T-POT KULLANARAK SALDIRI TESPİT ANALİZİ

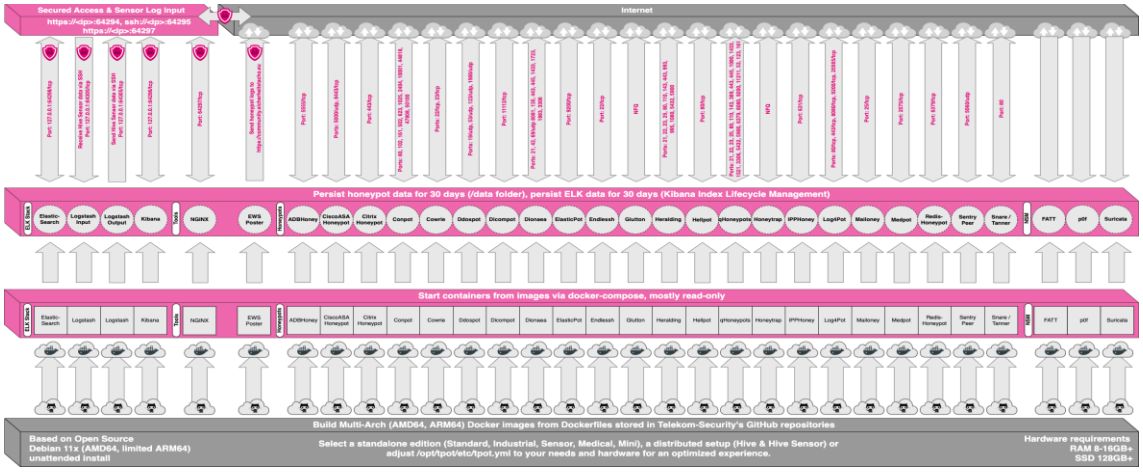
Yusuf Cennetoğlu

Honeypot (Bal küpü) Nedir

Bal küpü saldırganların kullandığı saldırı türlerini tespit ve incelemek için kullanılan ve aynı zamanda sisteme zarar vermeye çalışan saldırganları tuzağa düşürmeyi sağlayan ağa bağlı bir sistemdir. Üzerinde saldırganı tuzağa çekmek için kasıtlı olarak açıklık bulundurur. İnternette potansiyel bir hedef olarak hareket eder.

T-POT Nedir

Birçok honeypot aracını içerisinde bulunduran ve saldırı izleme imkanı sunan bir araçtır. İçerisinde barındırdığı honeypotlardan aldığı veri toplar ve ayrıntılı bir şekilde analiz etmemiz için bizlere sunar.

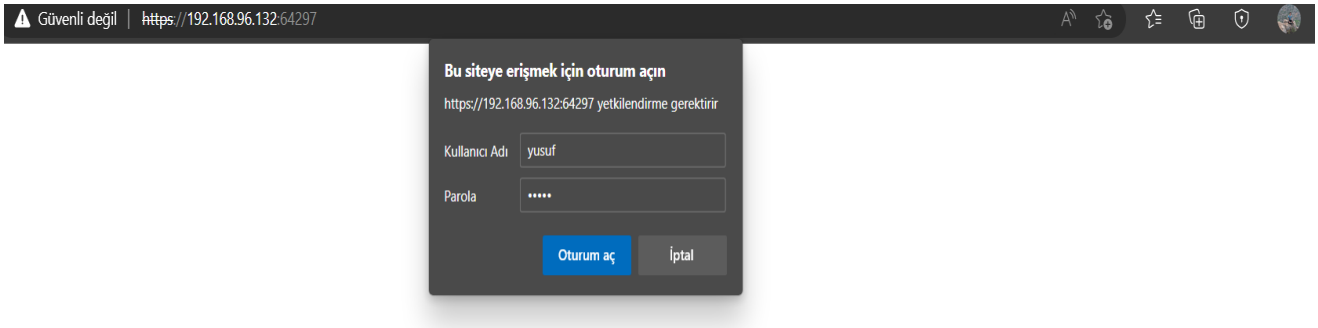


T-pot mimarisi yukarıdaki şekilde gösterilmiştir. T-Pot'un honeypot araçlarından hangi verileri hangi portlar üzerinden aldığı gösterilmiştir

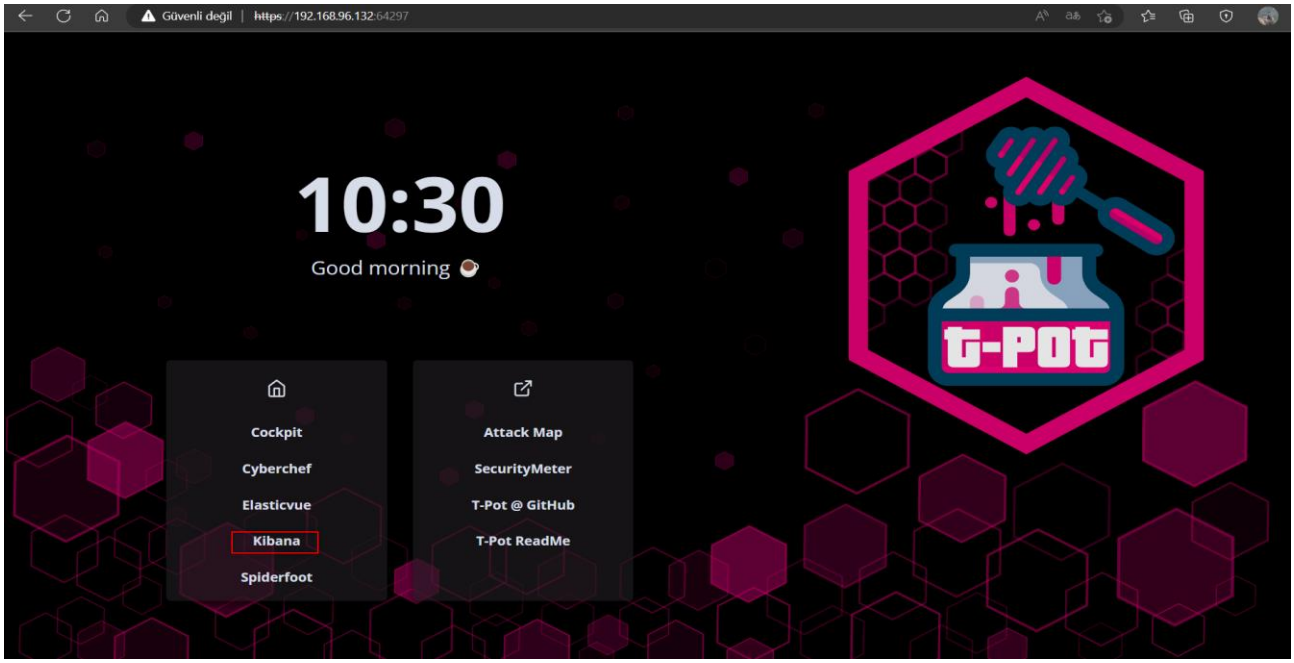
Saldırı Tespit ve Analizi Nasıl Yapılır

İşe ilk olarak T-Pot'u çalıştırarak başlıyoruz.

Kullanıcı adı ve şifremizi girdikten sonra WEB sayfası erişimi için bize verilen bilgileri tarayıcımızda açıyoruz.



Karşımıza çıkan ekrana kişisel bilgilerimizi girerek işlemimize devam ediyoruz.



Bu işlemlerden sonra T-Pot'un arayüzüne erişiyoruz. Saldırı Tespit ve Analizi için *Kibana* aracını kullanacağız. Fakat diğer araçlardan da kısaca bahsetmek gerekirse;

Cockpit: Gerçek zamanlı performan izleme web terminalidir.

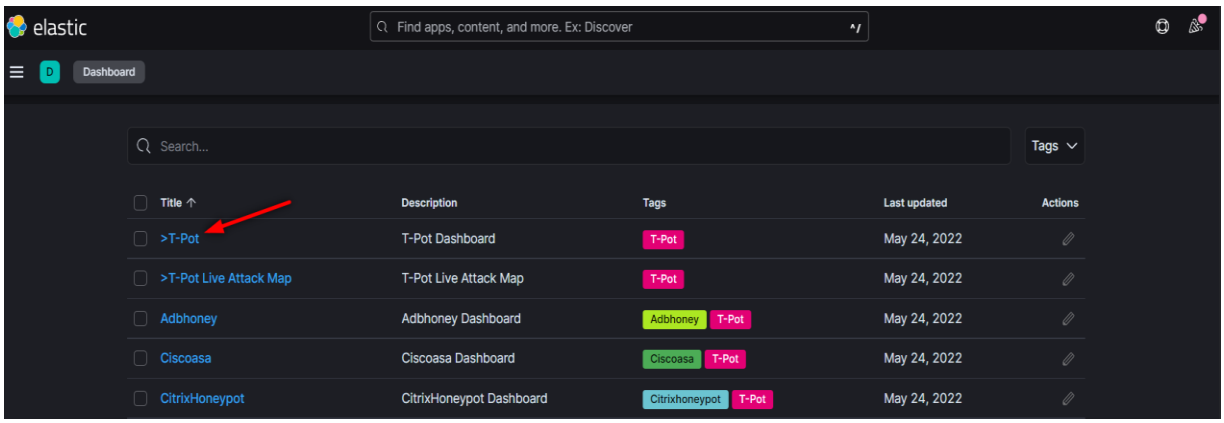
Cyberchef: Şifreleme ve verilerin analizi için kullanılan bir web terminalidir.

Elasticvue: Tarayıcı için ücretsiz ve açık kaynaklı bir elasticsearch gui'dir.

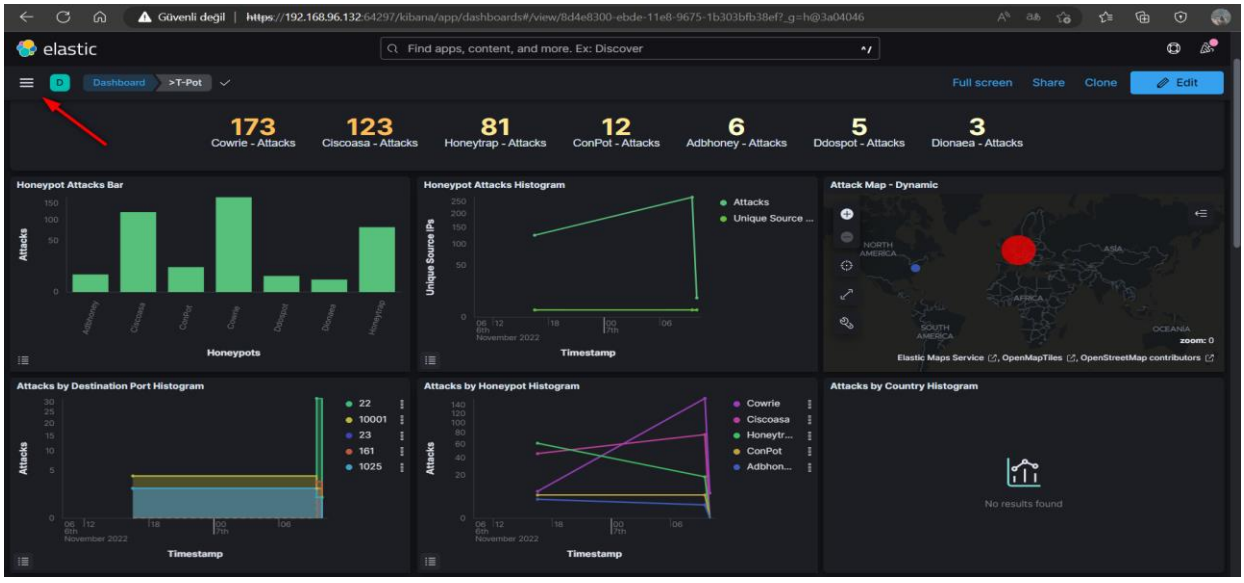
Kibana: Elasticsearch'ün üstünde çalışan ve kullanıcılara verileri analiz etme ve görselleştirme olanağı sağlayan bir görselleştirme katmanıdır.

SpiderFoot: Belirli bir hedef hakkında istihbarat toplama sürecini otomatikleştirme işlevi olan bir açık kaynaklı keşif aracır.

Bu bilgilendirmelerden sonra devam edecek olursak karşımıza çıkan arayüzden Kibanayı aracını seçiyoruz.

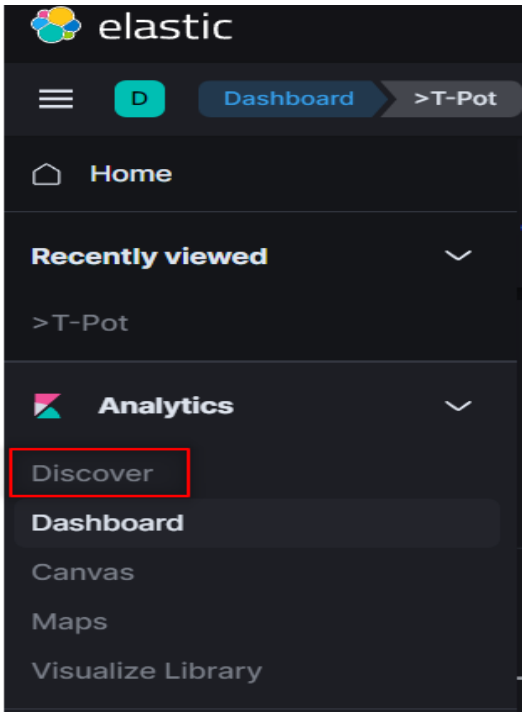


Yukarıda gösterdiği gibi karşımıza gelen seçeneklerden T-Pot seçerek Kibanın arayüzüne erişim sağlıyoruz.



Kibananın görsel arayüzü görselleştirilmiş bir şekilde şekildeki gibi karşımıza geliyor.

Saldırı analizi yapmak için sol üst köşede bulunan okla gösterilen seçeneğe tıklıyoruz.

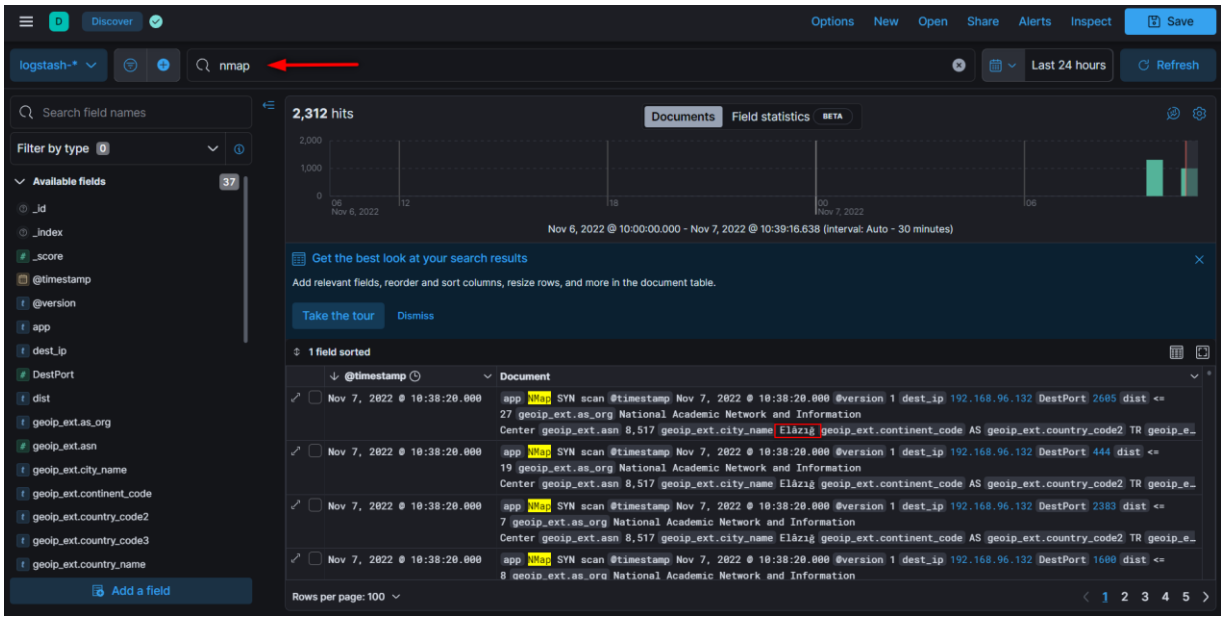


Daha sonra karşımıza açılan pencereden ***Discover*** seçeneğini seçerek işlemimize devam ediyoruz.

Saldırı analizini görmek için aşağıda gösterildiği gibi Linux makinemizden diğer makinemizin ip adresine basit bir ***nmap*** taraması yapıyoruz.

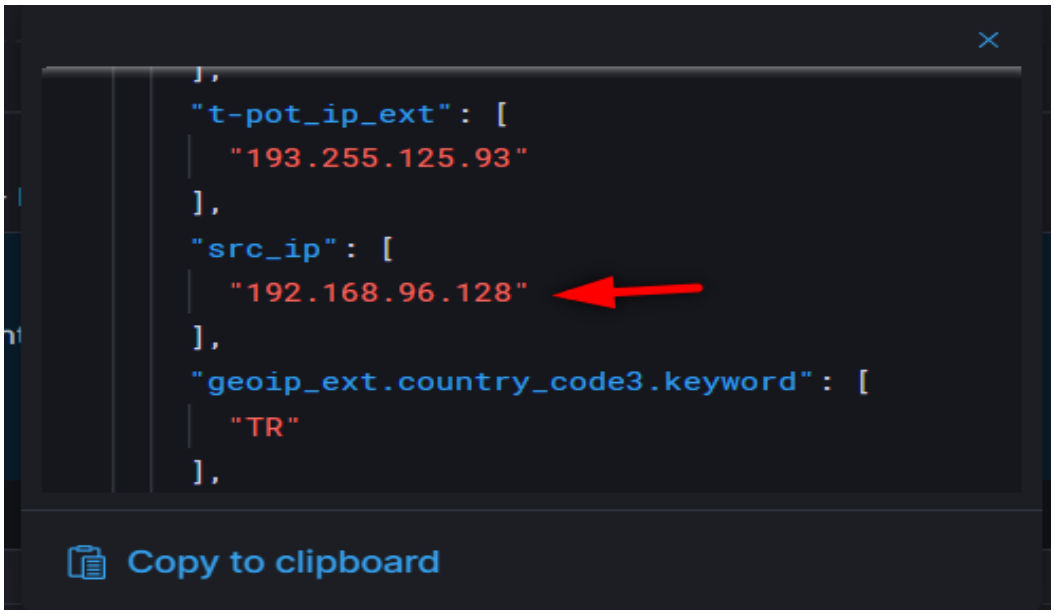
Nmap taraması sonucunda birçok portun açık olduğunu bizlere gösterecektir.

Nmap taramasının nasıl bir sonuç verdiğini görmek için T-Pot'a geri dönüyoruz.



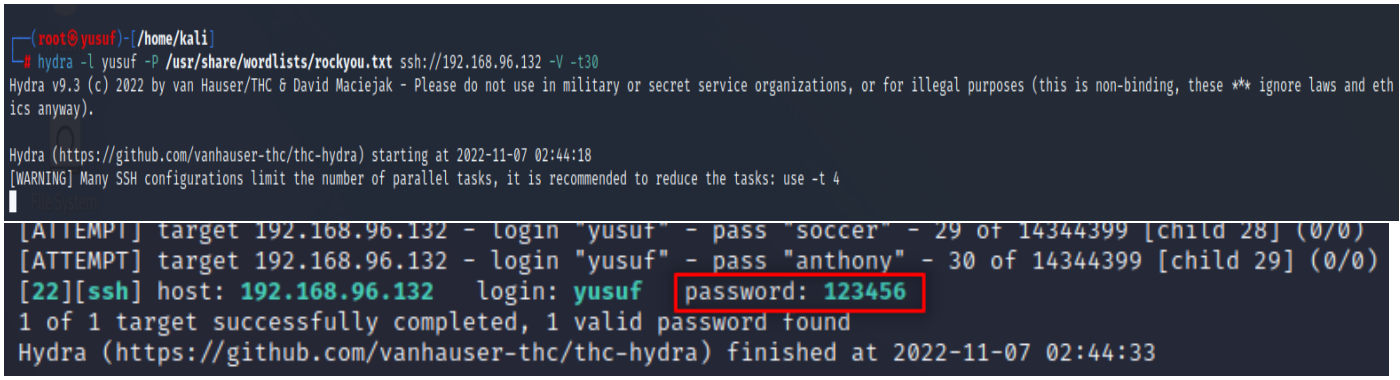
Daha sonra nmap filtrelemesi yaptığımızda saldırı türünden konuma kadar birçok bilgiyi bizlere veriyor.

Daha detaylı bir incelme yaparsak eğer aşağıda gösterildiği gibi saldırgan cihazın ip adresi gibi bilgilere de ulaşıyoruz.

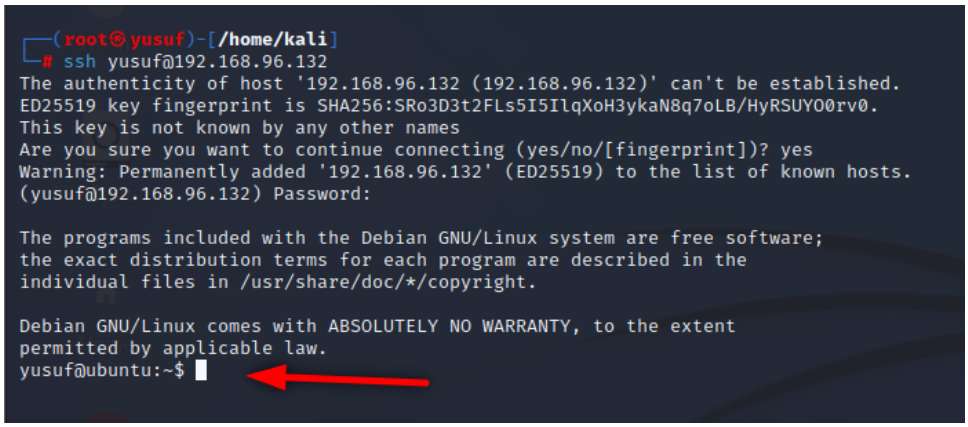


Daha sonra açık portlar üzerinden bir saldırı gerçekleştirmek istiyorum ve bu sebeple Linux makinemize geri dönüyorum. Yapacak olduğumuz şey ise açık olan ***ssh*** portu üzerinde *hydra* aracını kullanarak bir Brute-force attack gerçekleştirmek. Bu işlem sonucunda hydra aracımızdan öğrendiğimiz şifre ile sisteme giriş yapacağız yani bizim için hazırlanan açık port tuzağına düşeceğiz.

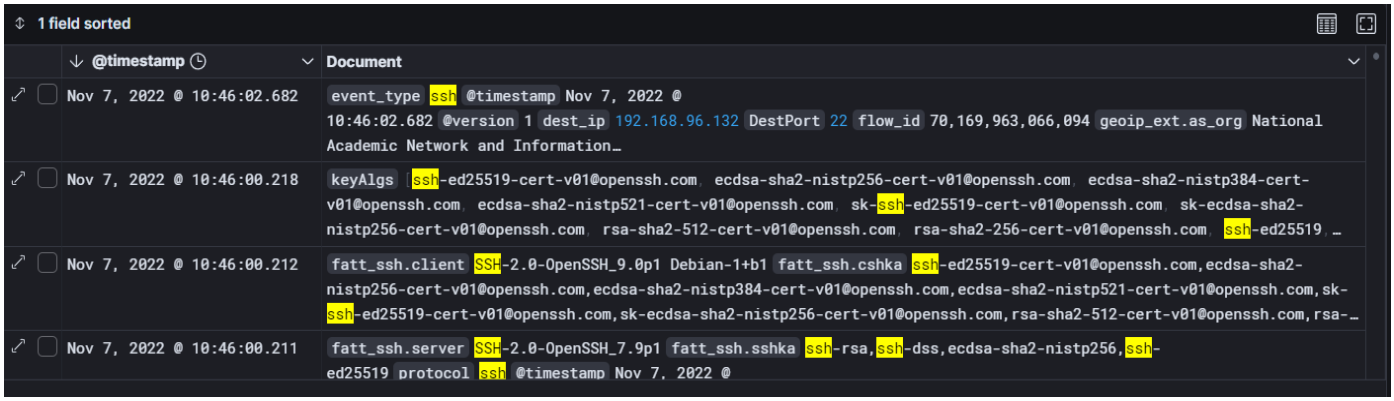
Şimdi Linux makinemizde aşağıda gösterildiği gibi saldırımızı gerçekleştiriyoruz.



Yukarıda gösterildiği gibi ssh bağlantısı yapmamız için bir şifre buluyoruz. Şimdi ise bu şifreyi kullanarak ssh bağlantımızı gerçekleştiriyoruz ve sisteme erişiyoruz

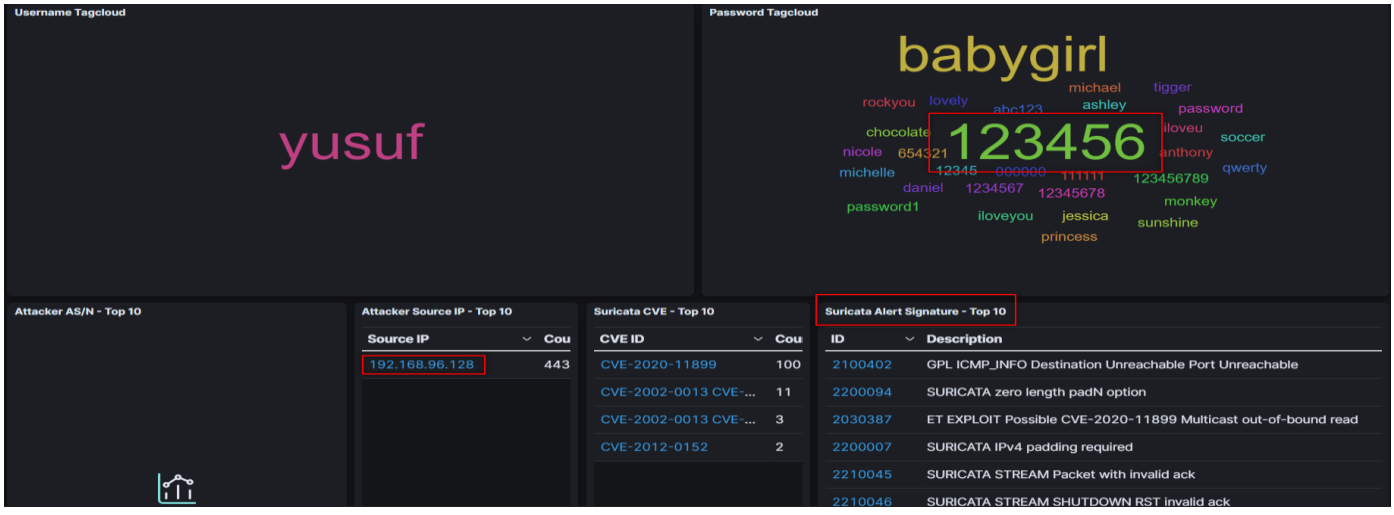


Ssh bağlantımızın ardında T-Pot'a geri döndüğümüzde ssh filtrelemesi yapıyoruz ve yapılan saldırı ile ilgili kayıtları aşağıda olduğu gibi bizlere sunuyor.



Yukarıda gösterilenlerden farklı olarak detaylı incelemeler sonucunda farklı bilgilere de ulaşmak mümkündür

Kibananın görselleştirilmiş arayüzüne geri döndüğümüzde ise aşağıdaki gibi bilgilerle karşılaşıyoruz.



Burada ise saldırgan cihazın ip adresinden hangi şifre ile giriş yaptığına kadar bazı bilgiler bizlere gösteriliyor.