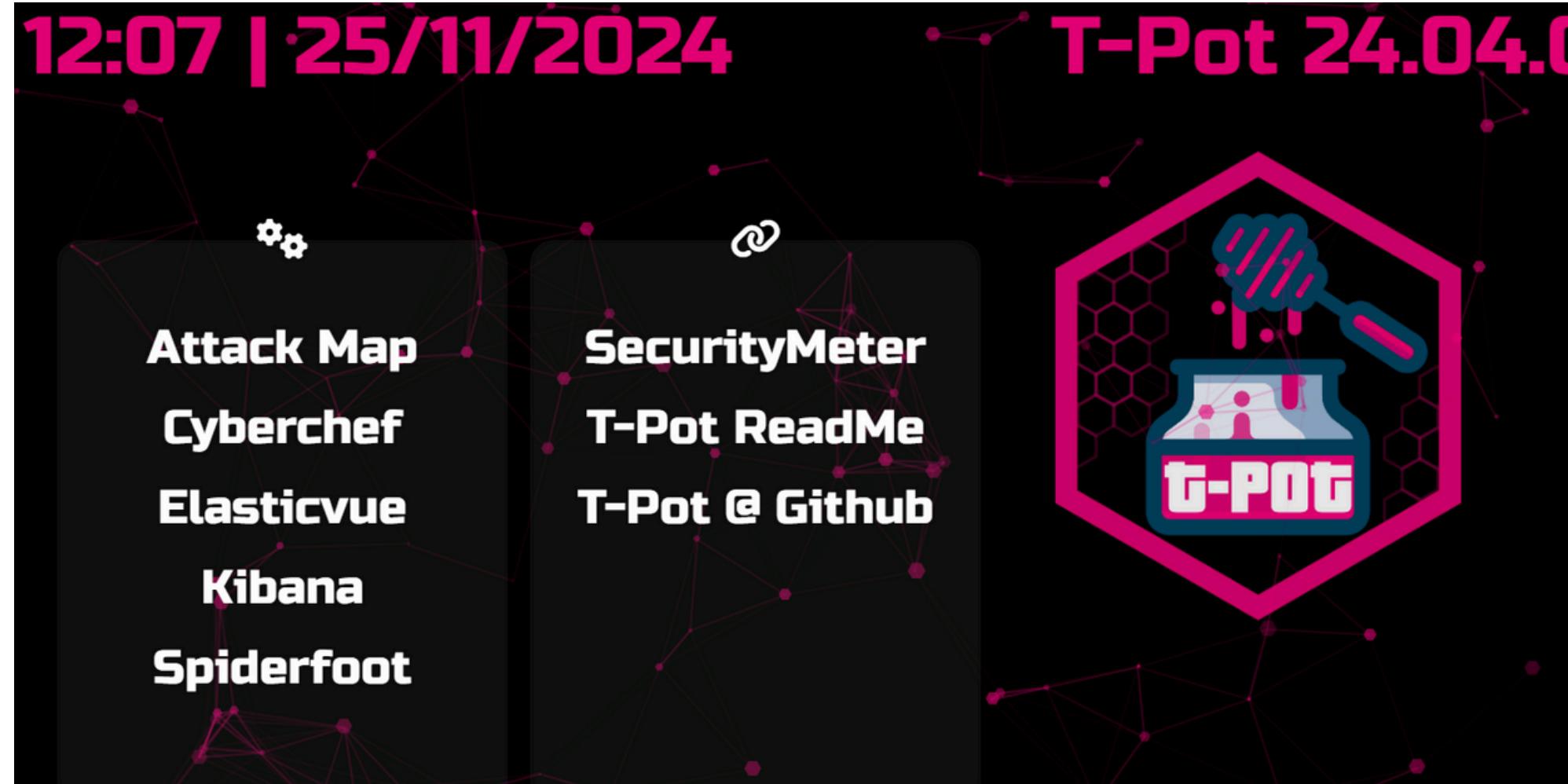
SPIDERFOOT

KIBANA

Hetzner şirketinden satın alınan sunucuya ubuntu server .iso olarak kuruldu. Sanal makina oluşturma imkanı tanıyan VMWare içerisinde Kali Linux kuruldu. Ubuntu server içerisinde t-pot ve splunk kurulumları yapıldı. 64297 ve 8000 portunda sistem ayağa kaldırıldı.



T-POT NEDİR?



Donanım Gereksinimleri:

Minimum 8 GB RAM.

En az 128 GB disk alanı.

Modern bir işlemci (x86_64).

Yazılım Gereksinimleri:

Ubuntu Server 22.04 LTS veya Debian tabanlı başka bir işletim sistemi.

Sunucuya root erişimi.

Internet bağlantısı.

Tanım

T-POT, genellikle siber güvenlik alanında kullanılan bir honeypot platformudur. Honeypot, saldırganları tespit etmek, analiz etmek veya aldatmak için tasarlanmış bir sistemdir. T-POT ise birçok farklı honeypot uygulamasını tek bir platformda birleştiren açık kaynaklı bir çözümüdür. Genellikle ağ güvenliği testleri ve tehdit analizi yapmak için kullanılır.

Kullanım Alanları

- Araştırma: Siber tehditleri anlamak ve analiz etmek.
- Eğitim: Siber güvenlik uzmanları için eğitim platformu.
- Tespit ve İzleme: Ağa yönelik saldırıları erken aşamada tespit etmek.

İçerdiği Uygulamalar

Cyberchef

Kibana

Spiderfoot

Attack Map

Elasticvue

```
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.
```



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

```
cybersecurity@ubuntu-2gb-nbg1-1:/root/tpotce$ ./install.sh
```



```
### This script will now install T-Pot and all of its dependencies.
```

```
### Install? (y/n) |
```

```
PLAY RECAP ****
127.0.0.1 : ok=42    changed=25    unreachable=0    failed=0
```

```
### Playbook was successful.
```

```
### 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: |
```

Active Internet connections (only servers)					
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
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

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

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

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

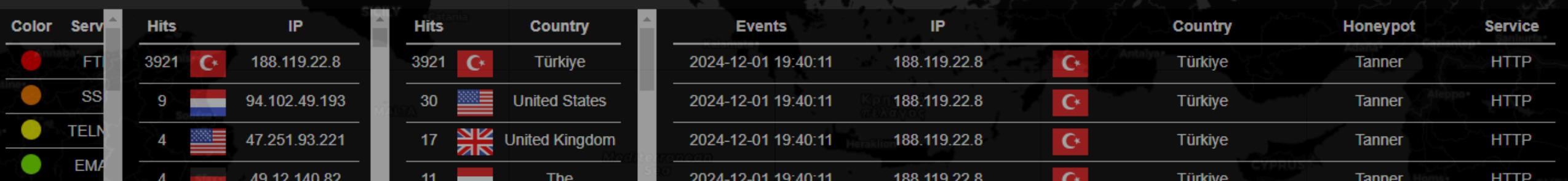
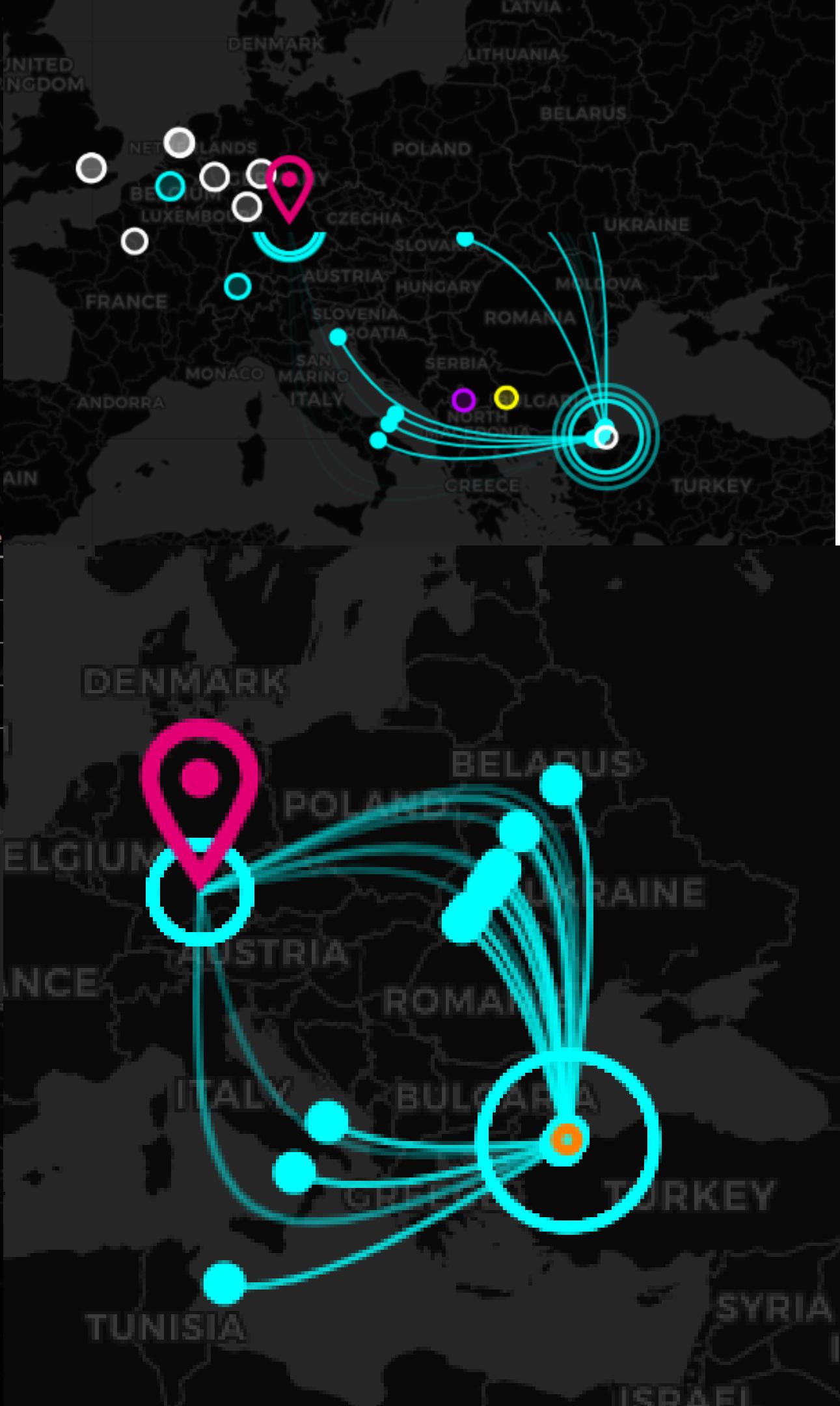
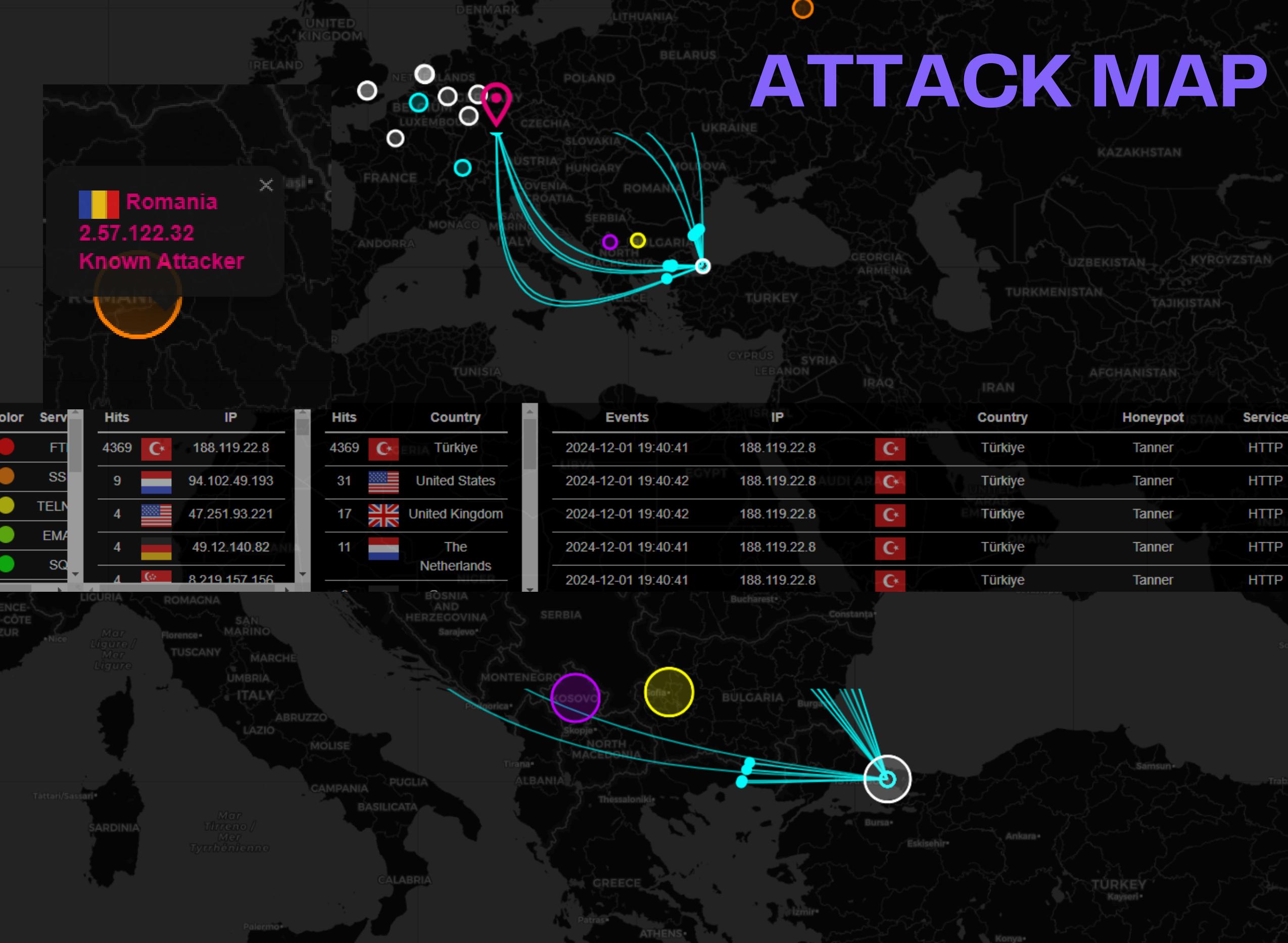
ATTACK MAP

Romania
2.57.122.32
Known Attacker

Color	Service	Hits	IP
●	FTI	4369	188.119.22.8
●	SS	9	94.102.49.193
●	TELN	4	47.251.93.221
●	EMA	4	49.12.140.82
●	SQ	4	8.219.157.156

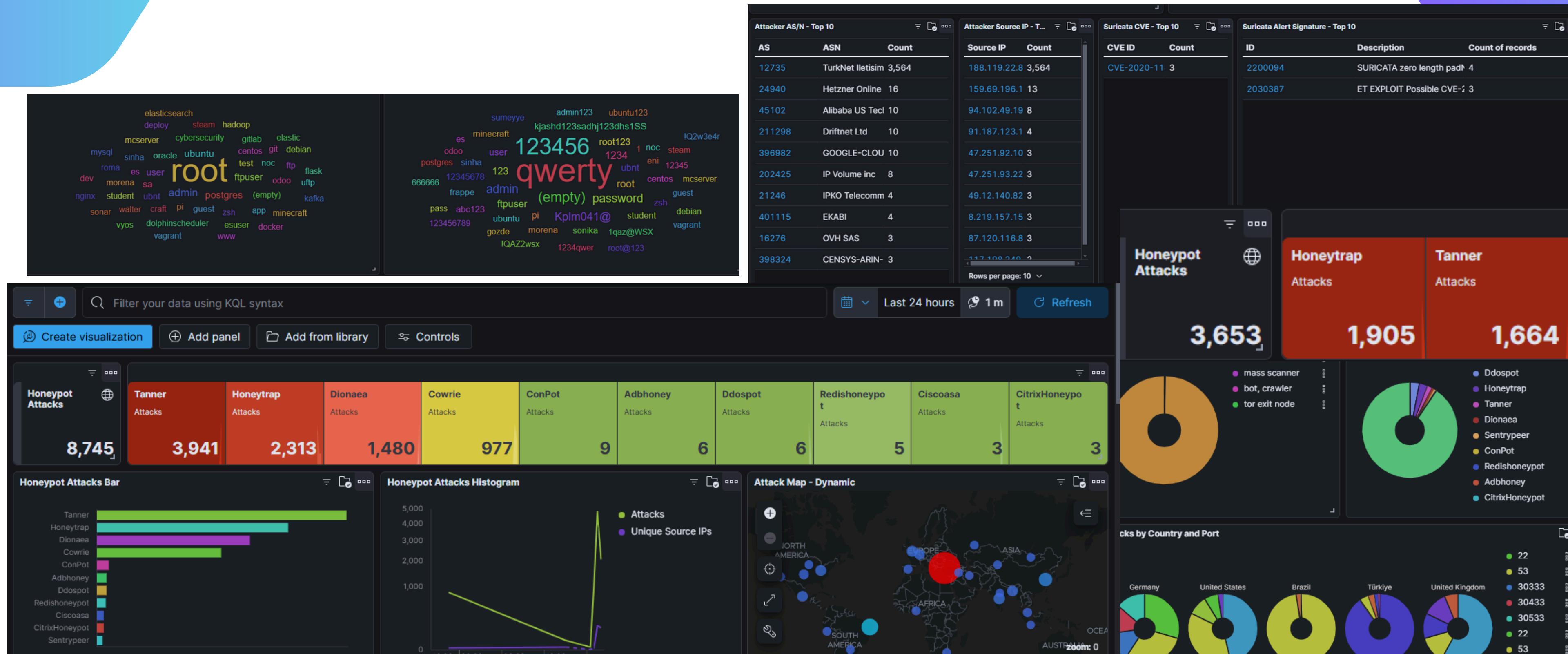
Color	Service	Hits	IP	Country
●	FTI	4369	188.119.22.8	Türkiye
●	SS	9	94.102.49.193	United States
●	TELN	4	47.251.93.221	United Kingdom
●	EMA	4	49.12.140.82	The Netherlands
●	SQ	4	8.219.157.156	Nigeria

Events	IP	Country	Honeypot	STAN	Service
2024-12-01 19:40:41	188.119.22.8	Türkiye	Tanner		HTTP
2024-12-01 19:40:42	188.119.22.8	Türkiye	Tanner		HTTP
2024-12-01 19:40:42	188.119.22.8	Türkiye	Tanner		HTTP
2024-12-01 19:40:41	188.119.22.8	Türkiye	Tanner		HTTP
2024-12-01 19:40:41	188.119.22.8	Türkiye	Tanner		HTTP



KİBANA DASHBOARD

Kibana, açık kaynaklı bir veri görselleştirme ve keşif aracıdır. Genellikle Elasticsearch ile birlikte kullanılır ve Elastic Stack'in (eski adıyla ELK Stack) bir parçasıdır. Kibana, kullanıcıların Elasticsearch'te depolanan verileri kolayca analiz etmelerini ve görselleştirmelerini sağlar.



SALDIRI TÜRLERİ

DdOS Saldırısı

Hping aracı ile yaptığımız ddos saldırılarını wireshark üzerinden izleyerek , paketlerin akışını gördük.

```
[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: root password: _olika  
[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: sumeyye  
[21][ftp] host: 159.69.196.102 login: morena password: sumeyye  
[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:
```

FTP Saldırısı

ftp üzerinden sistem açığını kontrol ederek, 21 numaralı porta saldırı gerçekleştirdik.

Sözlük Saldırısı

Sözlük saldırısı için Hydra aracını kullandık. Çeşitli parola ve kullanıcı isimlerinin bulunduğu gözlemledik.

Time	Source	Destination	Protocol
9.597129294	192.168.58.138	159.69.196.102	TCP
9.597171659	192.168.58.138	159.69.196.102	TCP
9.597199964	192.168.58.138	159.69.196.102	TCP
9.597242459	192.168.58.138	159.69.196.102	TCP
9.597271168	192.168.58.138	159.69.196.102	TCP
9.597313371	192.168.58.138	159.69.196.102	TCP
9.597341772	192.168.58.138	159.69.196.102	TCP
9.597383707	192.168.58.138	159.69.196.102	TCP
9.597412189	192.168.58.138	159.69.196.102	TCP
9.597454595	192.168.58.138	159.69.196.102	TCP

```
1: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface eth0  
Ethernet II, Src: VMware_2c:12:b5 (00:0c:29:b5:12:0b), Dst: Cybersecurity (00:0c:29:b5:12:0b)  
[ether] Src: VMware_2c:12:b5 (00:0c:29:b5:12:0b) [ethertype IPv4 (0x0800)]  
[proto] Version 4, Src: 192.168.58.138 [port 115], Dst: Cybersecurity [port 115]  
[app] Mission Control Protocol, Src Port: 115, Dst Port: 115  
0000 00 50 56 fe 09 72 00 0c 29 2c 1  
0010 00 a0 77 68 00 00 40 06 a4 11  
0020 c4 66 2d 11 00 50 79 02 b3 64  
0030 02 00 e2 1a 00 00 58 58 58 58  
0040 58 58 58 58 58 58 58 58 58  
0050 58 58 58 58 58 58 58 58 58  
0060 58 58 58 58 58 58 58 58 58  
0070 58 58 58 58 58 58 58 58 58  
0080 58 58 58 58 58 58 58 58 58  
0090 58 58 58 58 58 58 58 58 58  
00a0 58 58 58 58 58 58 58 58 58
```

Live capture in progress> Packets: 115054 · Displayed: 115054 (100%)

Brute Force

Kaba kuvvet saldırısı olan Brute Force saldırısını sistem üzerinde deneyerek kullanıcı adı ve parolarını ele geçirdik.

```
zsh: corrupt history file /home/gozde/.zsh_history  
[gozde@kalipurple)-[~]  
$ sudo su  
[sudo] password for gozde:  
[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
```

Saldırının Etkilediği T-POT Türleri



Tanner

Web sunucu veya web uygulama Honeypotudur. Http/https saldırılarının hedefidir. 80 ve 443 portunda çalışır.



Cowrie

Özellikle siber güvenlik tehditleri için hazırlanan ssh ve telnet bağlantılarını taklit eden modüldür. Ağ güvenliği uzmanları tarafından kullanılır. 22 /23 numaralı portlarda çalışır.



Sentrypeer

Temel amacı, VoIP sistemlerini dolandırıcılık, kötüye kullanım ve güvenlik açıklarından korumaktır. Ayrıca, çağrı trafiğini analiz etmek ve sistemlerin güvenliğini artırmak için kullanılır. (5060–5061)



honeytrap

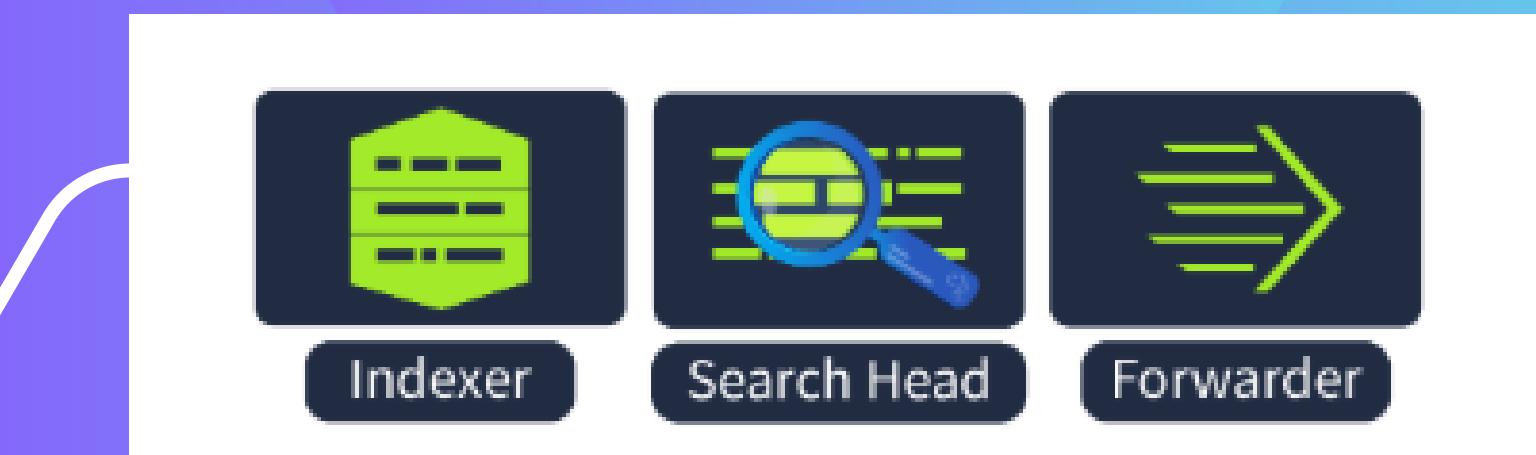
- Saldırganları cezbetmek için sosyal mühendislik amacıyla kullanılan modüldür. 22 (SSH): SSH brute-force saldırıları.
- 80 ve 443 (HTTP/HTTPS): Web tabanlı saldırılar.
- 21 (FTP): FTP protokolü üzerinden kimlik doğrulama denemeleri.
- 23 (Telnet): Zayıf parola saldırıları.
- 3306 (MySQL): Veritabanı saldırıları.
- 445 (SMB): Windows tabanlı dosya paylaşım protokollerine saldırılar.
- 53 (DNS): DNS tünelleme ve diğer saldırılar.



Splunk, veri analitiği ve sistem izleme için kapsamlı bir araçtır. Güvenlik, operasyonel mükemmellik ve iş zekası gibi alanlarda organizasyonlara değer katar. Hem teknik ekipler hem de iş birimleri için kritik bir araç olarak kabul edilir.

Splunk Çözümleri

- Splunk Enterprise: Büyük ölçekli veri analizi ve izleme.
 - Splunk Cloud: Bulut tabanlı veri analitiği.
 - Splunk IT Service Intelligence (ITSI): BT hizmetlerini izleme ve optimizasyon.
 - Splunk Phantom: Güvenlik otomasyonu ve olay müdahale.





```
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:f9c
1:d100:93a1, 2600:9000:20eb:5a00:1d: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]
```

```
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

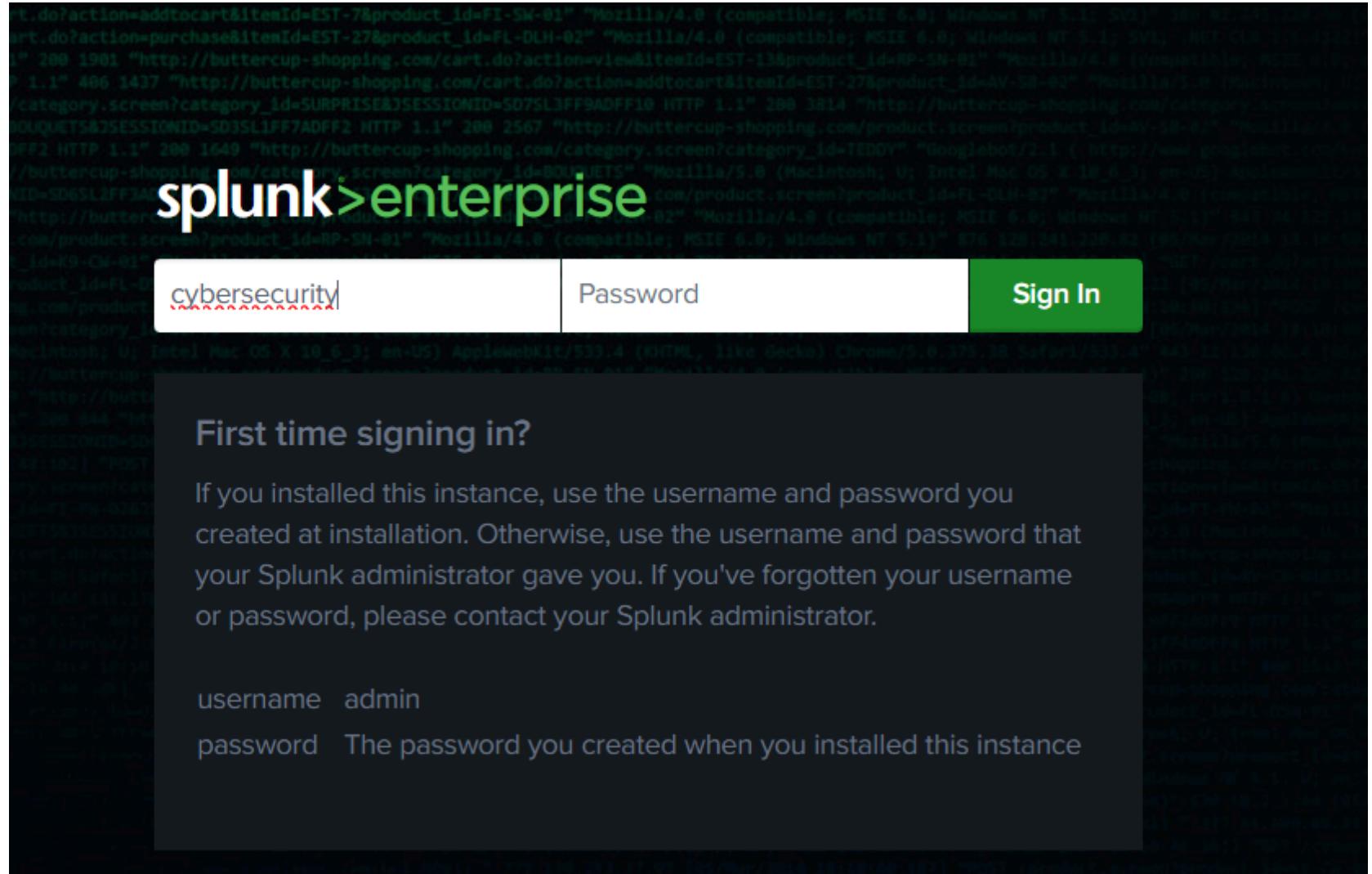
Last Updated: August 12, 2021
```

```
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'.
```

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



Add Data

Select Forwarders Select Source Input Settings Review Done < Back Next >

Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

Powershell v3 Modular Input
Execute PowerShell scripts v3 with parameters as inputs.

Select Event Logs

Available item(s) Application
ForwardedEvents Security
Setup System

Select the Windows Event Logs you want to index from the list.

FAQ

- > What event logs does this Splunk platform instance have access to?
- > What is the best method for monitoring event logs of remote Windows machines?

splunk>enterprise App: Search & Reporting

Input Settings

Optional set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

FAQ

- > How do indexes work?
- > How do I know when to create or use multiple indexes?

Index Default Create a new index

✓ Default

- history
- main
- summary
- win_logs**

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class New Existing

Available host(s) add all > Selected host(s) « remove all

WINDOWS coffelylab

New Server Class Name **coffely_lab**

Add Data

Select Forwarders Select Source Input Settings Review Done < Back Submit >

Review

Server Class Name coffelylab

List of Forwarders WINDOWS | coffelylab

Collection Name localhost

Input Type Windows Event Logs

Event Logs Application
Security
System

Index win_logs

etc

home

cybersecurity

tpotce

install_tpot.log

<input type="checkbox"/> Hide Fields	<input type="checkbox"/> All Fields	i	Time	Event						
		>	11/30/24 7:56:50.000 PM	{ [-] @timestamp: 2024-11-30T19:56:50Z attack_connection: { [+] } } download_count: 0 download_tries: 0 downloads: { [+] } } end_time: 2024-11-30T19:56:50Z is_virtual: false operation_mode: 1 proxy_connection: { [+] }						
				attack_connection.remote_ip						
				1 Value, 100% of events						
				Selected <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No						
				Reports						
				Top values Top values by time Rare values						
				Events with this field						
				<table border="1"> <thead> <tr> <th>Values</th> <th>Count</th> <th>%</th> </tr> </thead> <tbody> <tr> <td>188.119.22.8</td> <td>817</td> <td>100%</td> </tr> </tbody> </table>	Values	Count	%	188.119.22.8	817	100%
Values	Count	%								
188.119.22.8	817	100%								

honeytrap

attacks

downloads

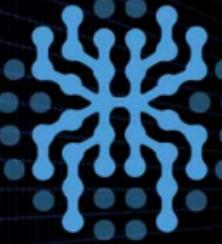
log

attacker.log

attackers.json

honeytrap.log

a/honeytrap/log/attackers.json | sourcetype = _json



spiderfoot

An Open Source Intelligence Automation Tool

SpiderFoot, açık kaynaklı istihbarat (OSINT – Open Source Intelligence) toplama ve analiz etme amacıyla kullanılan bir araçtır. Güvenlik araştırmacıları, siber tehdit analistleri ve diğer ilgili profesyoneller tarafından, bir hedef hakkında çevrimiçi kaynaklardan kapsamlı bilgi toplamak için kullanılır. Bu hedef bir kişi, şirket, IP adresi, alan adı veya başka bir varlık olabilir.

SpiderFoot'un Avantajları

- Kapsamlı Modüler Sistem: Farklı ihtiyaçlar için özelleştirilebilir.
- Otomasyon: İnsan müdahalesinе gerek kalmadan bilgi toplar.
- Açık Kaynak: Topluluk tarafından sürekli geliştirilebilir.
- Entegrasyon: Diğer güvenlik araçları ve veri kaynaklarıyla entegre olabilir.
- Platform Uyumluluğu: Linux, macOS ve Windows üzerinde çalışabilir.

SpiderFoot'un Dezavantajları

- Çok geniş bilgi toplaması, gereksiz verilerin analiz süresini artırmasına neden olabilir.
- API kullanımında bazı hizmetler için ücretli abonelik gerektirebilir.
- Yasal düzenlemeler ve etik kurallara uygun kullanım gerektirir.


[spiderfoot](#)
[!\[\]\(206ec7cb94545d8df1a21a109d9a7737_img.jpg\) New Scan](#)
[!\[\]\(32fc66e2d8433cfa95d8b14d0d5f1cc4_img.jpg\) Scans](#)
[!\[\]\(fb9e34bed8da5ee681b334a25cc7d089_img.jpg\) Settings](#)
Light Mode
[!\[\]\(846897bbc6d5ab869d97875203e48964_img.jpg\) About](#)

New Scan

Scan Name

Scan Target

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

Domain Name: e.g. example.com	E-mail address: e.g. bob@example.com
IPv4 Address: e.g. 1.2.3.4	Phone Number: e.g. +12345678901 (E.164 format)
IPv6 Address: e.g. 2606:4700:4700::1111	Human Name: e.g. "John Smith" (must be in quotes)
Hostname/Sub-domain: e.g. abc.example.com	Username: e.g. "jsmith2000" (must be in quotes)
Subnet: e.g. 1.2.3.0/24	Network ASN: e.g. 1234
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R	

[By Use Case](#)
[By Required Data](#)
[By Module](#)

All **Get anything and everything about the target.**

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

Footprint **Understand what information this target exposes to the Internet.**

Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate **Best for when you suspect the target to be malicious but need more information.**

Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

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

 spiderfoot  New Scan  Scans  Settings 

New Scan Scans Settings Light

Settings

[Save Changes](#) [Import API Keys](#) [Export API Keys](#) [Reset to Factory Default](#)

Global	
Storage	
AbstractAPI	Enable debugging? <input type="checkbox"/> False
abuse.ch	Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.
AbuseIPDB	Number of seconds before giving up on a HTTP request. <input type="text" value="5"/>
Abusix Mail Intelligence	List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics. <input type="text" value="abuse,maildaemon,devnull,dns,support,sysadmin,registry,noreply,compliance"/>
Account Finder	
AdBlock Check	
Ahmia	
AlienVault OTX	List of Internet TLDs. <input type="text" value="https://publicsuffix.org/list/effective_tld_names.dat"/>
AlienVault IP Reputation	Hours to cache the Internet TLD list. This can safely be quite a long time given that the list <input type="text" value="72"/>

Biz Kimiz ?



Sümeyye Erdoğan



Gözde Yağızyılmaz

Teşekkürler

