

T-Pot

Kurulum Rehberi

&

Splunk İlişkilendirmesi

Hazırlayanlar

Ertuğrul ÖZTOMSUK

Uğur KAYA

Zeynep Nur BAYRAM

Zümre ÖZTÜRK

İçindekiler

1. [Giriş](#)
 - 1.1 [HoneyPot](#)
 - 1.2 [T-POT The All In One Multi Honeypot Platform](#)
2. [Servisler](#)
3. [Kurulum](#)
4. [Arayüz Testi](#)
5. [Splunk](#)
6. [Splunk'ın T-Pot' a Entegrasyonu](#)
 - 6.1 [Dosya Dizininden Log Okunması](#)
 - 6.2 [Syslog İle Uzaktan Log Gönderilmesi](#)
7. [Kaynakça](#)

1.Giriş

1.1 T-POT Honeypot :

T-Pot honeypot (bal küpü) sistemi, birçok honeypot'u içerisinde barındıran bir honeypot aracıdır. İçerisinde barındırdığı honeypot'lardan (Cowrie, Dionaea, Conpot, CiscoASA Honeypot, ADBHoney, ElasticPot, Glutton, Heraldng, HoneyPy, Honeytrap, Malloney, Medpot, RDPY, Snare/Tanner) aldığı verileri toplar ve bu verileri merkezi bir şekilde bize sunar. Ayrıca elde edilen bilgilerin daha ayrıntılı şekilde analiz edilmesini sağlar.

Diğer Honeypotlardan Farkı Nedir:

Honeypotlar SCADA sistemleri dahil olmak üzere kullanım amaçlarına göre farklılık göstermektedir. T-POT Honeypot'u diğer honeypot'lardan ayırdığı en önemli özelliği, tek bir honeypot veya araç kullanmamasıdır. İçerisinde de ayrı servisleri çalıştıran birçok honeypot'u barındırması ile etkili bir Honeypot işlevi gerçekleştirmesine olanak sağlamaktadır. Ayrıca kullandığı Kibana yapısı ile görsel bakımdan anlaşılabilir bir grafik sunmaktadır. Kurulum esnasında Docker altyapısını kullanarak ayrı ayrı kurulum yerine, tek bir yerden kurulum imkanı da sağlamaktadır.

1.2 T-POT All In The One Multi Honey-Pot Platform

T-Pot, hepsi bir arada, isteğe bağlı olarak dağıtılan, çok farklı (amd64, arm64) bal küpü platformudur. 20'den fazla bal küpünü ve Elastic Stack, animasyonlu canlı saldırı haritaları ve aldatma deneyimini daha da geliştirmek için birçok güvenlik aracını kullanan sayısız görselleştirme seçeneğini destekler.

2. Servisler

T-Pot, temel olarak beş gruba ayrılan bir dizi hizmet sunar:

- İşletim sistemi tarafından sağlanan sistem hizmetleri
 - o Güvenli uzaktan erişim için SSH.
 - o Web tabanlı uzaktan erişim, yönetim ve web terminali için kokpit.
- Elastic Stack
 - o Olayları saklamak için Elasticsearch.
 - o Olayları almak ve Elasticsearch'e göndermek için Logstash.
 - o Kibana, olayları güzelce işlenmiş panolarda görüntülemek için.

- Tools

- o Kibana, CyberChef, Elasticvue, GeoIP AttackMap ve Spiderfoot'a güvenli uzaktan erişim (ters proxy) sağlamak için NGINX.
- o CyberChef şifreleme, kodlama, sıkıştırma ve veri analizi için bir web uygulaması.
- o Elasticvue, bir Elastic Search kümesine göz atmak ve bunlarla etkileşim kurmak için bir web ön ucu.
- o Geoip Attack Map, T-Pot için güzel animasyonlu bir saldırı haritası.
- o Spiderfoot, açık kaynaklı bir istihbarat otomasyon aracıdır.

- Honeypots

- o Seçilen sürüme ve / veya kurulumu göre mevcut 22 bal küpünden bir seçim.

- Ağ Güvenliği İzleme (NSM)

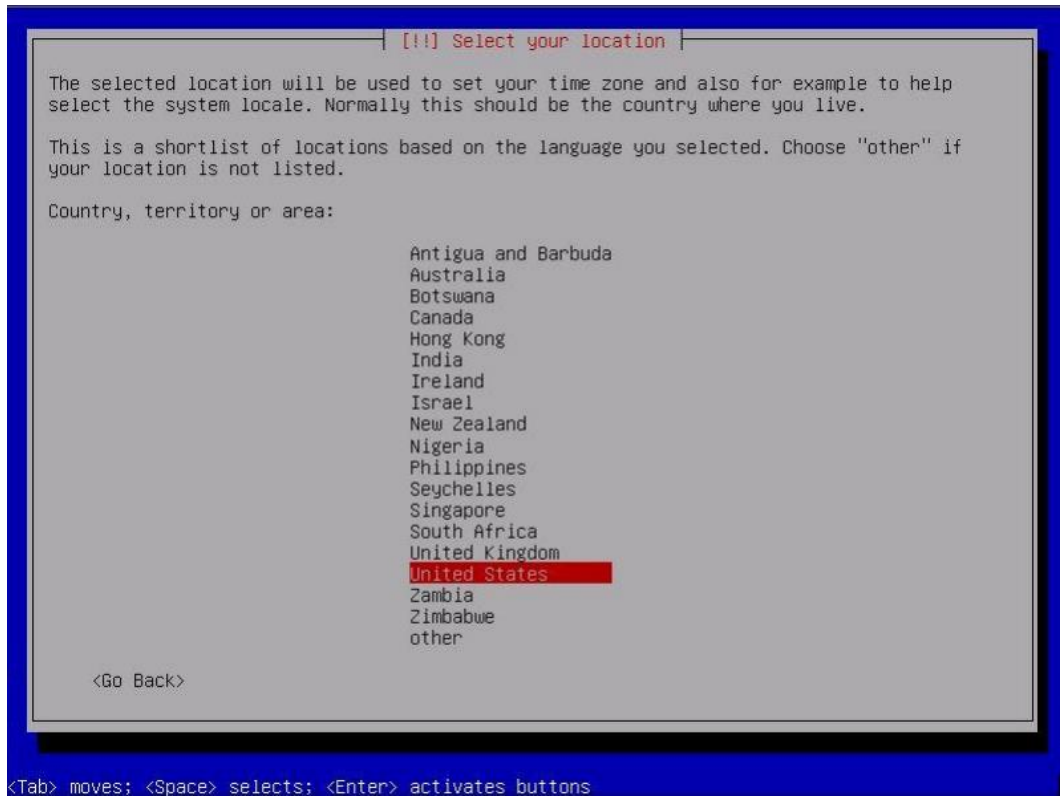
- o Fatt, pcap dosyalarından ve canlı ağ trafiğinden ağ meta verilerini ve parmak izlerini çıkarmak için pyshark tabanlı bir komut dosyası.
- o P0f, tamamen pasif trafik parmak izi için bir araçtır.
- o Suricata bir Ağ Güvenliği İzleme motoru.

3.Kurulum

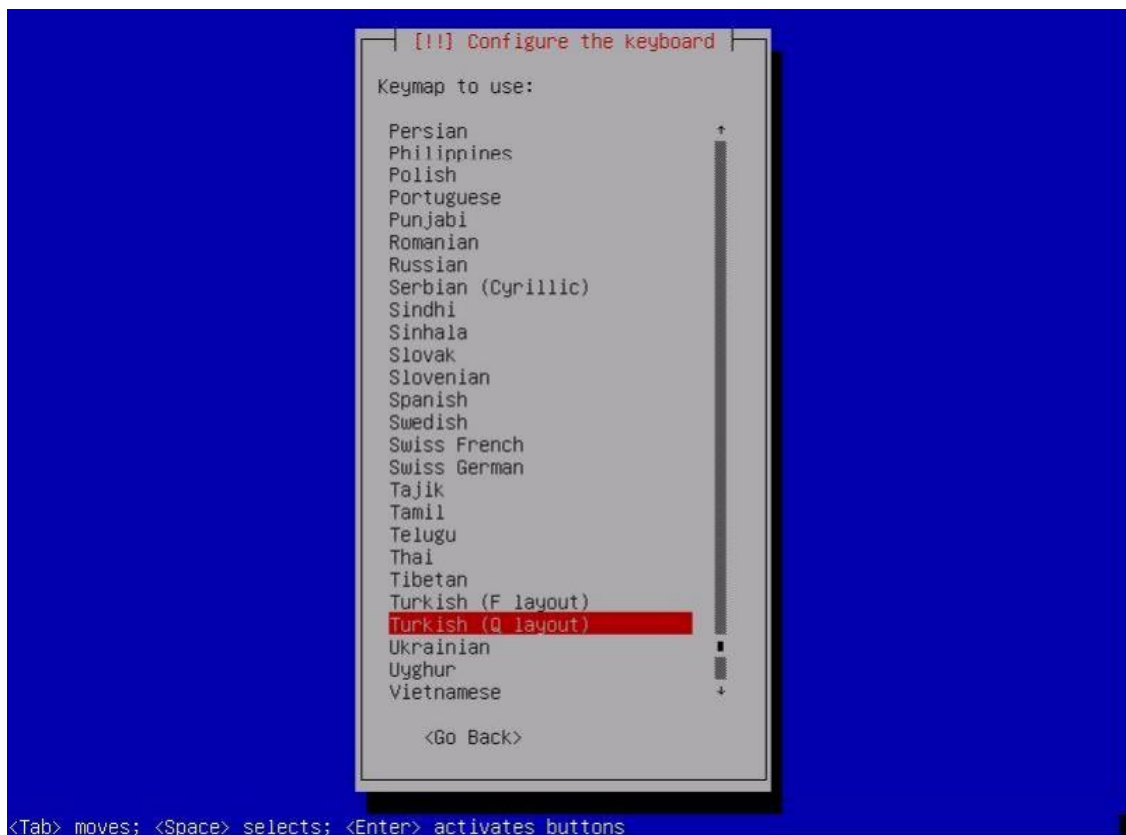
T-POT, ücretsiz olarak dağıtılmaktadır. Güncel derlenmiş kurulum dosyasını

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

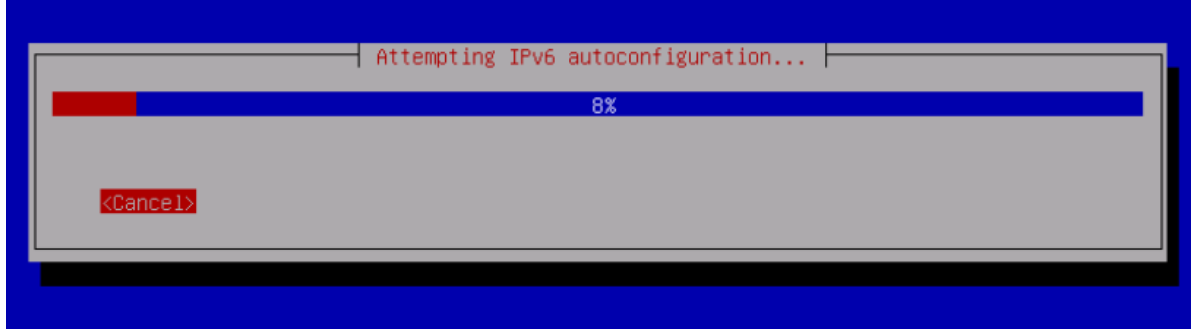
- İndirmiş olduğunuz iso yükleme dosyasını çalıştırınız. a



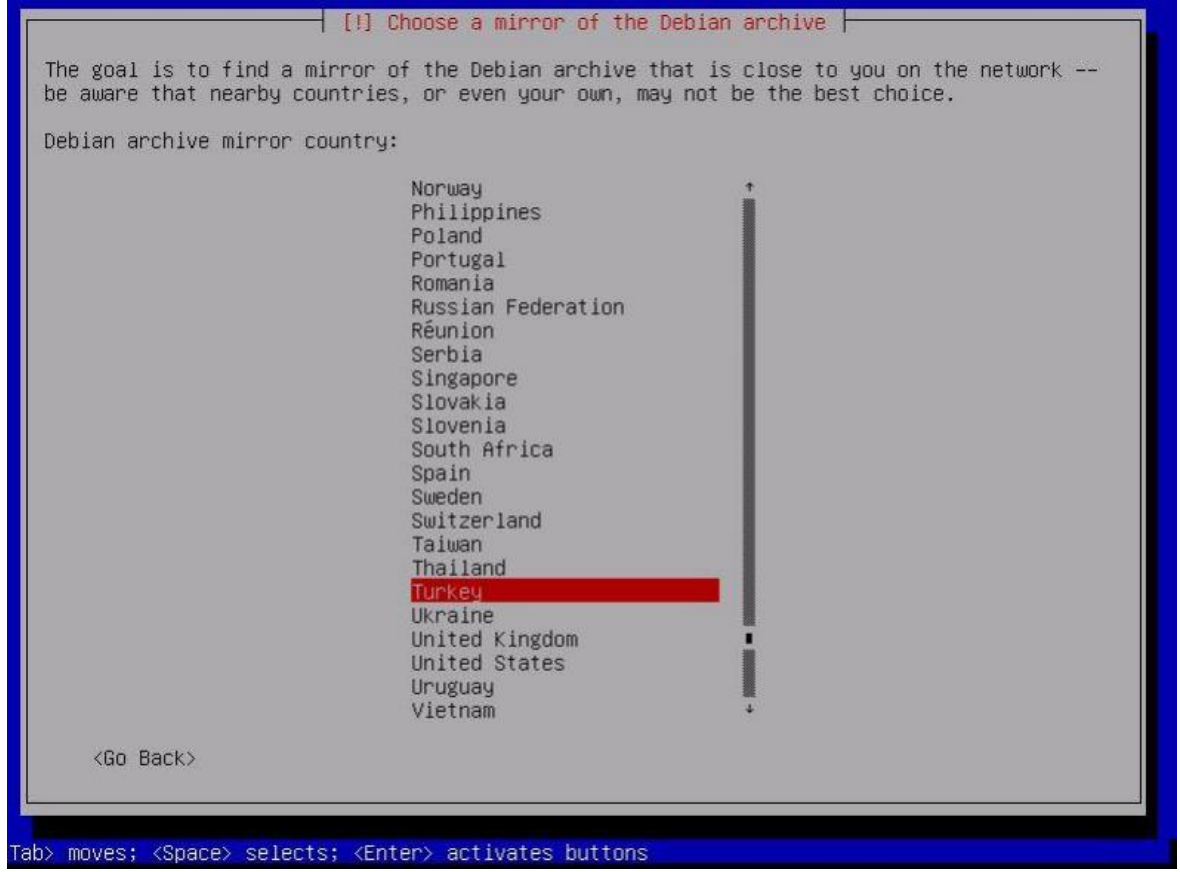
-Burada konum olarak United States' seçerek ilerleyiniz. (Konumunuza göre siz değiştirebilirsiniz.)



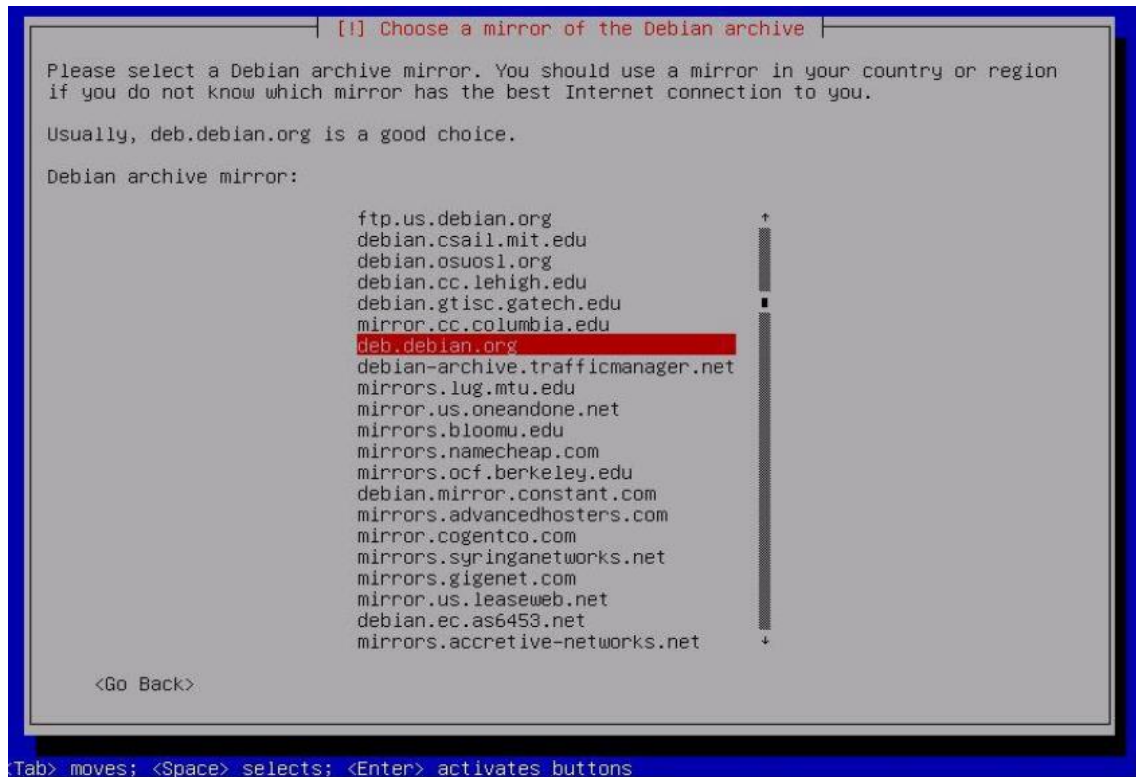
-Kullanacağınız klavye dilini seçiniz.



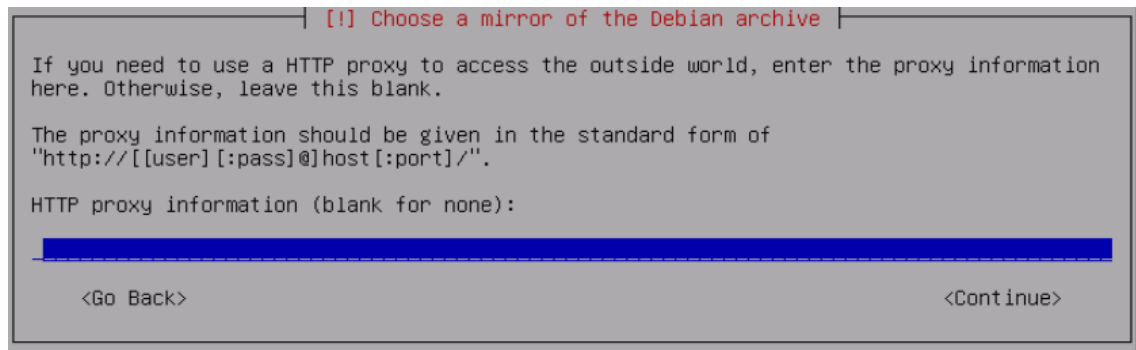
Şekildeki konfigürasyon ekranının tamamlanmasını bekleyiniz.



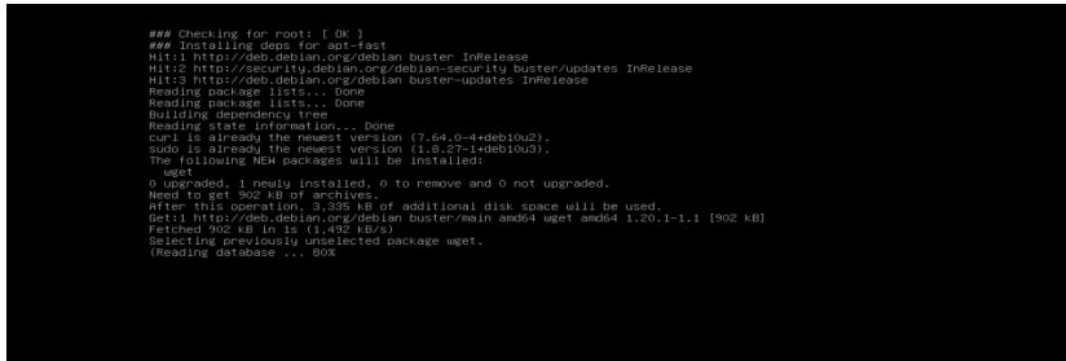
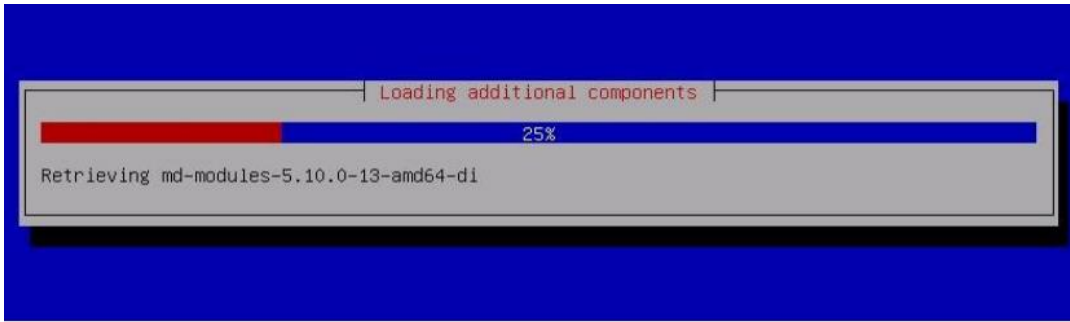
Bu ekranda ise Mirror için ülke seçimi yapıyoruz.



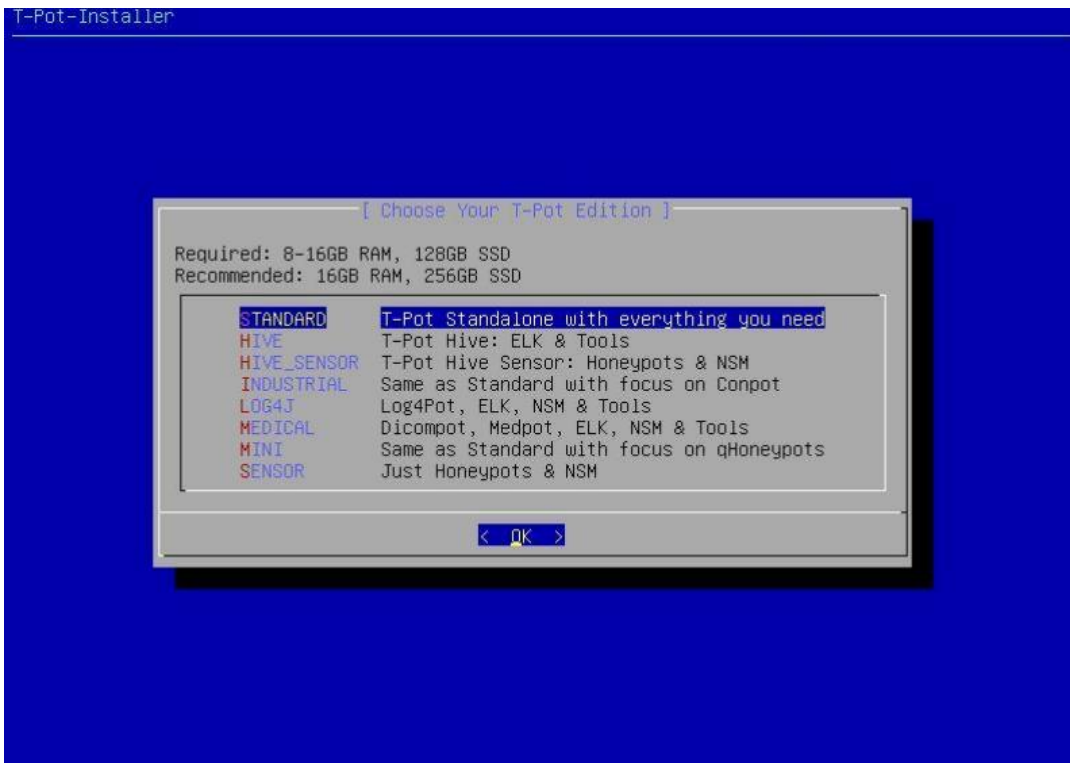
Debian archive aynalama yapılacak indirme sunucusunu seçiniz.



Gelen ekranda Continue deyip bir sonraki ekrana geçiniz.



Kurulum için gelen ekranın tamamlanmasını bekleyiniz.



Test ortamı için STANDARD seçimi yeterli olacaktır.

[Enter your web user name]

Username (tsec not allowed)

< OK > <Cancel>

[Enter password for your web user]

Password

< OK > <Cancel>

Sisteme giriş yapabilmek için güvenli kullanıcı adı ve şifre tanımlaması yapınız. (2 defa kul.adi ve şifre istenecektir.)

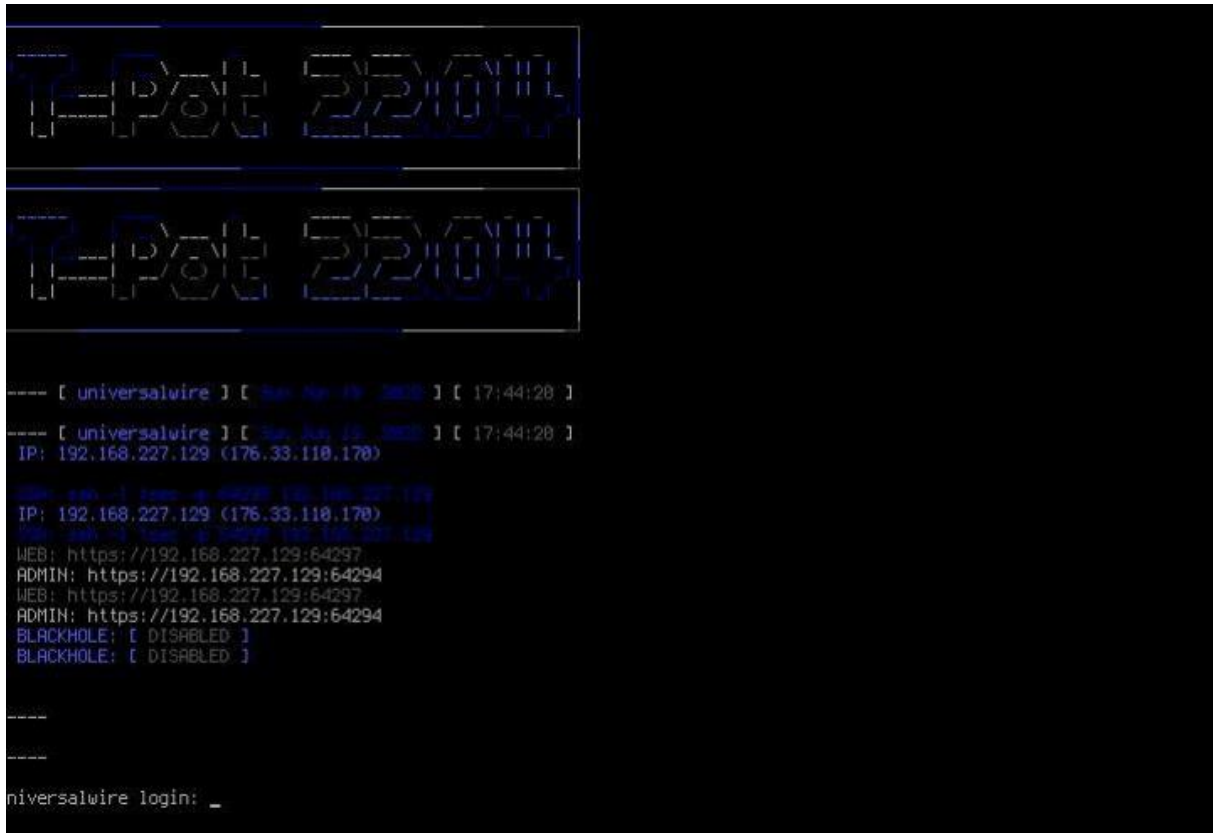
```
Installing...

### Getting update information.
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://security.debian.org/debian-security bullseye-security InRelease
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease
Reading package lists...

### Upgrading packages.
info: Trying to set 'docker.io/restart' [boolean] to 'true'
info: Loading answer for 'docker.io/restart'
info: Trying to set 'debconf/frontend' [select] to 'noninteractive'
info: Loading answer for 'debconf/frontend'
[apt-fast 20:09:38]
[apt-fast 20:09:38]Working... this may take a while.
W: --force-yes is deprecated, use one of the options starting with --allow instead.
Reading package lists...
Building dependency tree...
Reading state information...
Calculating upgrade...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
W: --force-yes is deprecated, use one of the options starting with --allow instead.

### Installing T-Pot dependencies.
[apt-fast 20:09:39]
[apt-fast 20:09:39]Working... this may take a while.
```

Kullanıcı adı ve şifreden sonra kurulum ekranını bekleyiniz.



SSH: Uzak bağlantı protokolü.

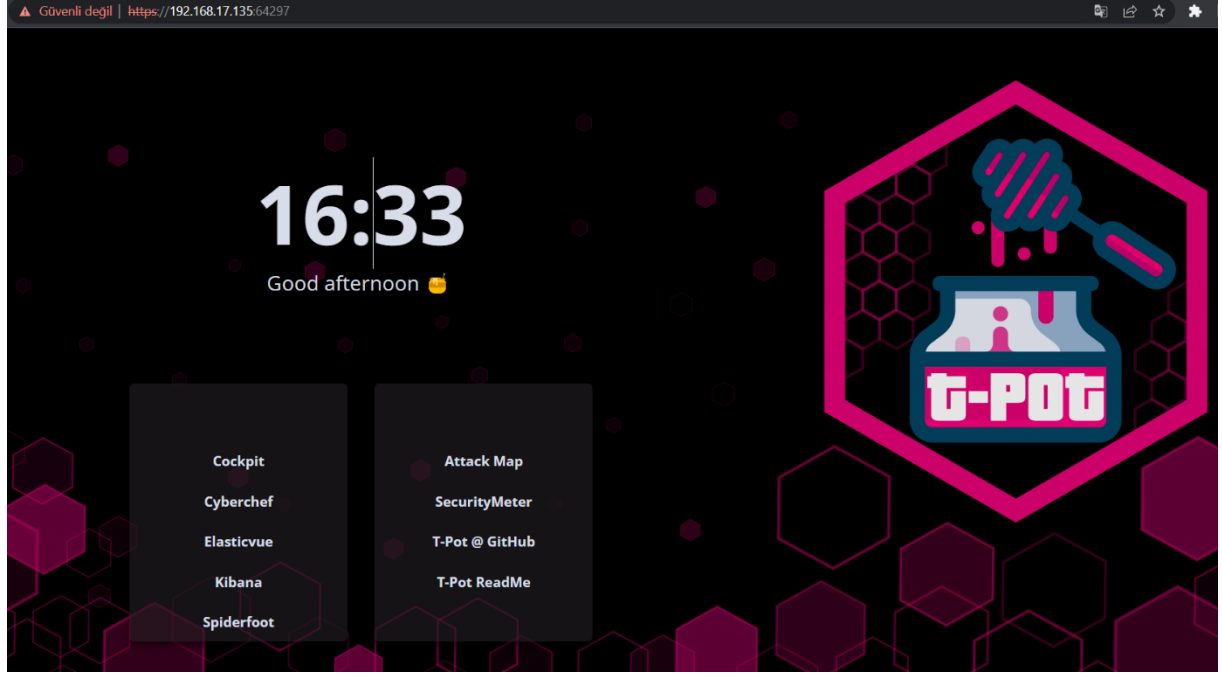
WEB: Bu kısımda ise Kibana, Cyberchef, Cockpit ve Elasticsearch Head gibi araçlara erişim sağlayabiliyoruz.

Admin: Bu kısımdan ise T-POT web ara yüzüne erişebiliyoruz.

Giriş için tanımladığınız kullanıcı adı ve Şifreyi giriniz.

4.Arayüz Testi

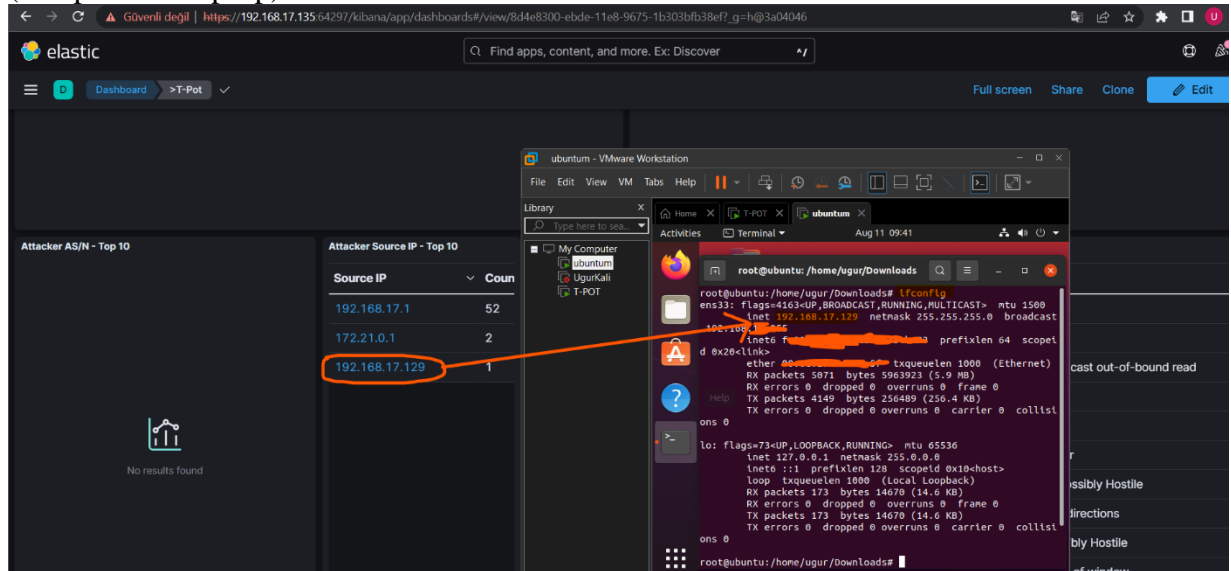
Bu aşamada T-pot servislerinin arayüzüne erişmeli ve hepsinin hizmet verdiğinden emin olmalıyız.

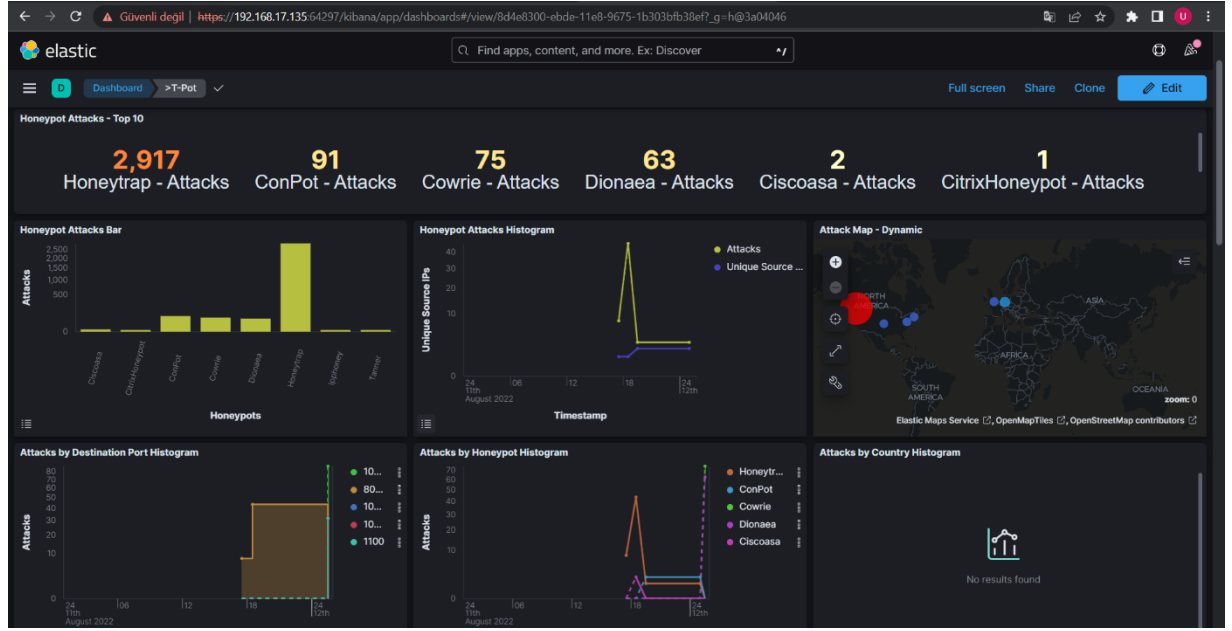


<https://ip:port>

Sistemimizin çalışabilirliğini test etmek için açık port taraması gerçekleştiriyoruz.

(nmap -sS -sV -p- ip)





Görüldüğü gibi saldırıları başarıyla algılayıp sınıflandırdı. Sistemimizin çalıştığından emin olduk. Bir sonraki aşama olan splunk ilişkilendirmesine geçebiliriz.

5.Splunk

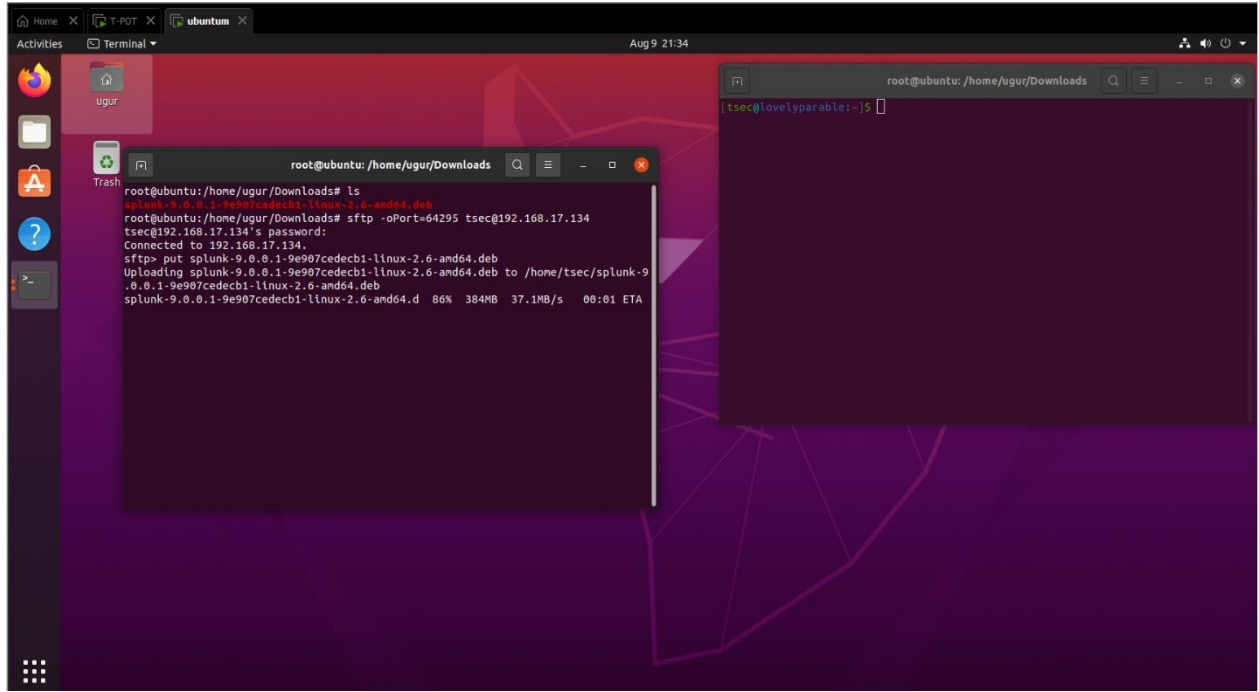
Splunk, siber güvenlik ve IT operasyonlarında çözüm sunan bir yazılım platformudur. Şirketin amacı, mevcut olan tüm sorular, kararlar ve eylemler için veriyi sürece dahil etmeyi içerir. Temelde güvenlik, IT operasyonları ve Devops çözümleri sunulur. Bu çözüm veri desenlerini tespit edip, metrik sağlayıp, sorunları teşhis ederek kurumların makine verilerinden faydalanmasına izin verir.

Makine verisi karmaşık, anlaşılması zor, yapılandırılmamış verilerden meydana gelir. İşletmelerin bu veriyi işlemekten kullanması mümkün değildir. Veriler yazılım çözümü tarafından işlenerek işletmelerin faydalanabileceği bir forma getirilir.

6.Splunk'ın T-Pot' a Entegrasyonu

6.1 Spesifik Bir Dosyadan Log Okunması

Bu aşamada Splunk birden farklı çözümlerle T-Pot' a entegre edilebilir. Bizim tercih ettiğimiz ilk yöntem için öncelikle; Splunk'ın kurulum dosyasını Ubuntu işletim sistemli makinemize indiriyoruz.



Bir dosyayı farklı bir makineye uzaktan göndermenin birden fazla yöntemi var (sftp,scp vb.). biz sftp komutuyla önce bağlantı oluşturup daha sonra put komutu ile kurulum dosyasını göndericeğiz.

```
&> sftp -oPort=64295 tsec@ip
```

>password: #bu kısma T-Pot kullanıcı şifrenizi girin.

Sftp> put Dosyaİsmi #put komutu ile seçtiğimiz dosyayı sftp aracılığı ile gönderiyoruz.

```
root@ubuntu: /home/ugur/Downloads

[tsec@lovelyarable:~]$ ls
splunk-9.0.0.1-9e907cedecb1-linux-2.6-amd64.deb
[tsec@lovelyarable:~]$ sudo dpkg -i splunk-9.0.0.1-9e907cedecb1-linux-2.6-amd64.deb
[sudo] password for tsec:
Selecting previously unselected package splunk.
(Reading database ... 56344 files and directories currently installed.)
Preparing to unpack splunk-9.0.0.1-9e907cedecb1-linux-2.6-amd64.deb ...
Unpacking splunk (9.0.0.1) ...

```

Splunk'ın kurulum dosyası artık T-Pot'un kurulu olduğu makineye gönderildi.

Splunk'ın kurulumu için aşağıdaki komutları sırasıyla uyguluyoruz.

>dpkg -i DosyaIsmi

```
[root@lovelyarable:/opt/splunk/bin]# ls
2to3-3.7          genSignedServerCert.sh  mongorestore-3.6      pydoc3.7          signtool
bloom            genWebCert.py          noah_self_storage_archiver.py  python            slim
bottle.py        genWebCert.sh          node                  python3           splunk
bttool          idle3                  openssl              python3.7         splunkd
btprobe         idle3.7               parse_xml_buckets.py  python3.7m        splunkmon
bzip2           importtool            pcregextest          pyvenv            splunk-optimize
classify        installit.py          pid_check.sh         pyvenv-3.7        splunk-optimize-lex
ColdStorageArchiver_GCP.py  jars                 pip3                 rapidDiag          tarit.py
ColdStorageArchiver.py     jp.py               pip3.7              recover-metadata   tocsv.py
coldToFrozenExample.py     jsmin              prichunkpng         rest_handler.py   tsidxprobe
copyright.txt            locktest            priforgepng         runScript.py      tsidxprobe_plo
dbmanipulator.py         locktool            prigreypng          S3benchmark       tsidx_scan.py
easy_install-3.7         mongod               pripalpng           safe_restart_cluster_master.py  untar.py
exporttool           mongod-3.6          pripamtopng         scripts            walklex
fill_summary_index.py    mongod-4.0          pripnglsh           scrubber.py        wheel
genAuditKeys.py         mongodump            pripngtopam         searchtest
genRootCA.sh           mongodump-3.6        priweavepng          setSplunkEnv
genSignedServerCert.py  mongorestore         pydoc3              shc_upgrade_template.py
[root@lovelyarable:/opt/splunk/bin]# ./splunk start
SPLUNK GENERAL TERMS
Last Updated: August 12, 2021
```

> sudo /opt/splunk/bin/splunk start #belirlilen dizindeki belirtilen servisi başlatıyoruz

1. lisans bilgileri: q (quit) ile çıkıyoruz.

2. lisans haklarını kabul ediyor musunuz? sorusu : y (yes)

```
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-9.0.0.1-9e907cedecb1-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=CN=lovelyparable/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embed
ded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://lovelyparable:8000

[root@lovelyparable:/opt/splunk/bin]#
```

>sudo ./splunk enable boot-start # restart sonrası otomatik olarak başlaması için.

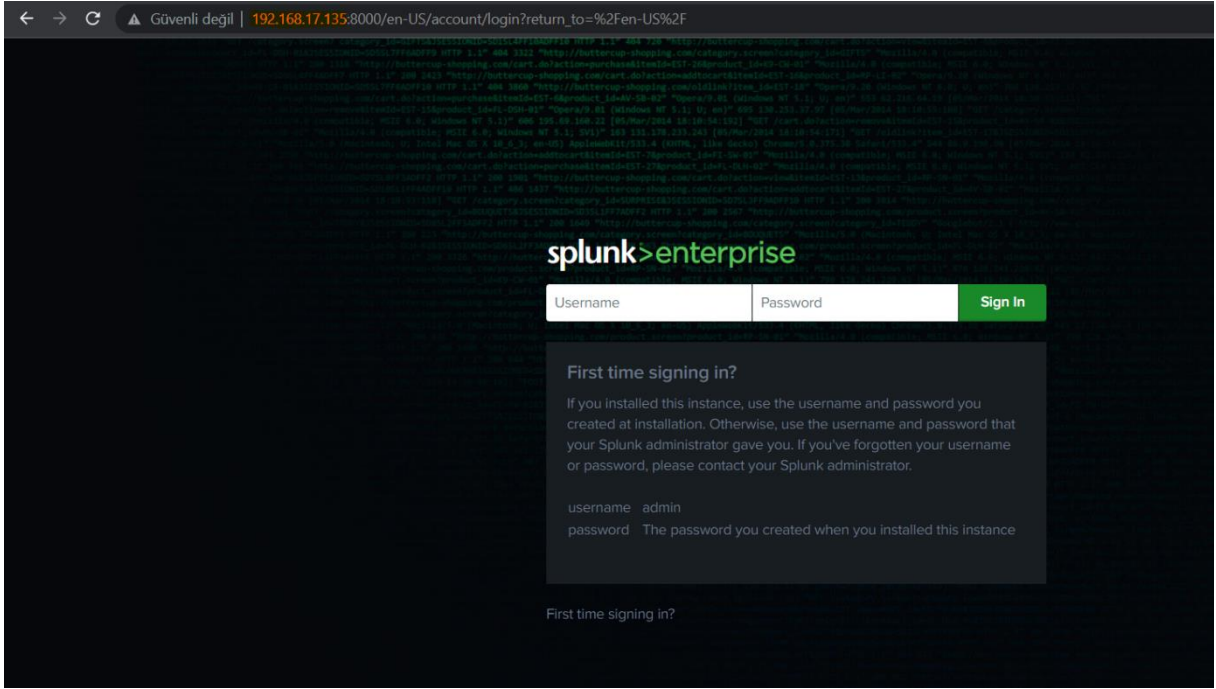
>systemctl enable splunk # splunk'ı etkinleştiriyoruz

>systemctl start splunk # splunk'ı anlık başlatıyoruz.

```
[root@lovelyparable:/opt/splunk/bin]# ./splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
[root@lovelyparable:/opt/splunk/bin]# systemctl enable splunk
splunk.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable splunk
[root@lovelyparable:/opt/splunk/bin]# systemctl start splunk
```

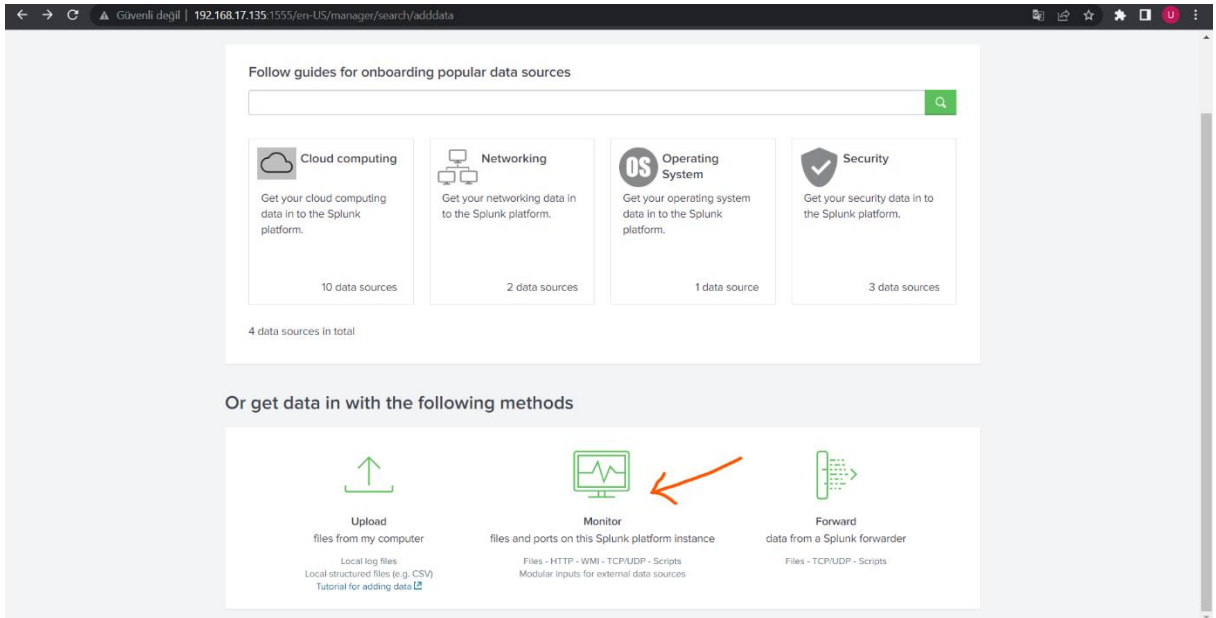
Artık Splunk kuruldu ve erişilebilir duruma geldi.

Web üzerinden link kısmına : Ip:Port yazarak arayüz sayfasına erişebiliriz.

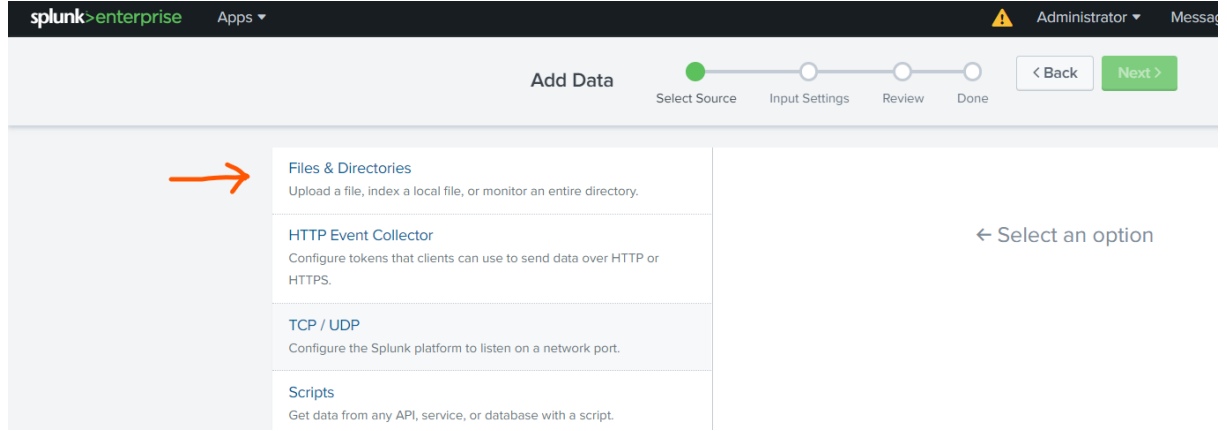


Kurulum aşamasında belirlediğimiz kullanıcı adı ve parola ile giriş yapıyoruz.

Artık dosya dizini üzerinden log okutma aşamasına geçebiliriz.

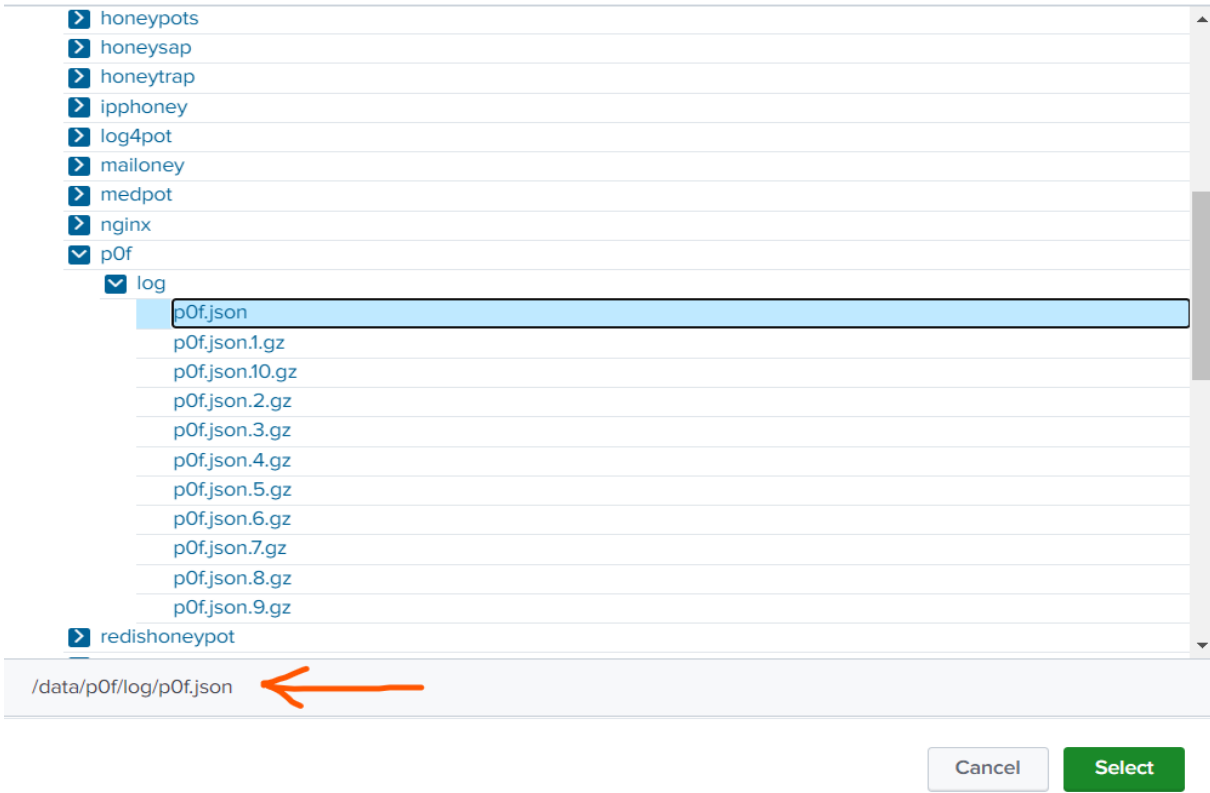


Giriş yaptıktan sonra karşımıza çıkan ana ekrandan “Monitor” seçeneğine tıklıyoruz.



Bir sonraki adımda “Files & Directories” seçeneğini işaretliyoruz.

Select source



NMap taramalarını görüntülemek için görseldeki dizin seçilmiştir. Amacınıza yönelik log dosyalarını bulabilir ve dizini gösterebilirsiniz.

Add Data

< Back

Submit >

Review

Input Type File Monitor

Source Path /data/p0f/log/p0f.json

Continuously Monitor Yes

Source Type _json

App Context search

Host lovelyparable

Index default

Submit seçeneği ile data ekleme aşamasını bitiriyoruz.

New Search

Save As Create Table View Close

NMap

All time

220,932 events (before 8/12/22 10:47:39.000 AM) No Event Sampling

Job

Smart Mode

Events (220,932) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

< Hide Fields

All Fields

SELECTED FIELDS

a host 2

a source 13

a sourcetype 10

INTERESTING FIELDS

a app 1

a client_ip 1

client_port 100+

date_hour 7

date_mday 2

date_minute 34

a date_month 1

date_second 60

a date_wday 2

date_year 1

a date_zone 2

a dist 23

a index 1

linecount 25

List

Format

20 Per Page

i	Time	Event
>	8/12/22 10:47:27.000 AM	<div>app: NMap SYN scan</div> <div>client_ip: 192.168.17.129</div> <div>client_port: 48283</div> <div>dist: <= 19</div> <div>mod: syn</div> <div>params: random_ttl</div> <div>raw_sig: 4:45*19:0:1460:1024,0:mss::0</div> <div>server_ip: 192.168.17.135</div> <div>server_port: 32783</div> <div>subject: cll</div> <div>timestamp: 2022/08/12 10:47:27</div>

| > | 8/12/22 10:47:27.000 AM | app: NMap SYN scan client_ip: 192.168.17.129 client_port: 48283 dist: <= 19 |

host = lovelyparable | source = /data/p0f/log/p0f.json | source

ubuntu - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

ubuntu

UgurKali

T-POT

Activities

Terminal

Aug 12 03:47

root@ubuntu: /home/ugur/Desktop

443/tcp open https

445/tcp open microsoft-ds

465/tcp open smtp

631/tcp open lpp

993/tcp open lmtp

995/tcp open pop3s

1025/tcp open nfs-or-iis

1080/tcp open socks

1433/tcp open ms-sql-s

1723/tcp open pptp

1900/tcp closed upnp

3306/tcp open mysql

5000/tcp closed upnp

5060/tcp closed sip

5432/tcp open postgresql

5555/tcp open freetv

5900/tcp open vnc

8443/tcp open https-alt

9200/tcp open nap-map

10001/tcp open scp-config

NAC Address: 00:0C:29:F1:47:06 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.61 seconds

root@ubuntu: /home/ugur/Desktop

Test etmek için bir nmap taraması gerçekleştiriyoruz ve logların Splunk'a aktarıldığını görüyoruz.

Bu yöntem sonucunda başarıya ulaştık.

6.2 Syslog İle Uzaktan Log Gönderilmesi

Temelinde conf dosyalarında yapılan ayarlamalar ile TCP/UDP vb. protokoller ile hedef gösterilen ip adresine, belirlenmiş olan portlardan log gönderilmesidir.

İlk olarak, rsyslog.d dosyası içerisinde gidip oraya tpot.conf adında bir dosya açıyoruz.

Varsayılan ayarlarda rsyslog dizini : /etc/rsyslog.d

/etc>\$: cd rsyslog.d # rsyslog dosyası içine giriyoruz.

>sudo touch tpot.conf # touch komutu ile tpot.conf dosyamızı oluşturuyoruz.

>sudo nano tpot.conf # yazma gerçekleştireceğimiz için nano komutuyla conf dosyamızı açıyoruz.

Açılan conf dosyasına aşağıdaki ayarları yazıyoruz.

```
GNU nano 5.4 tpot.conf *
$ModLoad imfile
$InputFilePollInterval 10
$PrivDropToGroup adm
$InputFileName /data/p0f/log/p0f.json
$InputFileTag tpot-access
$InputFileStateFile stat-tpot-access
$InputFileSeverity alert
$InputFileFacility local7
$InputRunFileMonitor
$InputFilePersistStateInterval 1000

$template tpot_log, " %msg% "

if $programname == 'tpot-access' then @@192.168.119.130:514;tpot_log
if $programname == 'tpot-access' then stop
```

#InputFileName'in karşısına veri aktarımı yapılacak dosyanın dizini yazılır.

#InputFileSeverity'nin karşısına info,alert vb sınıflandırmalar yapılabilir.

ip yi yazmadan öncesine @@ veya @ eklememiz TCP veya UDP protokolünü belirtmek içindir.

CTRL+S & CTRL+X ile kaydedip çıkış yapıyoruz.

>sudo systemctl restart rsyslog # rsyslog'u yeniden başlatıyoruz.

Daha önceki yöntemde yaptığımız gibi Splunk arayüzüne erişerek (ip:port) add data ikonuna tıklıyoruz.

Bir sonraki ekranda "Monitor" seçeneğine tıklıyoruz.

"Select an option" aşamasında 'TCP/UDP' seçeneğini seçerek işaretliyoruz.

Sağ tarafta istenen değerler ;

port :514

Source name override: default

Only accept connection from: default

The screenshot shows the 'Add Data' configuration page in Splunk Enterprise. The page is divided into a left sidebar with a list of data sources and a main configuration area on the right. The 'TCP / UDP' option is selected in the sidebar, indicated by a blue arrow labeled '1.'. The main configuration area shows the 'TCP / UDP' configuration form. The 'Port' field is set to '514', indicated by a blue arrow labeled '2.'. The 'Source name override' field is set to 'optional host:port'. The 'Only accept connection from' field is set to 'optional'. A blue arrow labeled '3.' points to the 'Next >' button at the top right of the configuration area. The top navigation bar includes 'splunk>enterprise', 'Apps', and various user and system links.

Add Data Select Source Input Settings Review Done < Back Next >

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

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP 1. >
Configure the Splunk platform to listen on a network port. 2.

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

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

Systemd Journal Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Assist Self-Update
Detects and Downloads Assist Supervisor Updates

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). [Learn More](#)

TCP **UDP**

Port: 514
Example: 514

Source name override: optional
host:port

Only accept connection from: optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

FAQ

- > How should I configure the Splunk platform for syslog traffic?
- > What's the difference between receiving data over TCP versus UDP?
- > Can I collect syslog data from Windows systems?
- > What is a source type?

Add Data

< Back

Review >

Input Settings

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

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

1.

Select

New

syslog

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

Search & Reporting (search) ▼

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

2.

Method ?

IP

DNS

Custom

Index

The Splunk platform stores incoming data as events in the

Bu adımda görseldeki gibi Source Type seçeneğini syslog olarak seçiyoruz.

Add Data

< Back

Submit >

Review

Input Type	TCP Port
Port Number	514
Source name override	N/A
Restrict to Host	N/A
Source Type	syslog
App Context	search
Host	(IP address of the remote server)
Index	default

Son aşamada, ayarlarımızın görseldeki gibi olduğundan emin olarak “Submit” butonuna tıklıyoruz.

source="tcp:514" sourcetype="syslog"

✓ 126,881 events (8/11/22 12:00:00.000 PM to 8/12/22 12:01:52.000 PM) No Event Sampling ▼

Events (126,881) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

1 day 1 hour

List ▼ Format 20 Per Page ▼

< Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1	INTERESTING FIELDS a app 2 a client_ip 3 # client_port 100+ a dist 24 a index 1 # linecount 1 a mod 8 a params 4 a process 2 a punct 4 a raw_sig 28 a server_ip 11 # server_port 100+ a splunk_server 1 a subject 2 a timestamp 100+ 8 more fields + Extract New Fields	>	8/12/22 12:01:47.000 PM	{ [-] client_ip: 192.168.17.135 client_port: 52758 link: Ethernet or modem mod: mtu raw_mtu: 1500 server_ip: 52.85.5.100 server_port: 443 subject: srv timestamp: 2022/08/12 12:01:46 } Show as raw text host = 127.0.0.1 source = tcp:514 sourcetype = syslog
		>	8/12/22 12:01:47.000 PM	{ [-] client_ip: 192.168.17.135 client_port: 52758 dist: 0 mod: syn+ack os: ??? params: none raw_sig: 4:128+0:0:1460:mss*44,0:mss:0 server_ip: 52.85.5.100 server_port: 443 subject: srv timestamp: 2022/08/12 12:01:46 } Show as raw text host = 127.0.0.1 source = tcp:514 sourcetype = syslog
		>	8/12/22 12:01:47.000 PM	{ [-] client_ip: 192.168.17.135

Artık splunk belirttiğimiz hosttaki 514 portunu dinliyor ve kayıt tutuyor.

Search filtrelerini düzenledikten sonra logların başarılı bir şekilde iletilildiğini gözlemleyip entegrasyonu tamamlamış olduk.

7.Kaynakça

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

<https://www.splunk.com>

[Splunk Nedir? Avantajları Nelerdir? Splunk Çözümleri Nelerdir? | Redington](#)