T-Pot

Kurulum Rehberi

&

Splunk İlişkilendirmesi

Hazırlayanlar

Ertuğrul ÖZTOMSUK

Uğur KAYA

Zeynep Nur BAYRAM

Zümre ÖZTÜRK

İçindekiler

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, Heralding, 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. İçerisin 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 kuruluma 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.

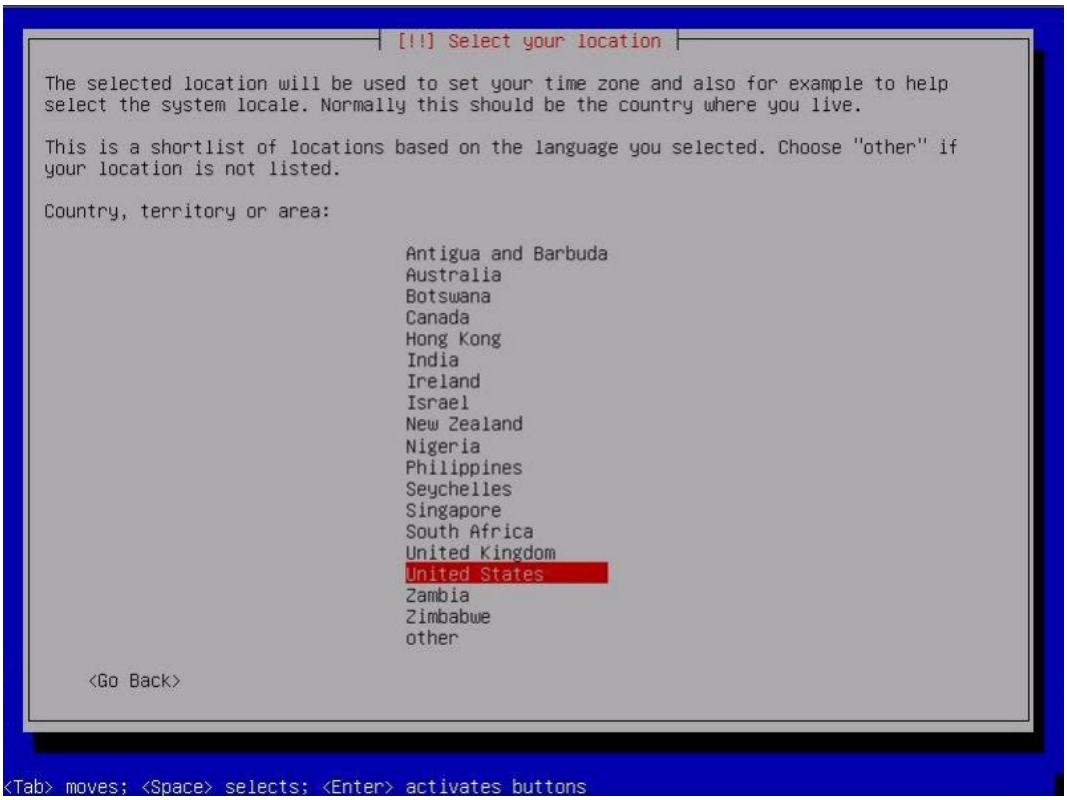
o Suricata bir Ağ Güvenliği İzleme motoru.

3.Kurulum

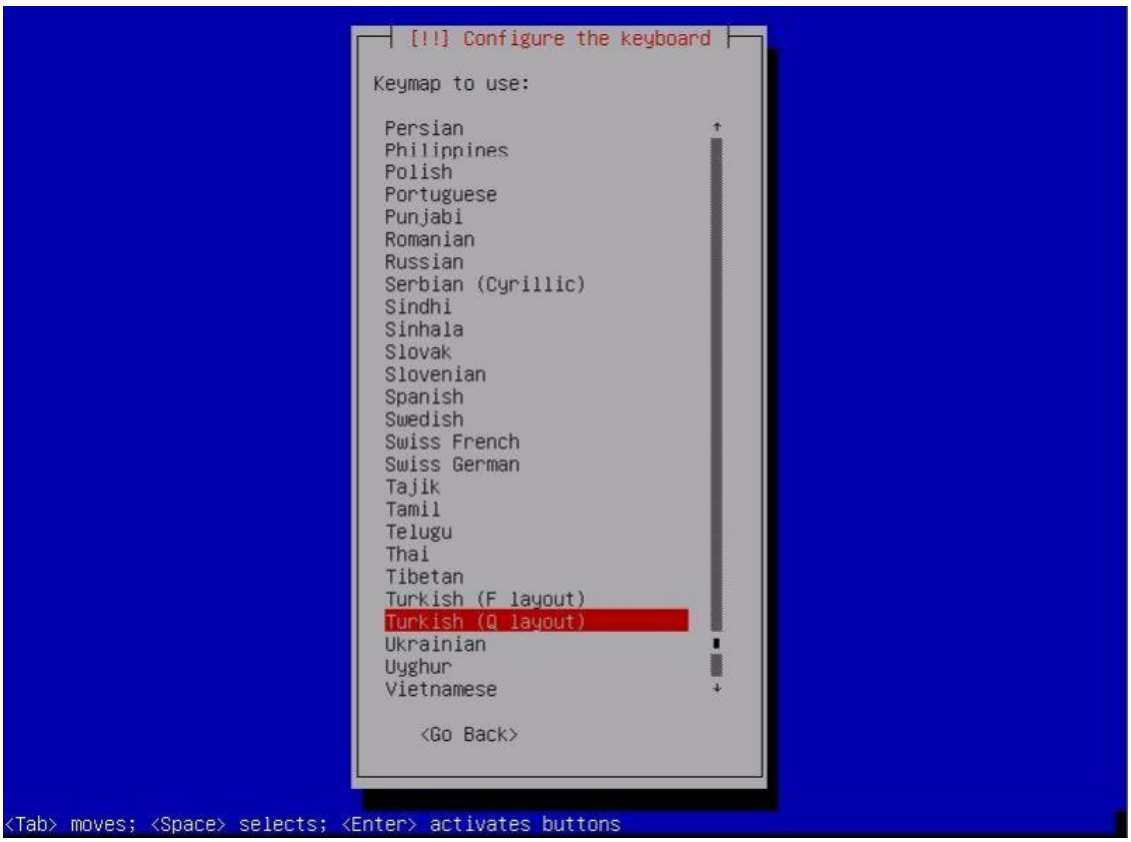
T-POT, ücretsiz olarak dağıtılmaktadır. Güncel derlenmiş kurulum dosyasını

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

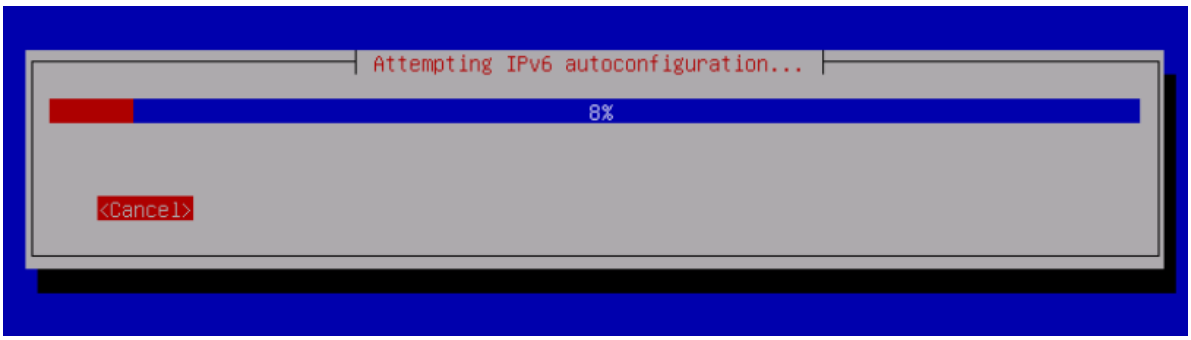
• İndirmiş olduğunuz iso yükleme dosyasını çalıştırınız. a



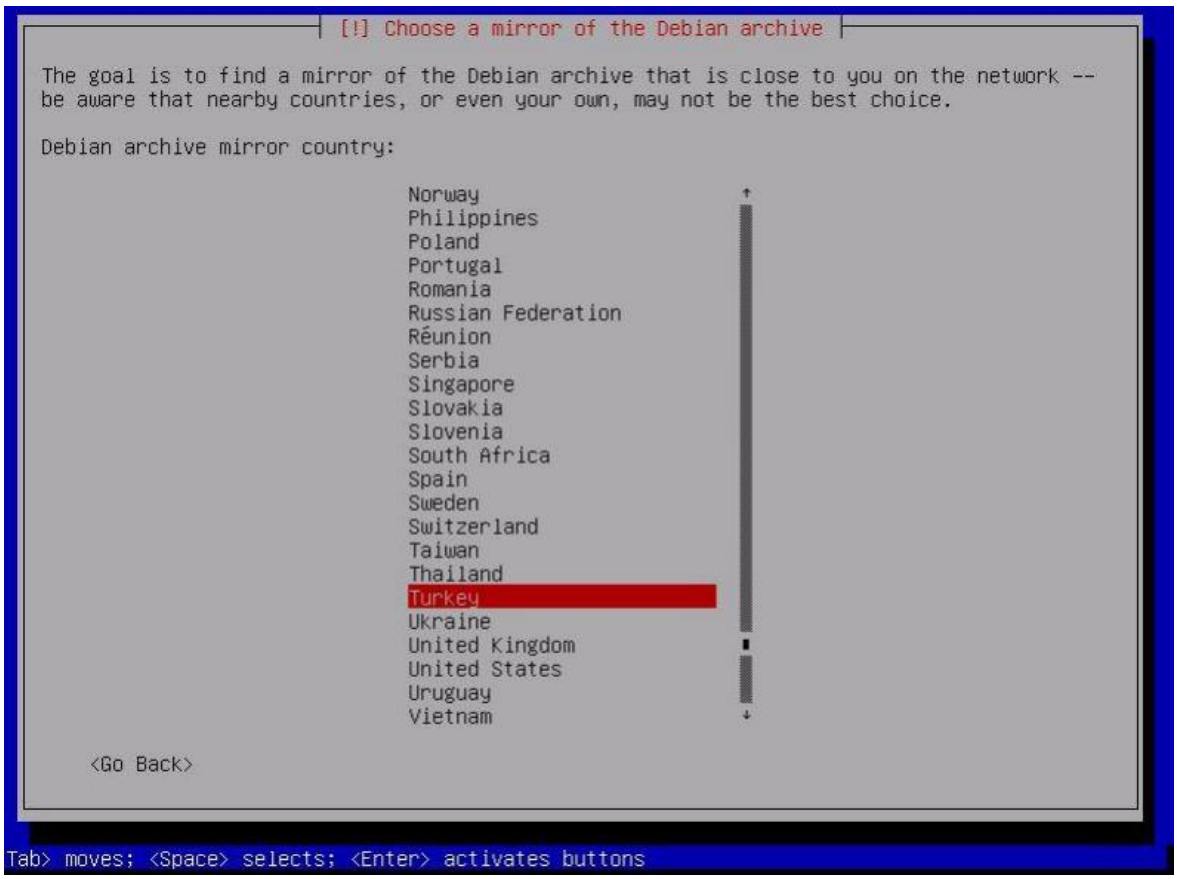
-Burada konum olarak United States' seçerek ilerleyiniz. (Konumunuza göre siz değiştirebilirsiniz.)



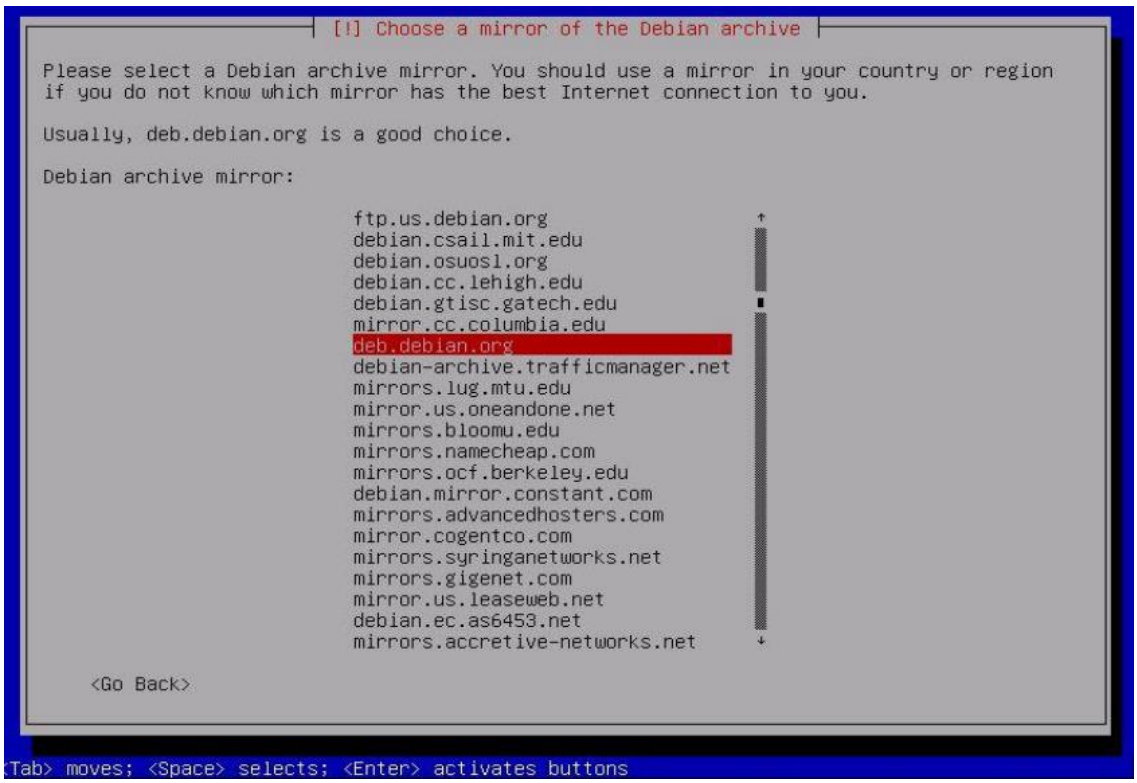
-Kullanacağınız klavye dilini seçiniz.



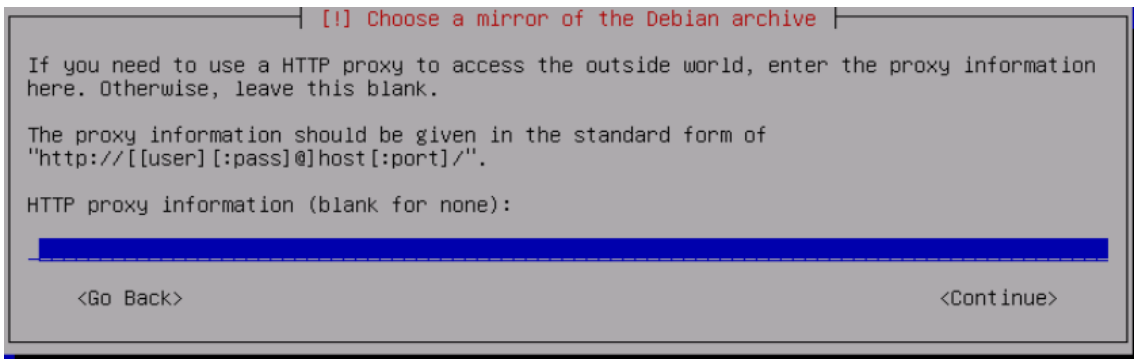
Şekildeki konfigürasyon ekranın tamamlanmasını bekleyiniz.



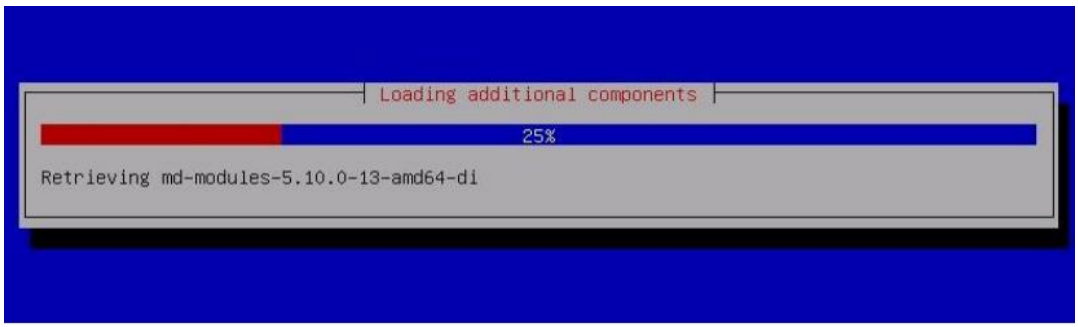
Bu ekranda ise Mirror için ülke seçimi yapıyoruz.

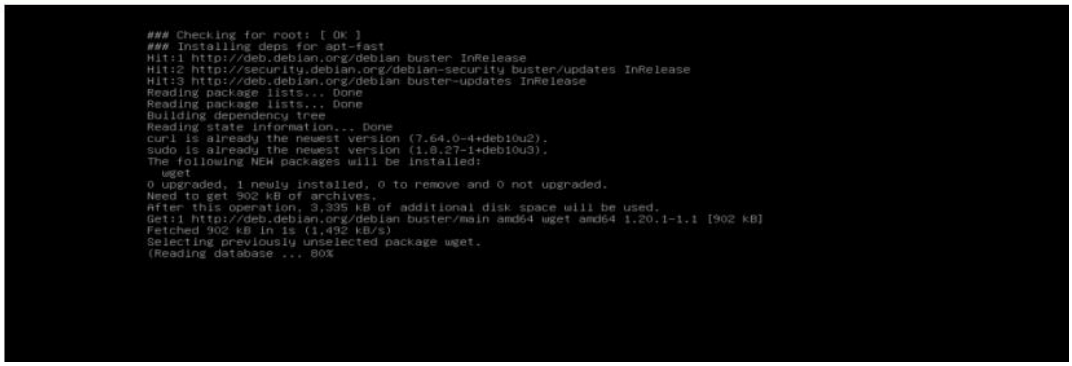


Debain archive aynalama yapılacak indirme sunucusunu seçiniz.

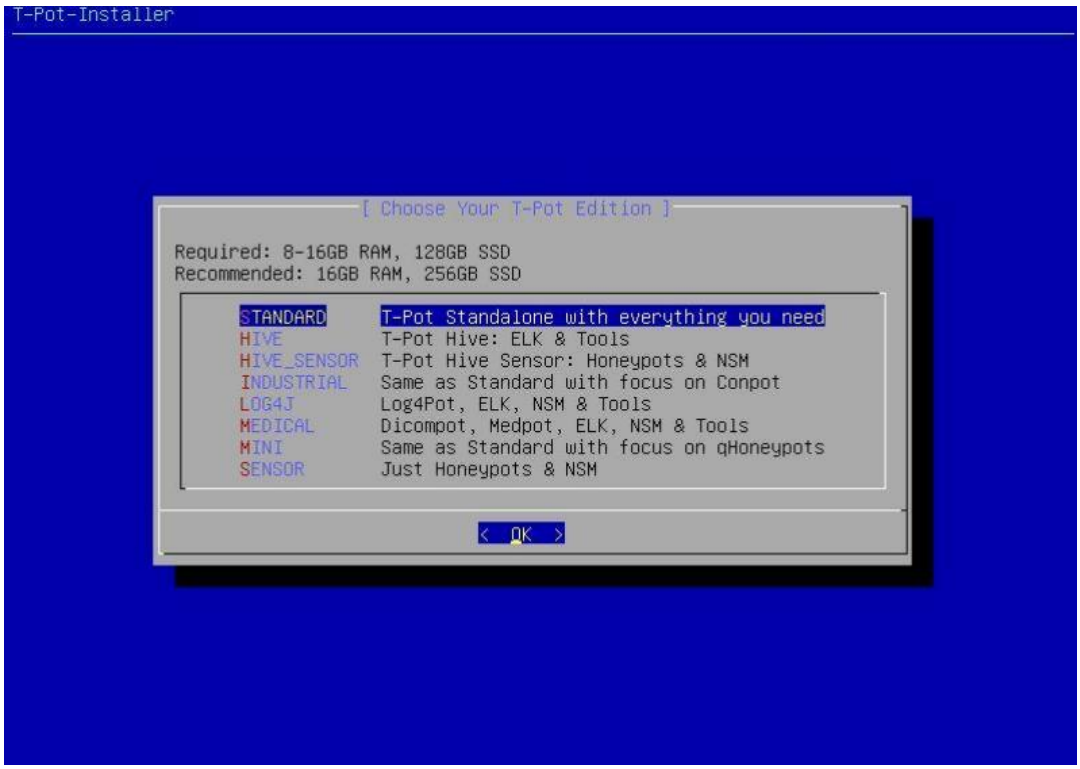


Gelen ekranda Continue deyip bir sonraki ekrana geçiniz.

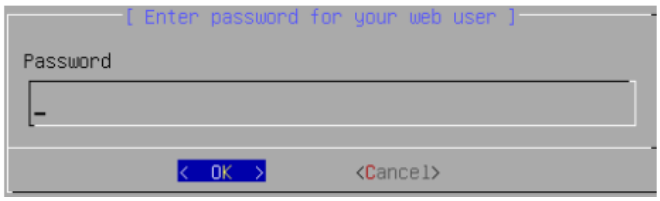




Kurulum için gelen ekranın tamamlanmasını bekleyiniz.

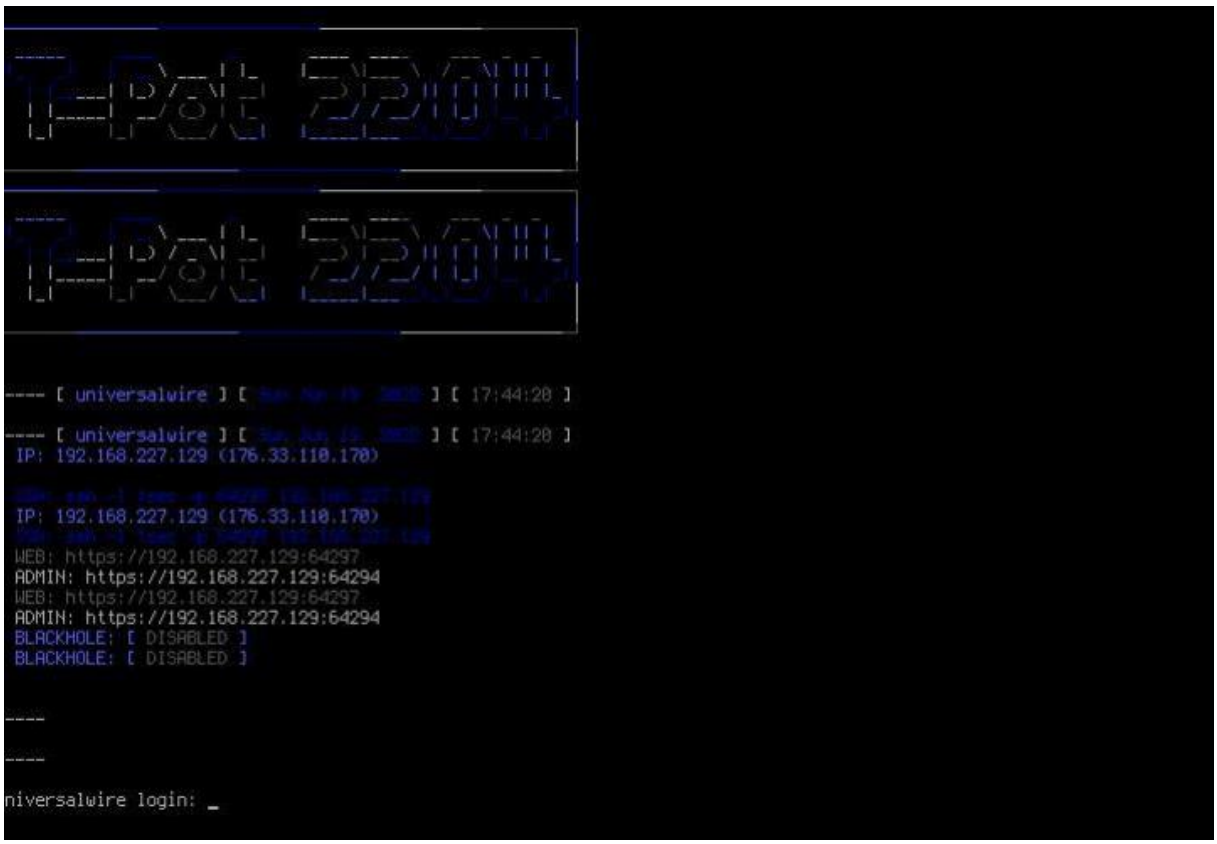


Test ortamı için STANDARD seçimi yeterli olacaktır.



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

Kullanıcı adı ve şifreden sonra kurulum ekranını bekleyiniz.



SSH: Uzak bağlantı protokolü.

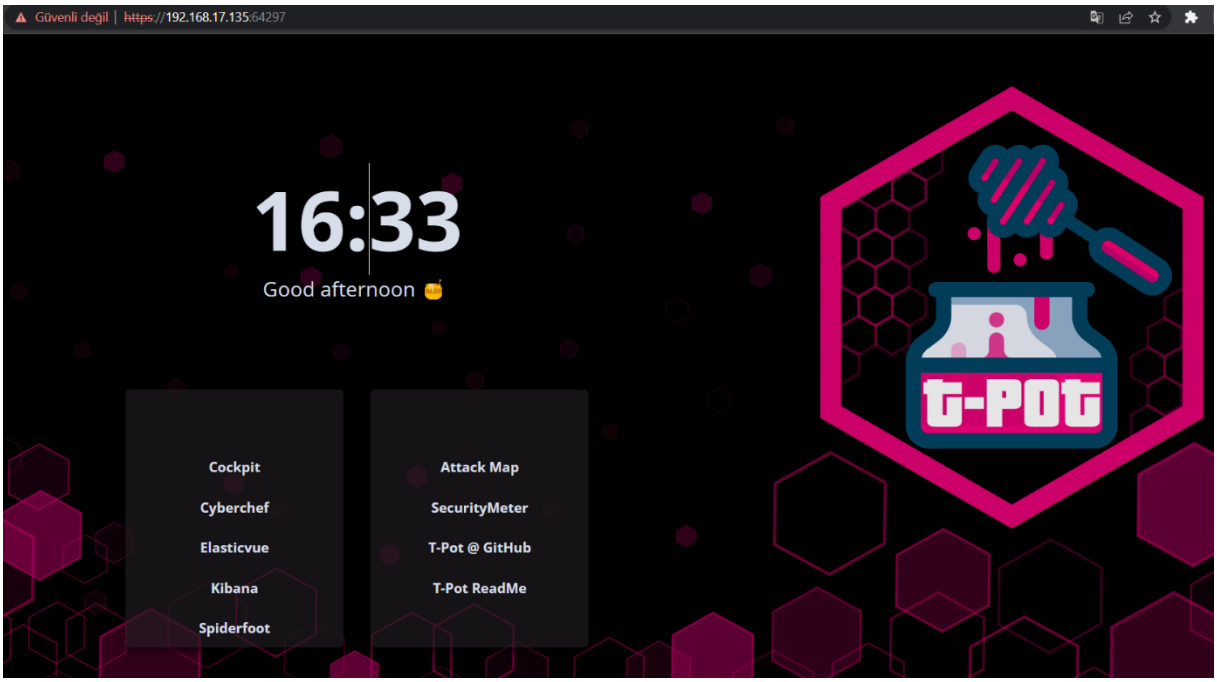
WEB: Bu kısımda ise Kibana, Cyberchef, Cockpit ve Elasticsearch Head gibi araçlara erişim sağlayabiliyoruz.

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

Giriş için tanımladığınız kullanıcı adı ve Şifreyi giriniz.

4.Arayüz Testi

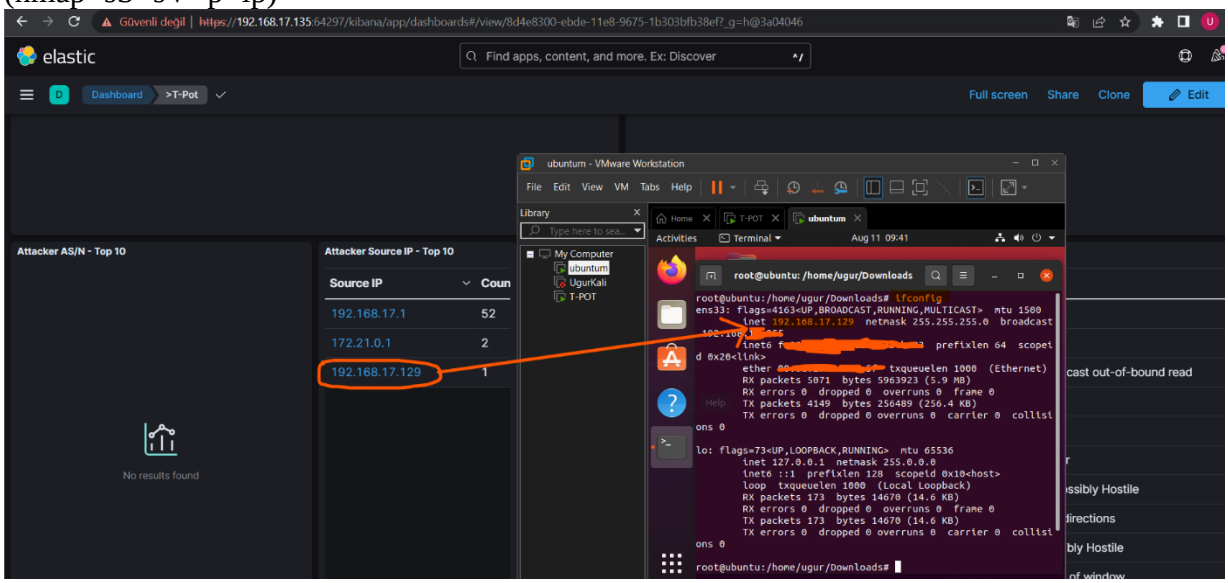
Bu aşamada T-pot servislerinin arayüzüne erişmeli ve hepsinin hizmet verdiğinden emin olmalıyız.

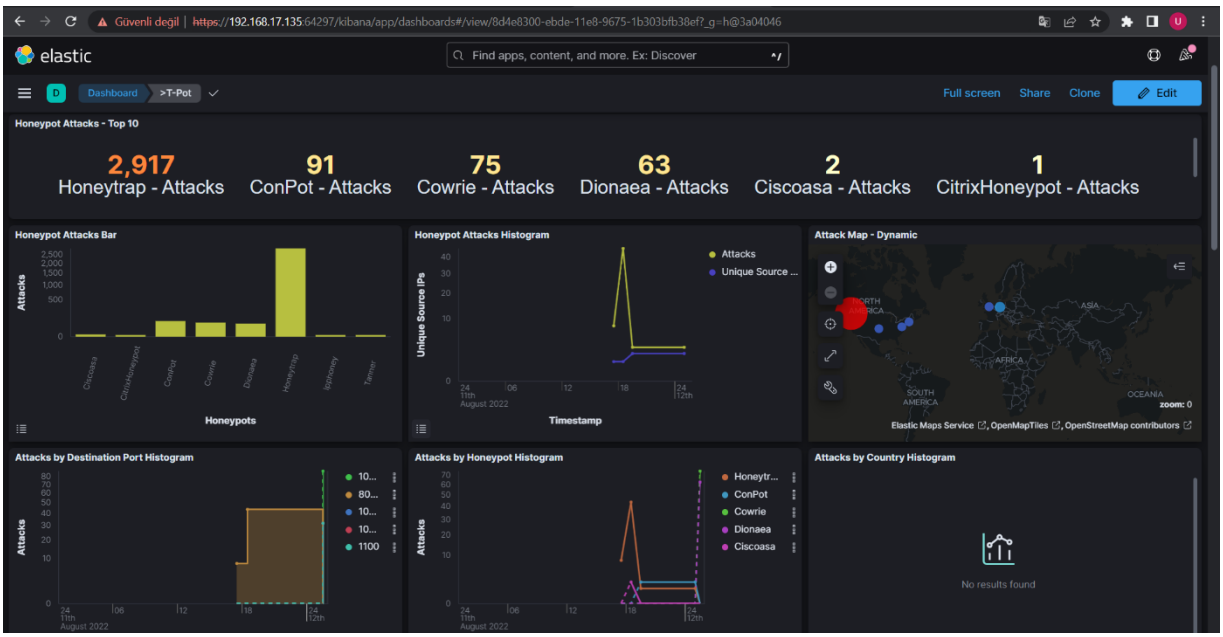


https://ip:port

Sistemimizin çalışabilirliğini test etmek için açık port taraması gerçekleştiriyoruz.

(nmap -sS -sV -p- ip)





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

5.Splunk

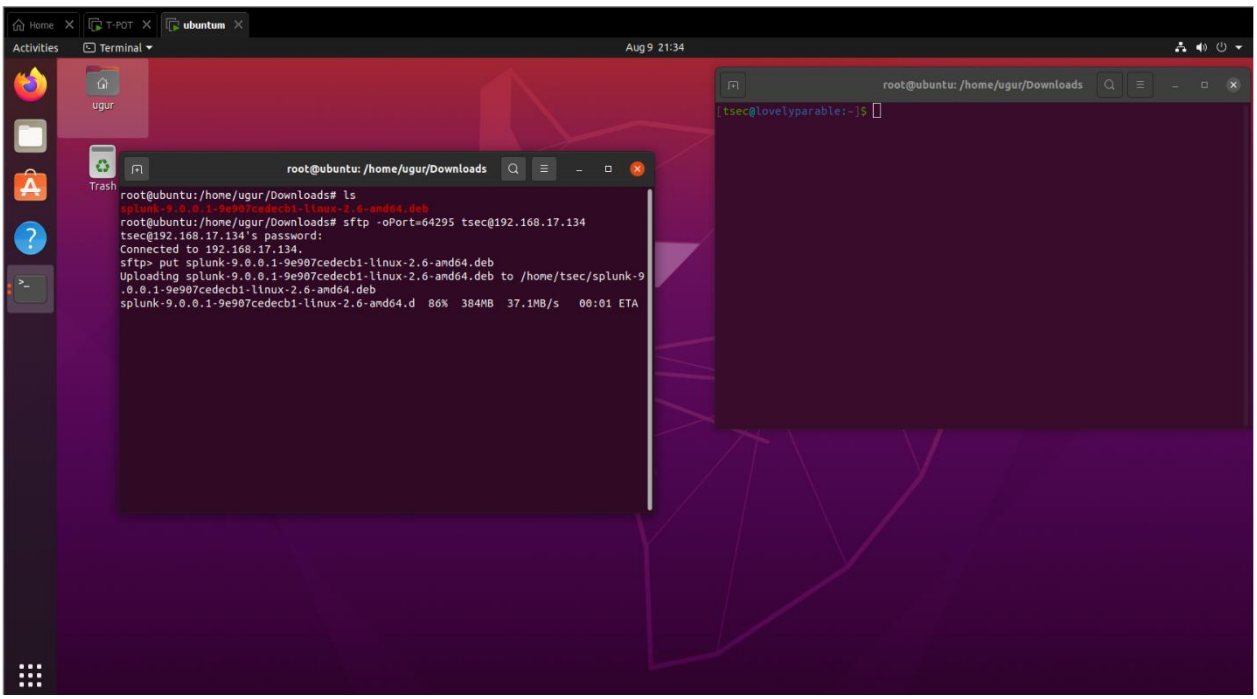
Splunk, siber güvenlik ve IT operasyonlarında çözüm sunan bir yazılım platformudur. Şirketin amacı, mevcut olan tüm sorular, kararlar ve eylemler için veriyi sürece dahil etmeyi içerir. Temelde güvenlik, IT operasyonları ve Devops çözümleri sunulur. Bu çözüm veri desenlerini tespit edip, metrik sağlayıp,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

Makine verisi karmaşık, anlaşılması zor, yapılandırılmamış verilerden meydana gelir. İşletmelerin bu veriyi işlemden 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 Okunnması

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.

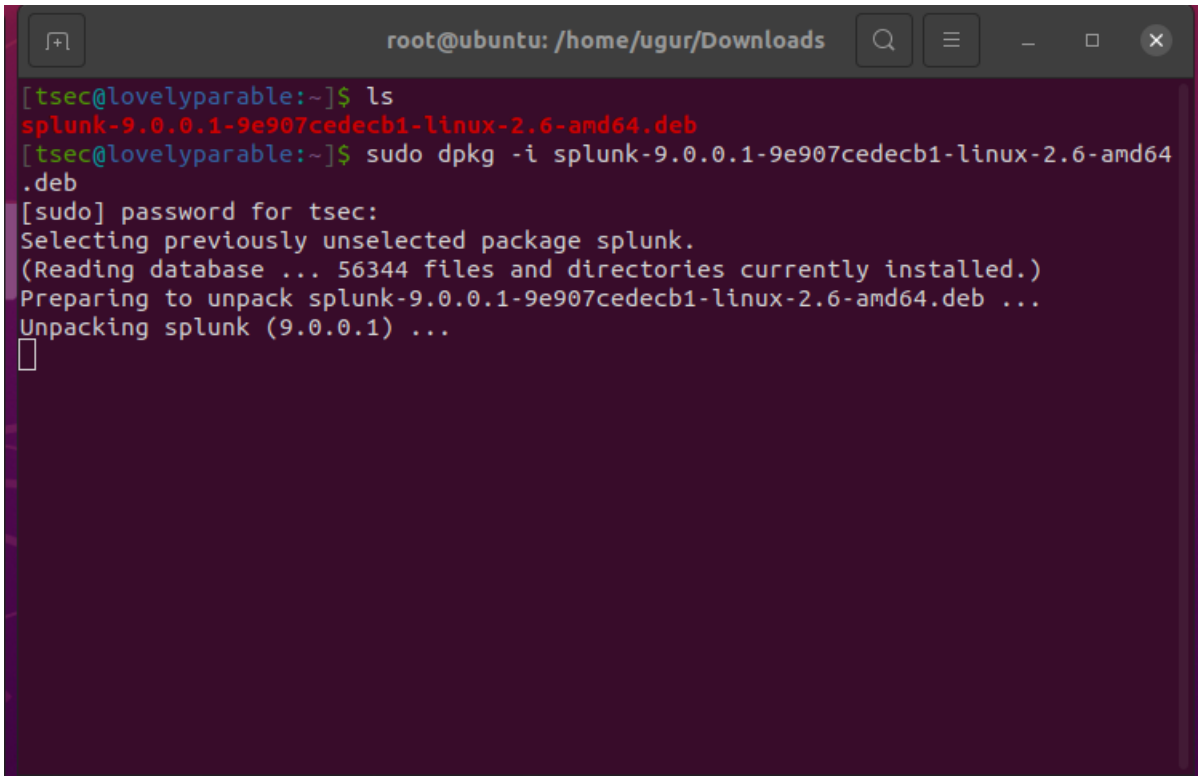


Bir dosyayı farklı bir makineye uzaktan göndermenin birden fazla yöntemi var (sftt,scp vb.). biz sftp komutuyla önce bağlantı oluşturup daha sonra put komutu ile kurulum dosyasını göndericeğiz.

&> sftp -oPort=64295 tsec@ip

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

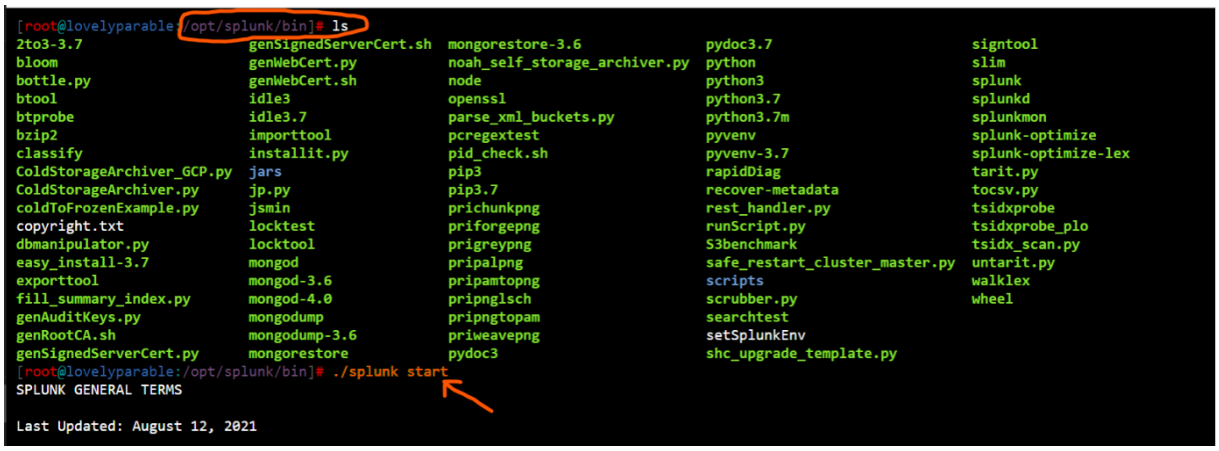
Sftp> put DosyaIsmi #put komutu ile seçtiğimiz dosyayı sftp aracılığı ile gönderiyoruz.



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

Splunk'ın kurulumu için aşağıdaki komutları sırasıyla uyguluyoruz.

>dpkg -i DosyaIsmi



> 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.

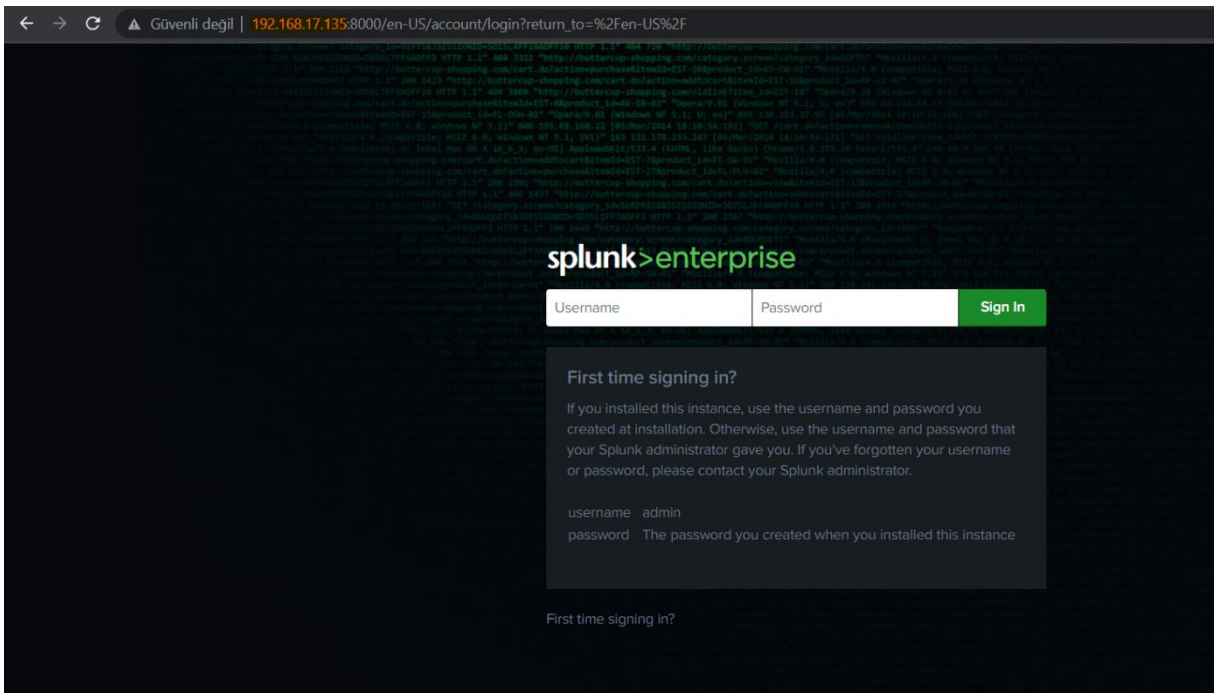
>systemctl enable splunk # splunk'ı etkinleştiriyoruz

>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
```

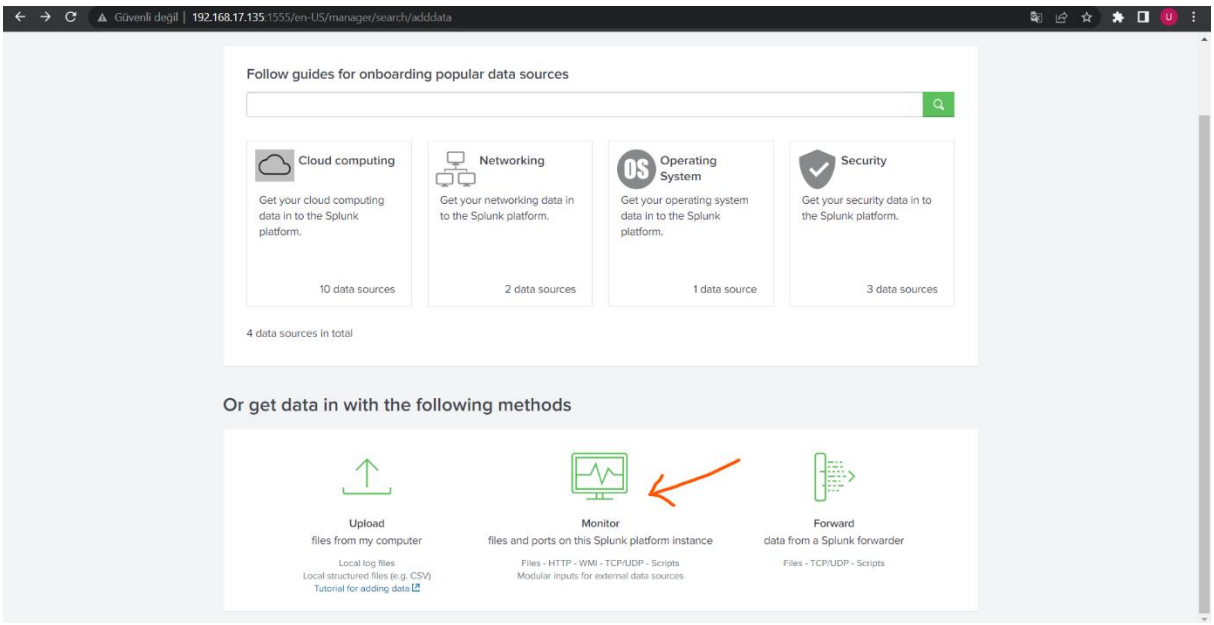
Artık Splunk kuruldu ve erişilebilir duruma geldi.

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

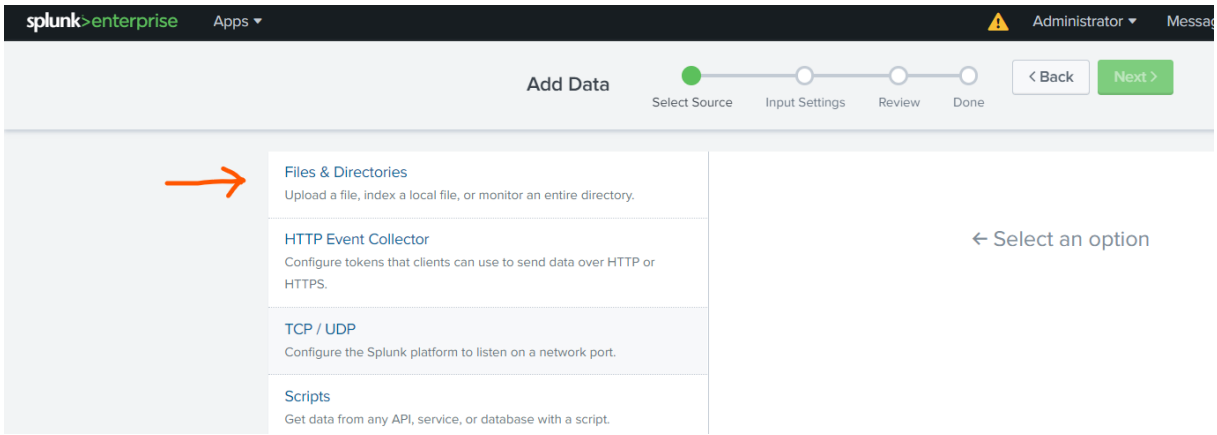


Kurulum aşamasında belirlediğimiz kullanıcı adı ve parola ile giriş yapıyoruz.

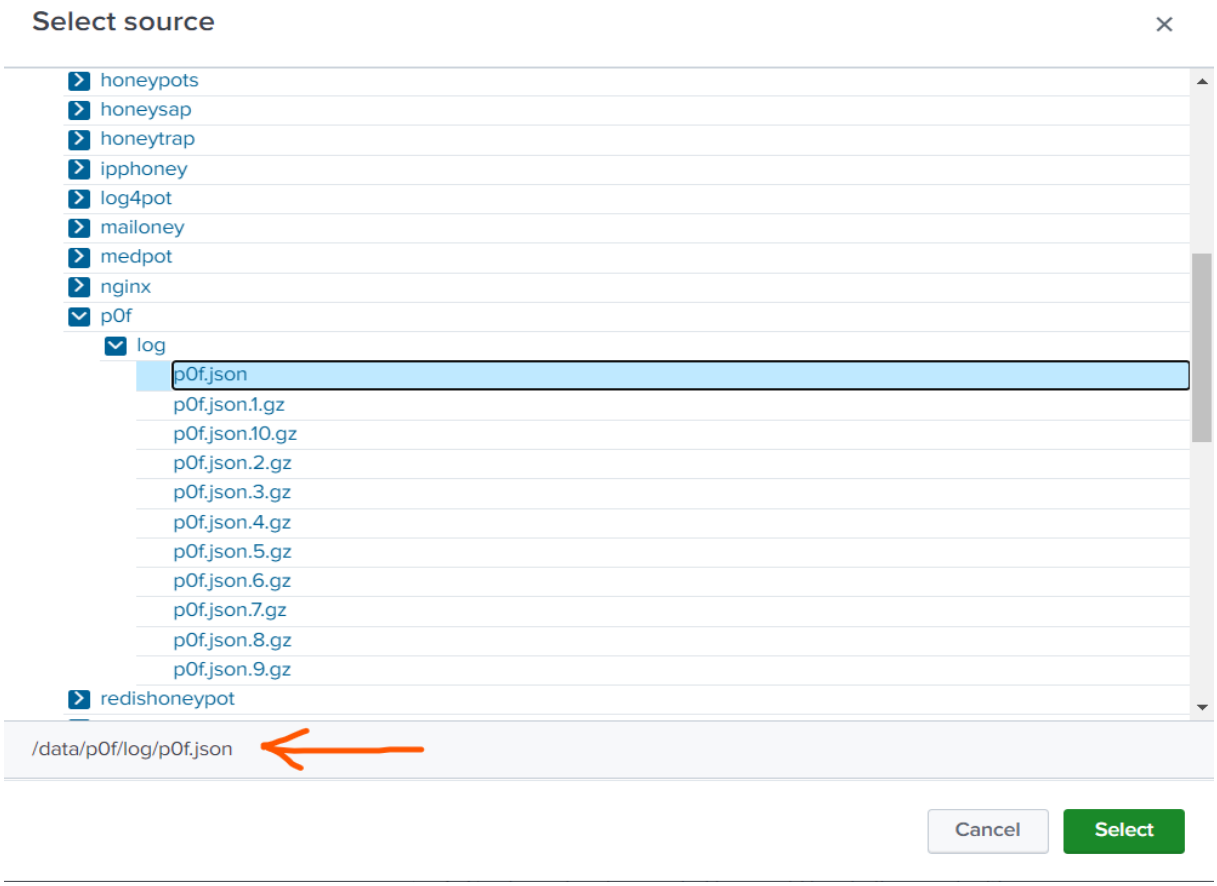
Artık dosya dizini üzerinden log okutma aşamasına geçebiliriz.



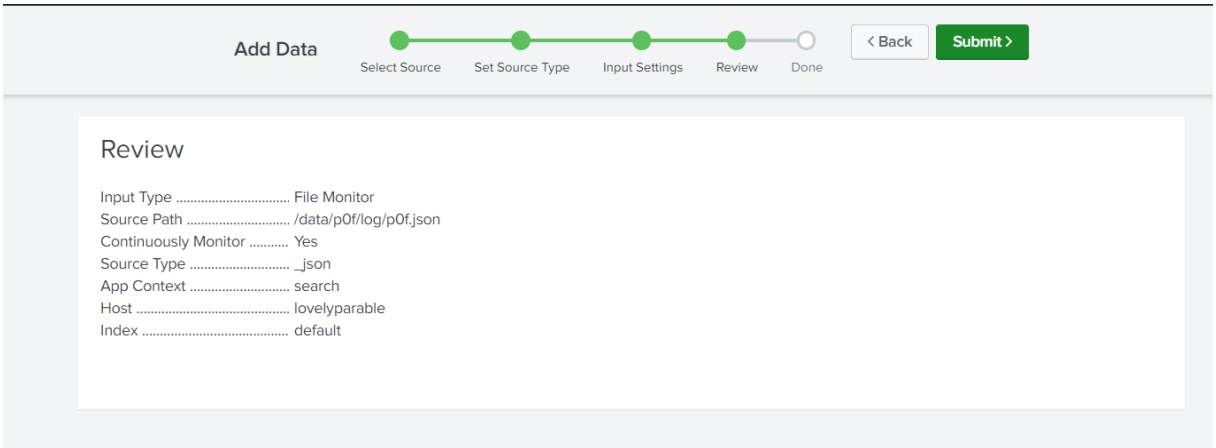
Giriş yaptıktan sonra karşımıza çıkan ana ekrandan “Monitor” seçeneğine tıklıyoruz.



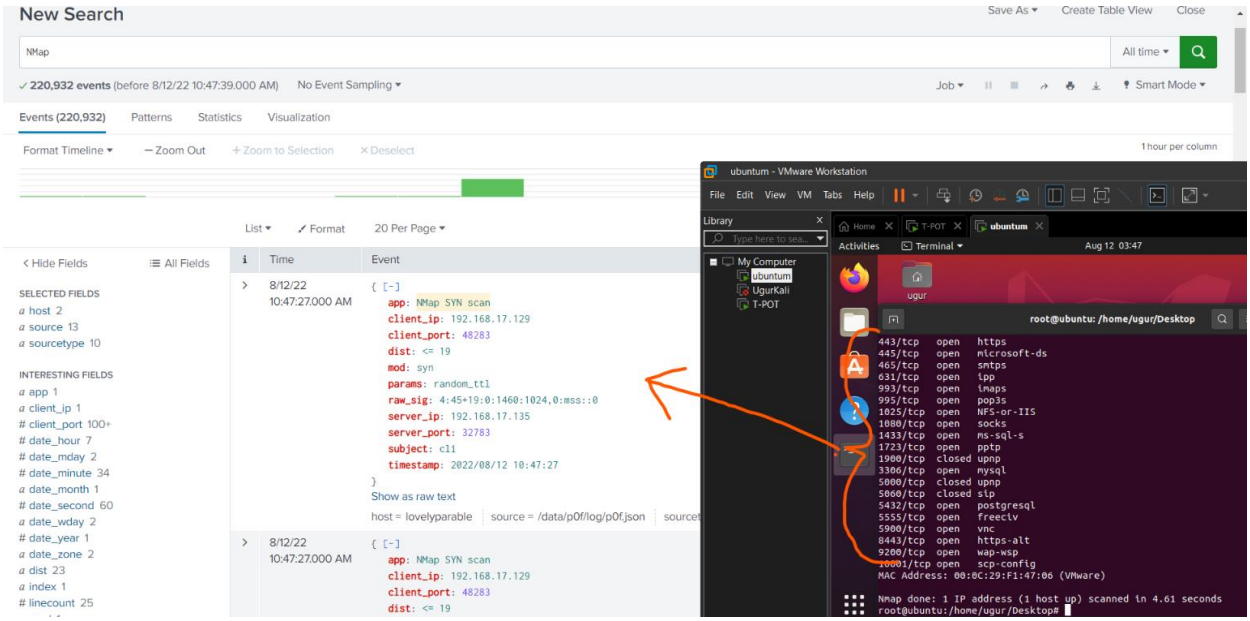
Bir sonraki adımda “Files & Directories” seçeneğini işaretliyoruz.



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



Sumbit seçeneği ile data ekleme aşamasını bitiriyoruz.



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

Bu yöntem sonucunda başarıya ulaşmış olduk.

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 gerçekleştiriceğimiz 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 yapılıcak 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.

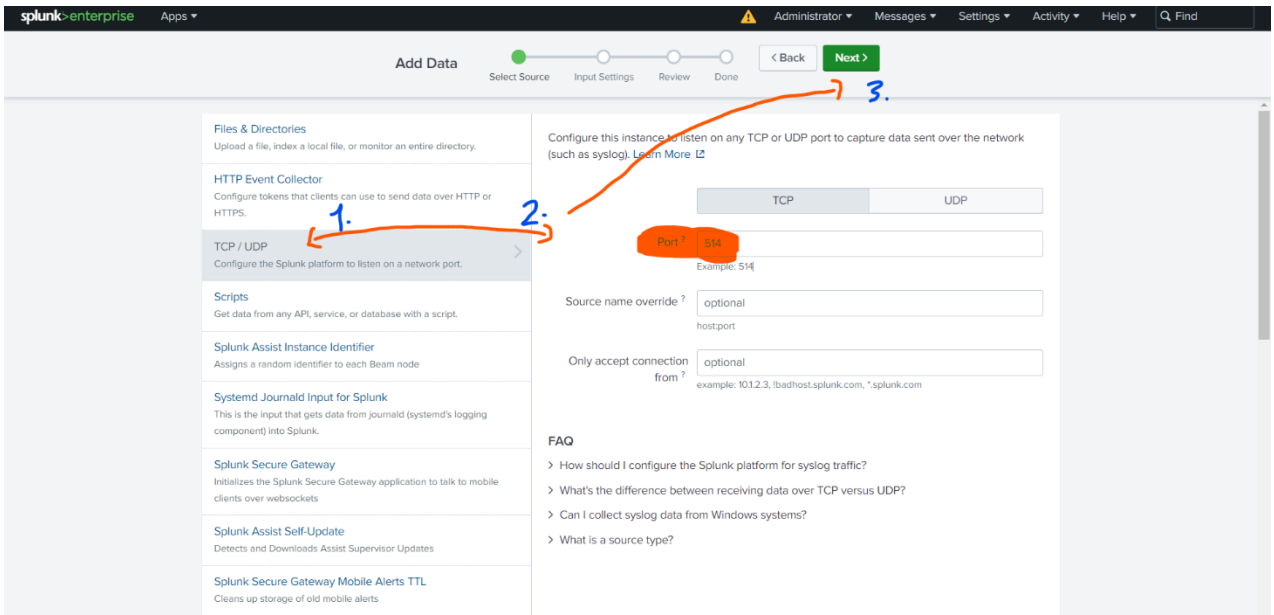
"Select an option" aşamasında 'TCP/UDP' seçeneğini seçerek işaretliyoruz.

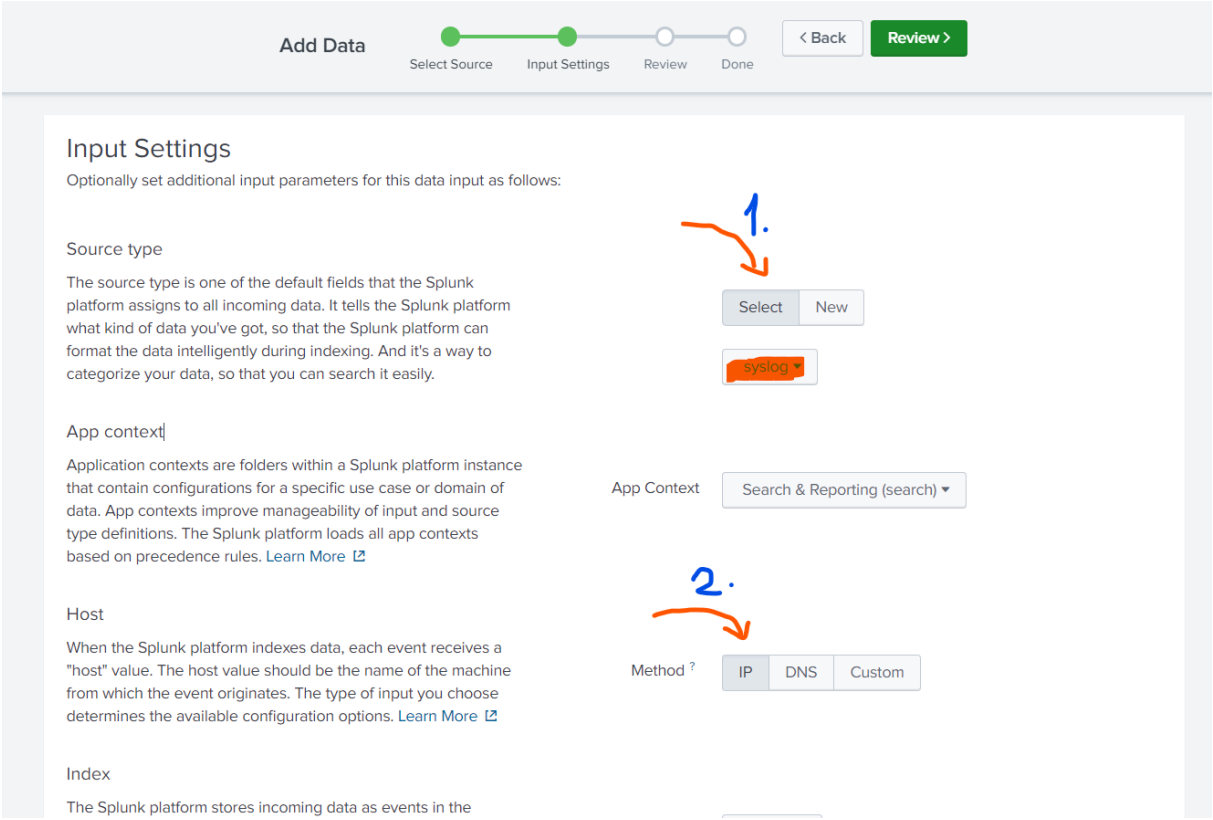
Sağ tarafta istenen değerler ;

port :514

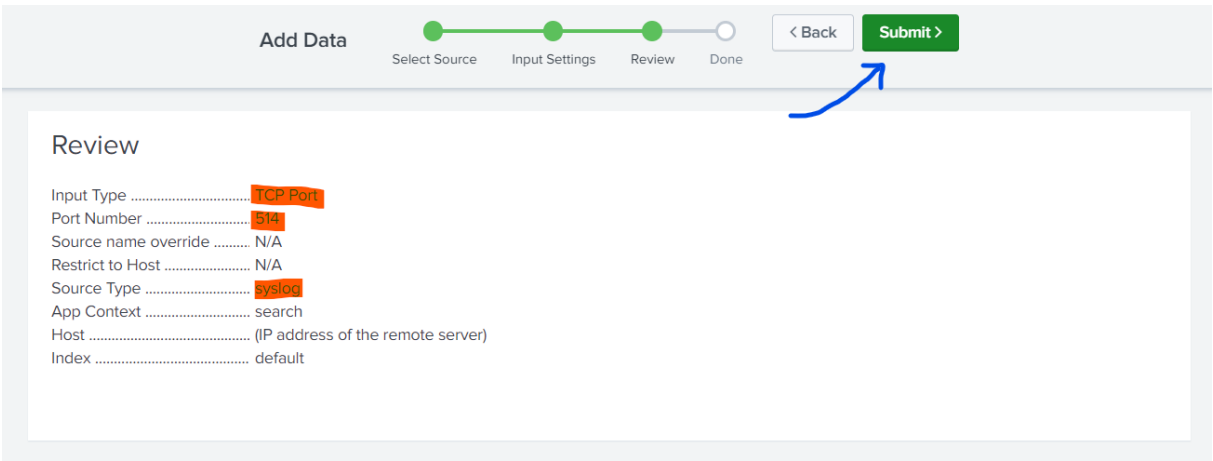
Source name override: default

Only accept connection from: default

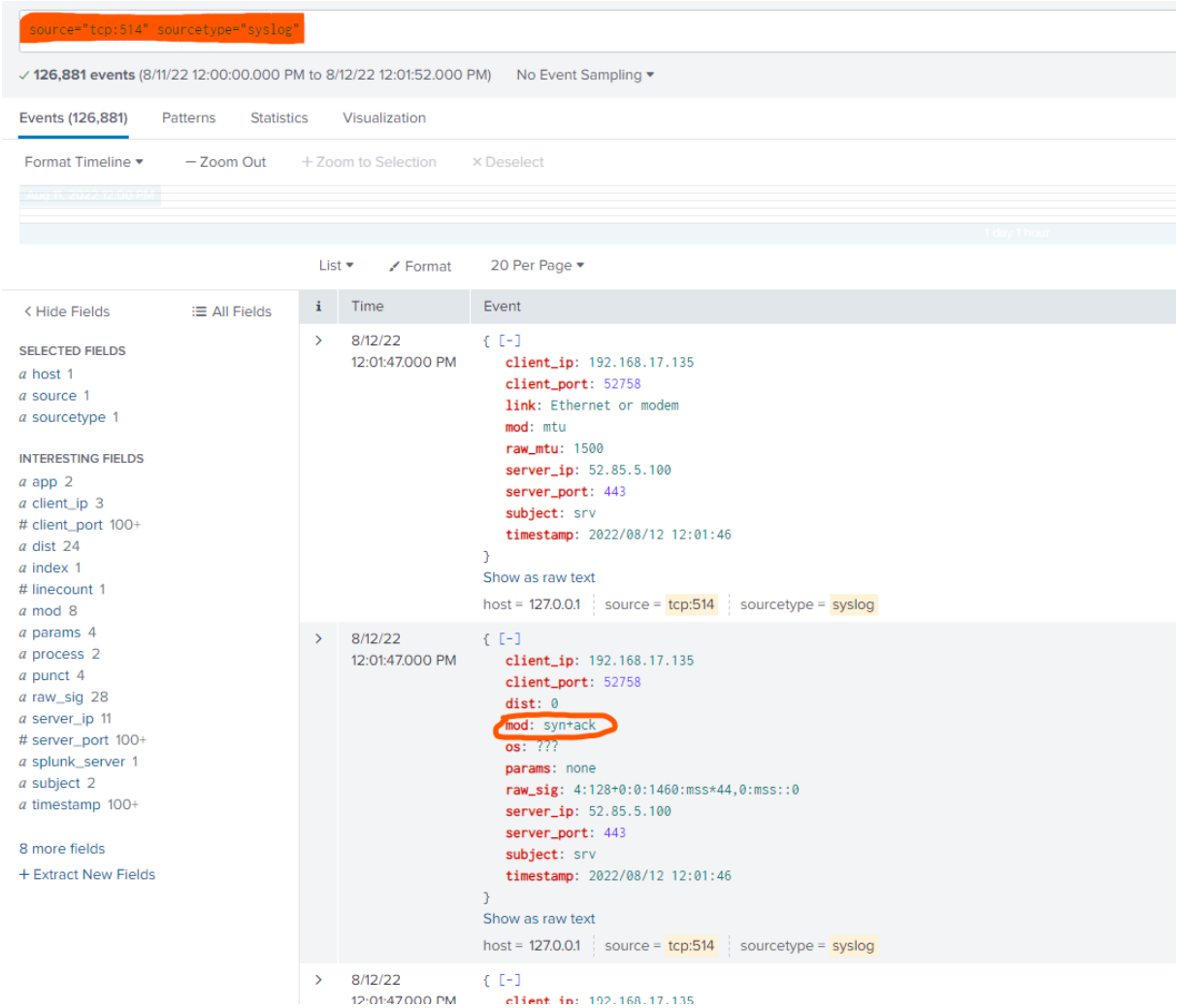




Bu adımda görseldeki gibi Source Type seçeneğini syslog olarak seçiyoruz.



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



Artık splunk belirttiğimiz hosttaki 514 portunu dinliyor ve kayıt tutuyor.

Search filtrelerini düzenledikten sonra logların başarılı bir şekilde iletildiğini 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