**T.C.**

**DOKUZ EYLÜL ÜNİVERSİTESİ**

**İKTİSADİ VE İDARİ BİLİMLER FAKÜLTESİ**

**YÖNETİM BİLİŞİM SİSTEMLERİ BÖLÜMÜ**

**DÖNEM PROJESİ**

**YBS 4002:**

**YÖNETİM BİLİŞİM SİSTEMLERİ SEMİNERİ**

**Sunucu Tabanlı Saldırı Tespit Sistemi - idsPy**

**2017469044**

**Yasin SEVEN**

**Danışman**

**Prof.Dr. Vahap TECİM**

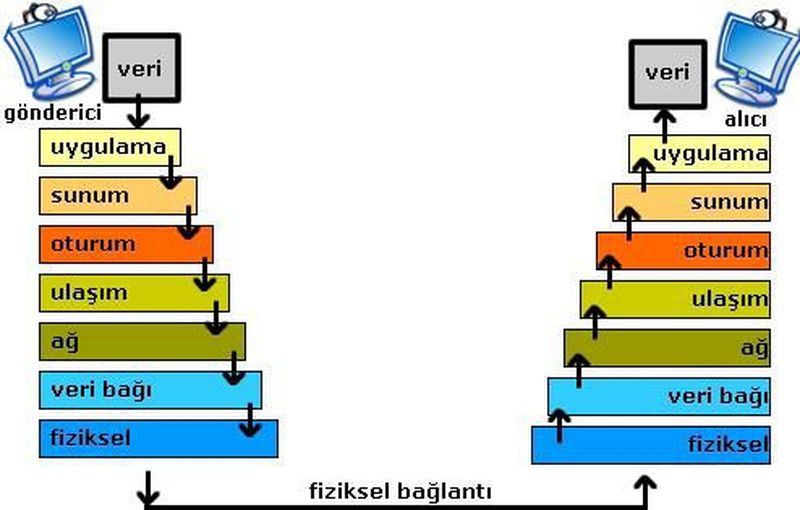
**İZMİR - 2022**

**Özet**

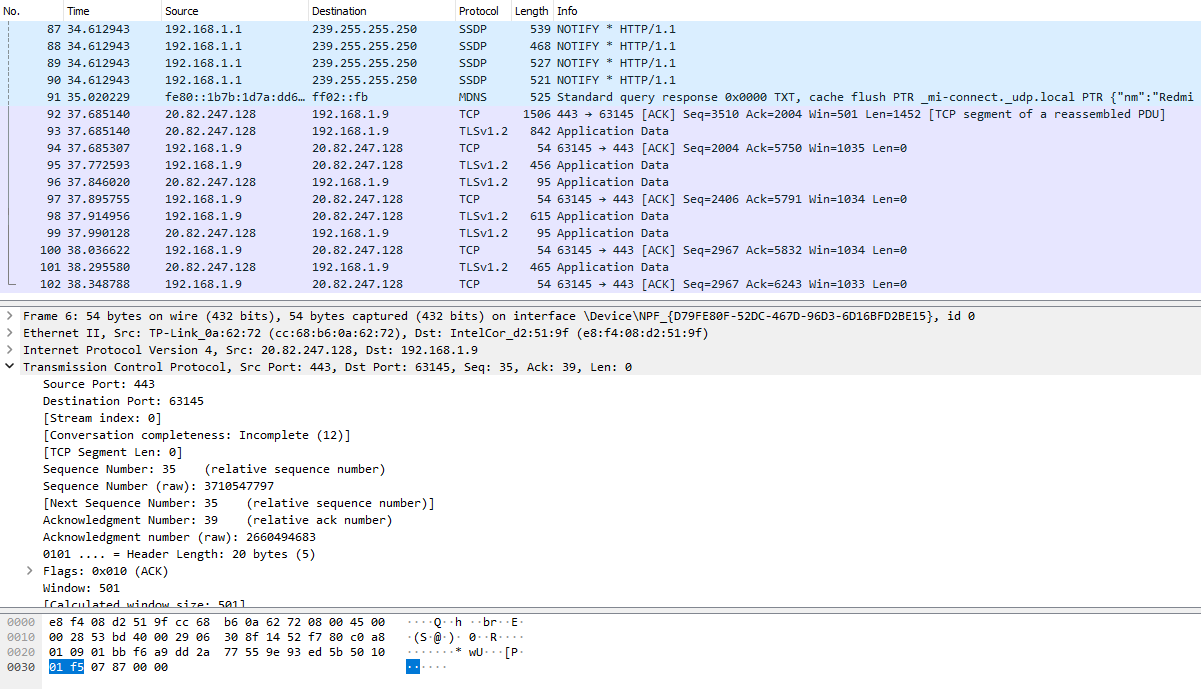
idsPy, izlenecek ağ üzerinde bir sunucu üzerine kurularak yönlendirilen ağ trafiğindeki her bir paketin içeriğini kullanıcı tarafından yazılan kurallara göre inceleyerek tehdit gördüğü taktirde alarm üreten bir siber güvenlik sistemidir. Kurulan sunucuya diğer kullanıcılar ve yöneticiler aynı ağa bağlı herhangi bir bilgisayar veya telefondan erişim sağlayıp sistemi kullanabilir. Sistemin web arayüzü responsive olarak çoğu cihaza uygun şekilde tasarlanmıştır. Yazılan kurallara göre tespit edilen paketler sunucu üzerinde bulunan veritabanına tüm bilgileriyle ve zaman damgasıyla kaydedilir. Veritabanındaki paketler web arayüzündeki tüm bilgileri sağlamak amacıyla dinamik olarak web arayüzüne aktarılır. Yakalanan paketler alarm olarak bir liste şeklinde paket bilgileriyle sistemden sorumlu analistin önüne düşer, burada incelenen paketler eğer normal bir trafikse ve saldırı değilse arşive gönderilerek alarm yok sayılır.

**Giriş**

idsPy’ın nasıl çalıştığını anlamak için öncelikle internetin nasıl çalıştığını anlamalıyız. İnternet basitçe bir cihazda oluşturulan verilerin küçük paketler haline getirilerek (text dosyaları gibi düşünebilirsiniz) diğer cihaza iletildikten sonra aynı sırayla tekrar açılması ve birleştirilmesi ile sağlanır. Aşağıdaki görselde bu iletişimin katmanlarını görebilirsiniz.



Bu paketler bilgisayarımızda aşağıdaki şekilde görselleştirilerek WireShark programı aracılığıyla izlenebilir. Bu tip programlara ağ izleme programları (Packet Sniffer) denir.

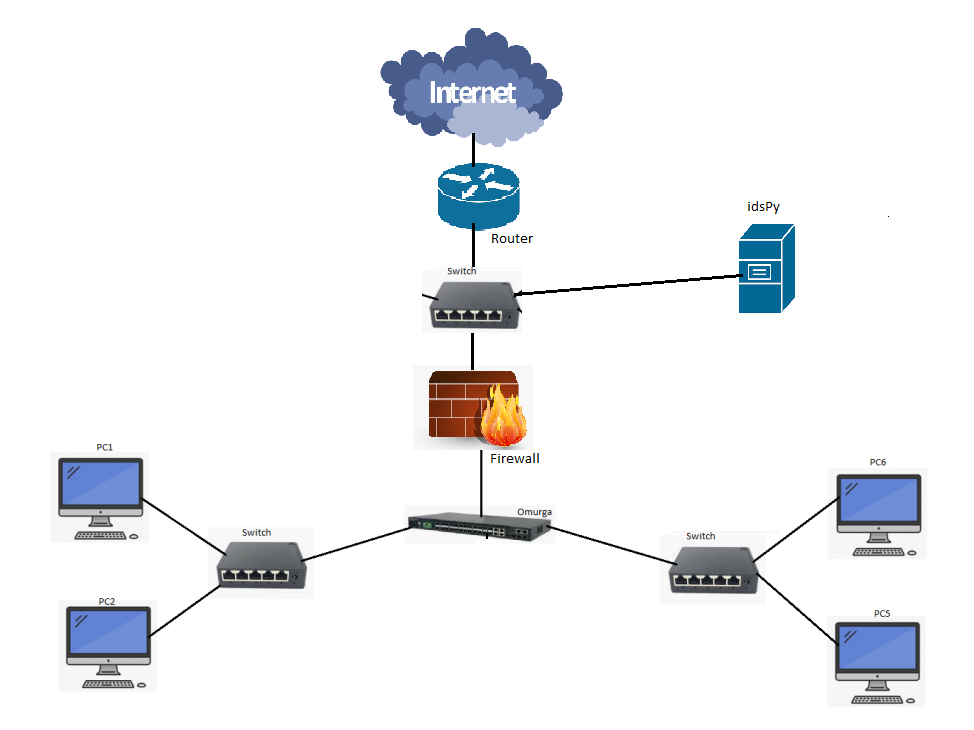


idsPy bu paketlerin içindeki bilgileri inceler ve verilen kurallara yani kelime ve cümlelere göre istenmeyen paketleri yakalar ve tüm kullanılabilecek verileri ( kaynak ip, hedef ip, kaynak port, hedef port, protokol numarası, zaman damgası vb.) ile veritabanına kaydeder. Bu veriler analiste sunulan web arayüzündeki özet ekranı veri ve grafiklerini ve alarm ekranında kullanılmak üzere depolanır.

**Yöntem - Metod**

Bu projeyi geliştirirken sanal makineler üzerinde sanal bir ağ kurarak hem sunucu geliştirmelerini yaptım hem de ağ üzerinde bulunacak olan diğer kullanıcıların tarafından geliştirme sürecine ve sistemin kullanımını test ettim.

Geliştirmeler ubuntu desktop üzerinde yapılmış ve raspberry pi (ubuntu server 22.04) üzerinde gerçek ortamda test edilmiştir. idsPy’ın network üzerindeki konumu aşağıdaki gibi olmalıdır.



**Kullanılan Teknolojiler**

Projenin sunucu tarafı Django framework’ü ile geliştirilmiş ve backend tarafında Python dili kullanılmıştır. Threading mantığı kullanılarak sunucunun aynı anda hem web server hizmeti vermesi hem de paket analizi işini yapması sağlanmıştır.

Web arayüzü responsive olarak tasarlanmış, html, css, javascript, jquery ve bootstrap ile desteklenmiştir. Veritabanı olarak ise Sqlite3 kullanılmıştır.

**Sistemin Kurulumu**

idsPy’ı istenilen linux server üzerine aşağıdaki yönetgeleri adım adım izleyerek kurabilirsiniz.

Kurulum:

* idsPy dosyalarını <https://github.com/svnyasin/idsPy> adresinden indirin
* sudo apt install python3-pip (u need pip3 for install other dependencies)
* sudo apt install tshark
  + “yes” veya “evet”i seçin
* sudo pip3 install django django-filter pyshark pycountry
* rm db.sqlite3
* rm alert/migrations/0001\_initial.py
* sudo python3 [manage.py](http://manage.py) makemigrations
  + - Create model CapturedPacket” yazısını görünce ctrl+c klavye kombinasyonuyla işlemi durdurun
* sudo python3 [manage.py](http://manage.py) migrate
  + “Applying sessions.0001.initial... OK” yazısını görünce ctrl+c klavye kombinasyonuyla işlemi durdurun
* sudo python3 [manage.py](http://manage.py) createsuperuser
  + geçici olarak dinlemeyi etkinleştirip işleme devam etmek için ağ arayüzlerinden birini rakam yazarak seçin
  + kullanıcı adı yazın
  + e-posta yazın (isteğe bağlı)
  + superuser created successfully yazısını gördüğünüzde ctrl+c ile işlemden çıkabilirsiniz
* İşte bu kadar, şimdi kendi sunucunuzu başlatabilirsiniz!

Sunucuyu Başlatma ve Paket Dinlemeyi Aktifleştirme:

* sudo python3 [manage.py](http://manage.py) runserver 0:80

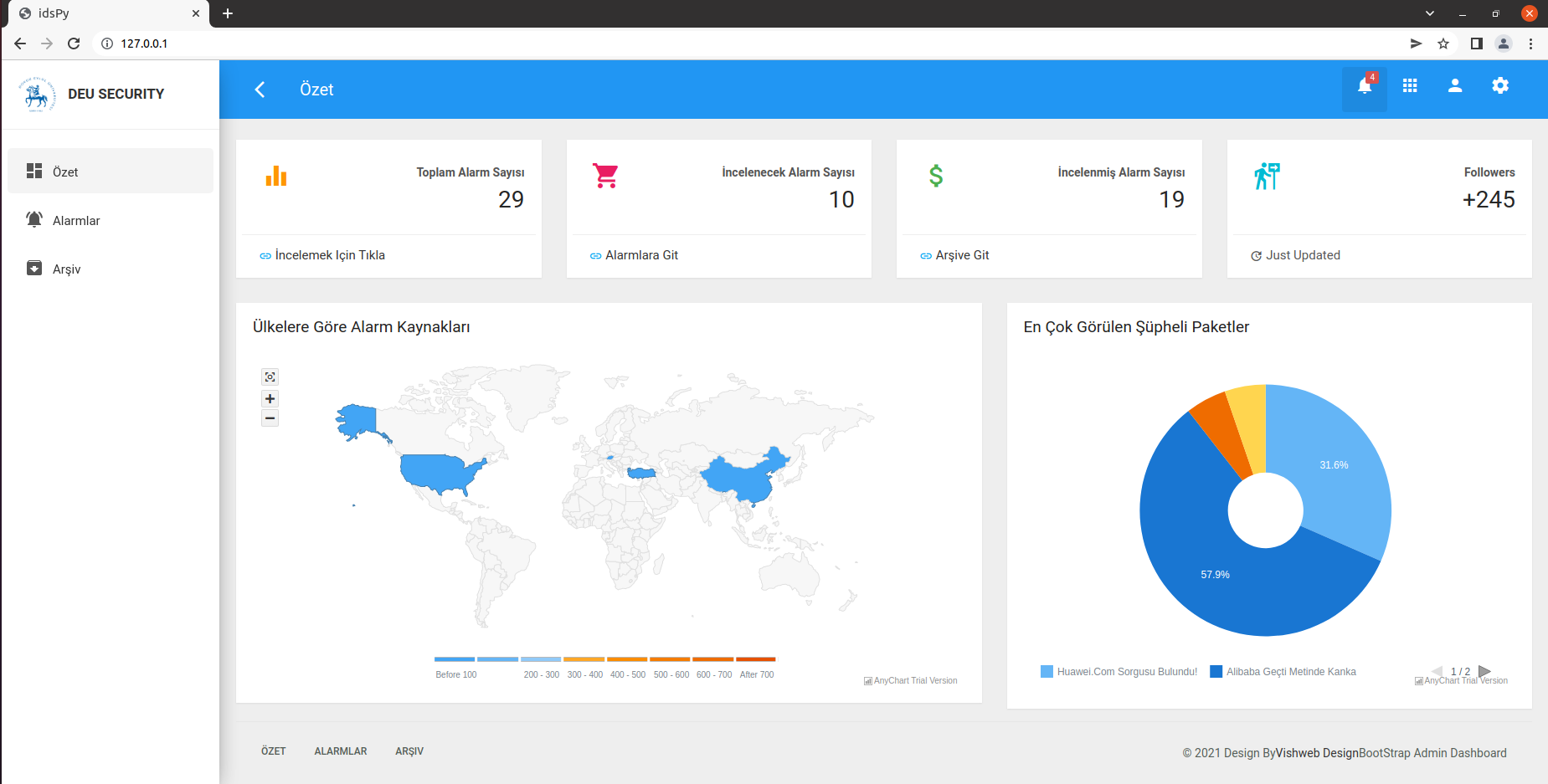
Sunucuyu yukarıdaki komutla başlattıktan sonra artık diğer cihazlarınızdan sunucu adresini tarayıcınıza yazarak idsPy’ın web arayüzüne ulaşabilirsiniz. Sunucuyu başlattığınızda cihazınızdaki ağ arayüzleri numaralı şekilde karşınıza çıkacaktır. Burada rakamlardan istediğiniz arayüzü seçerek dinlemeyi başlatabilirsiniz.

Not: idsPy en az iki adet ağ arayüzüne ihtiyaç duyar, bunlardan biri iç ağa bağlıyken iletişim için kullanılır diğeri ise analiz edilecek paketlerin iletileceği arayüzdür. Eğer iki işlem için aynı arayüzü kullanırsanız paketler çakışacak ve gereksiz alarmlar üreyecektir.

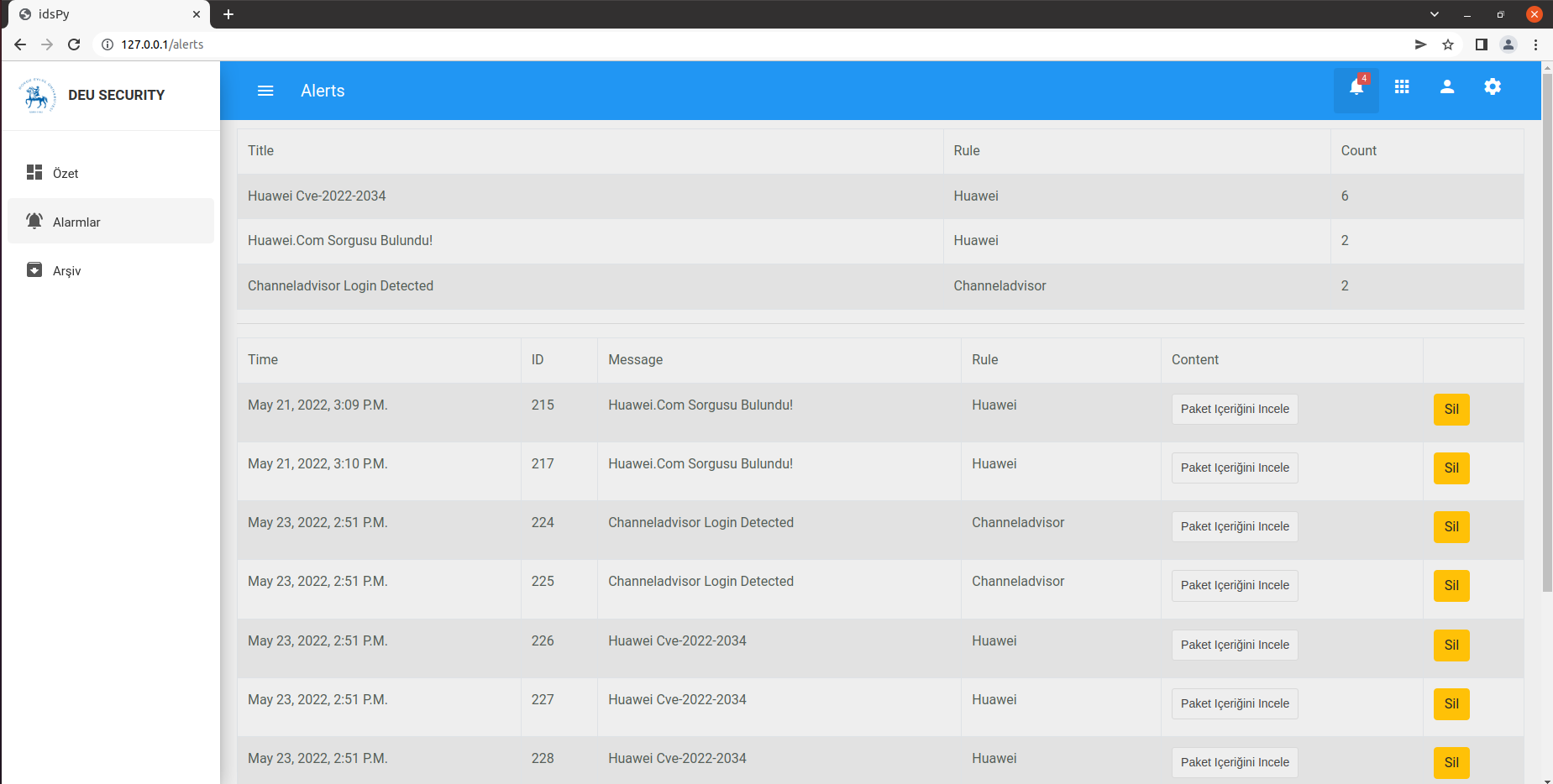
Not: Şifreli paket içeriklerinin analiz edilebilmesi için ağınıza bir proxy firefox kurarak, şifreli trafiği bölebilir ve şifresi çözülmüş trafiği idsPy’a yönlendirerek tüm paketleri sisteme inceletebilirsiniz.

**Göreseller**

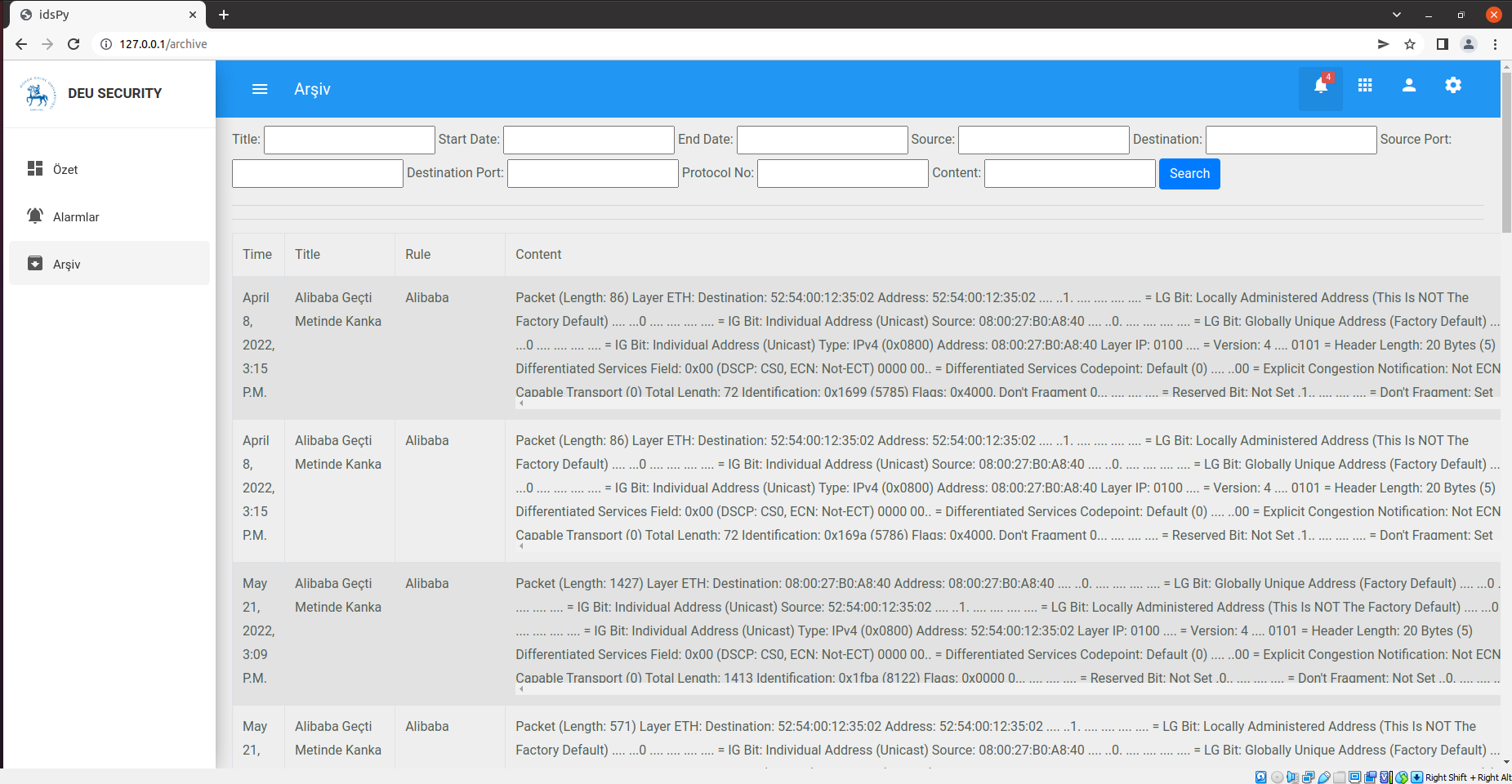
Özet Ekranı:



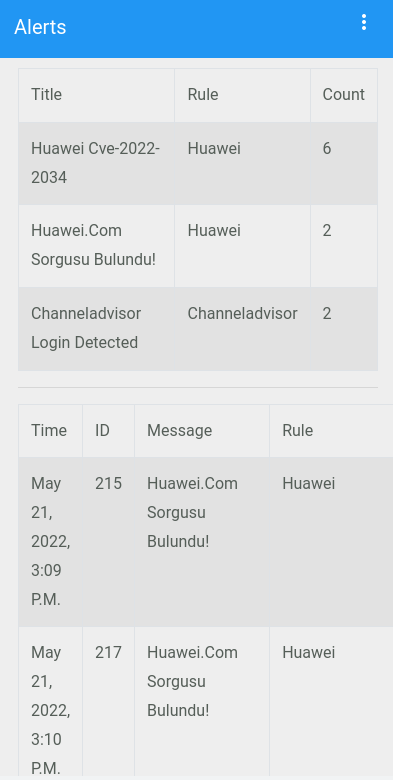
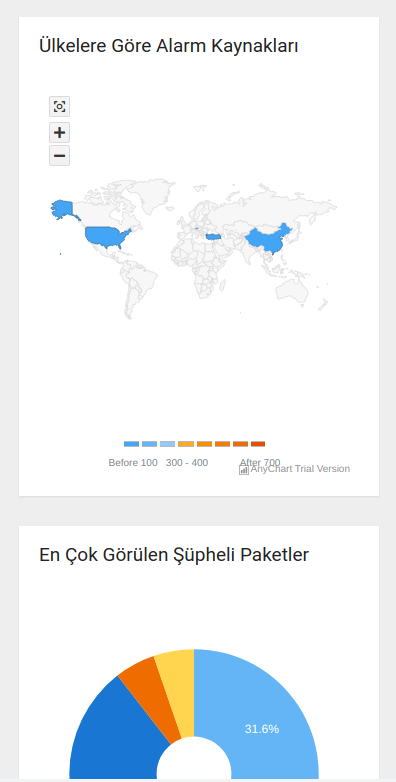
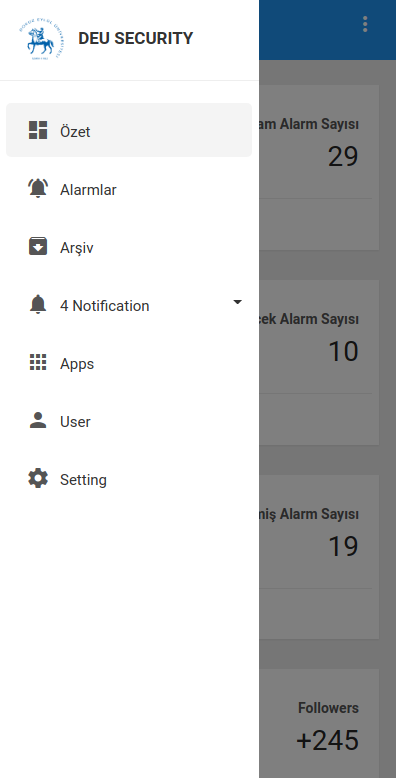
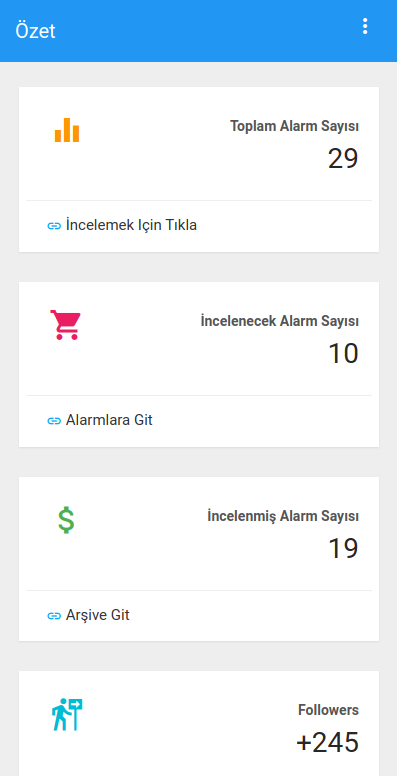
Alarmlar Ekranı:



Arşiv Ekranı:



Mobil Ekranlar:



**Sonuç**

Günümüz dünyasında siber güvenlik hem şirketler hem de bireyler için vazgeçilmez ve düşünülmesi gereken bir olgu haline gelmiştir. Bu nedenle her organizasyon ve birey kendini siber dünyada korumak adına katmanlı bir yapıda savunma sistemleri kurmalı ve önlemler almalıdır.

Bu proje ağ üzerine doğru bir şekilde entegre edilerek paketlerin analizi ve ağ trafiğinin izlenmesine yardımcı olur ve ücretsiz bir şekilde aşağıdaki bağlantıdan indirilip geliştirilebilir veya kullanılabilir.

https://github.com/svnyasin/idsPy

Proje daha fazla zaman ve daha çok kaynak ayrılarak aşağıdaki öneriler ışığında geliştirilebilir.

* Proje şuanda imza tabanlı bir analiz yapmaktadır. Daha iyi analiz için davranış tabanlı tespit fonksiyonu eklenebilir.
* Şifreli trafiğin izlenmesi için (Örneğin https veya ssh bağlantıları) ağ üzerine proxy firewall kurulup network tap olarak kullanılarak şifresiz trafik sunucu üzerine yönlendirilip tüm akış çıplak bir şekilde izlenebilir.
* Diğer IDS platformlarının (snort) kurallarının sisteme entegre edilerek idsPy içerisinde kullanılması sağlanabilir.
* Veri tabanı olarak elastic search eklenerek alarmların daha hızlı analizi, işlenmesi ve arşivlenmesi sağlanabilir.
* Analist görüşleri ile arayüz ve analiz fonksiyonları geliştirilebilir.

**Kaynakça**

* <https://www.djangoproject.com/start/>
* <https://www.youtube.com/watch?v=wWio-D2ObPo>
* <https://www.youtube.com/watch?v=hbx39adciac>
* <https://realpython.com/intro-to-python-threading/>
* <https://github.com/KimiNewt/pyshark>
* <https://github.com/nadrojisk/python-ids>