

T-POT KULLANARAK SALDIRI TESPİT ANALİZİ



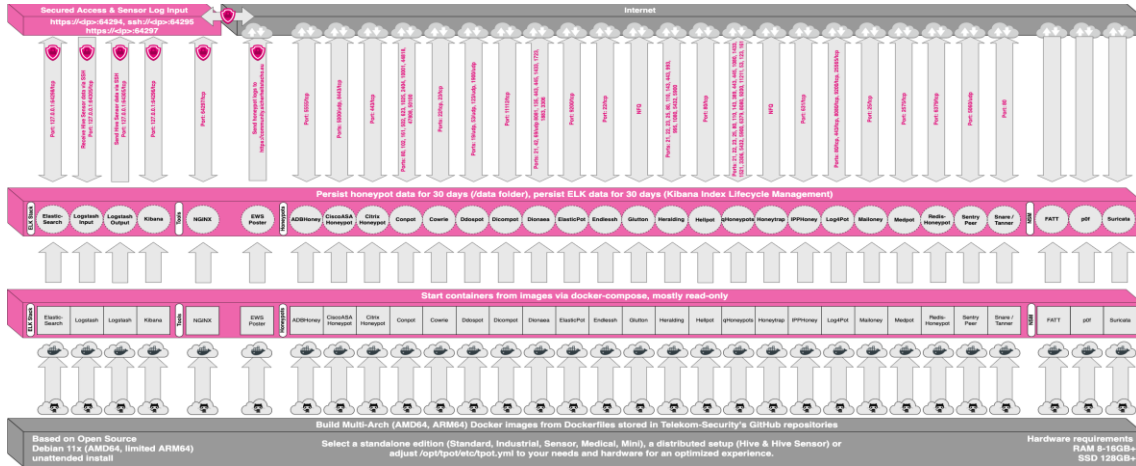
Yusuf Cennetoğlu

Honeypot (Bal k p ) Nedir

Bal k p  saldırganların kullandığı saldırı t rlerini tespit ve incelemek i in kullanılan ve aynı zamanda sisteme zarar vermeye  alıřan saldırganları tuzağına d ř rmeyi saėlayan aėa baėlı bir sistemdir.  zerinde saldırganı tuzağına  ekmek i in kasıtlı olarak a ıklık bulundurur. İnternette potansiyel bir hedef olarak hareket eder.

T-POT Nedir

Bir ok honeypot aracını i erisinde bulunduran ve saldırı izleme imkanı sunan bir ara tır. İ erisinde barındırdığı honeypotlardan aldıėı veri toplar ve ayrıntılı bir řekilde analiz etmemiz i in bizlere sunar.



T-pot mimarisi yukarıdaki řekilde g sterilmiřtir. T-Pot'un honeypot ara larından hangi verileri hangi portlar  zerinden aldıėı g sterilmiřtir

Saldırı Tespit ve Analizi Nasıl Yapılır

İşe ilk olarak T-Pot'u çalıştırarak başlıyoruz.

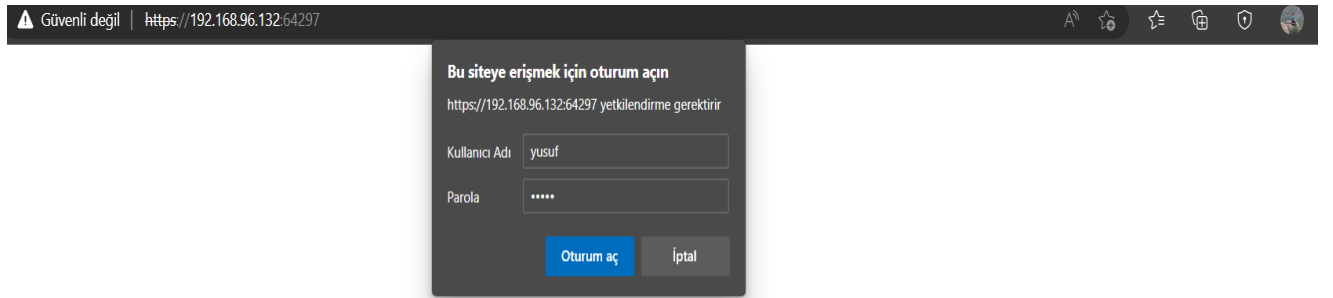
```

  _____
 | T-POT 2000 |
 |_____|

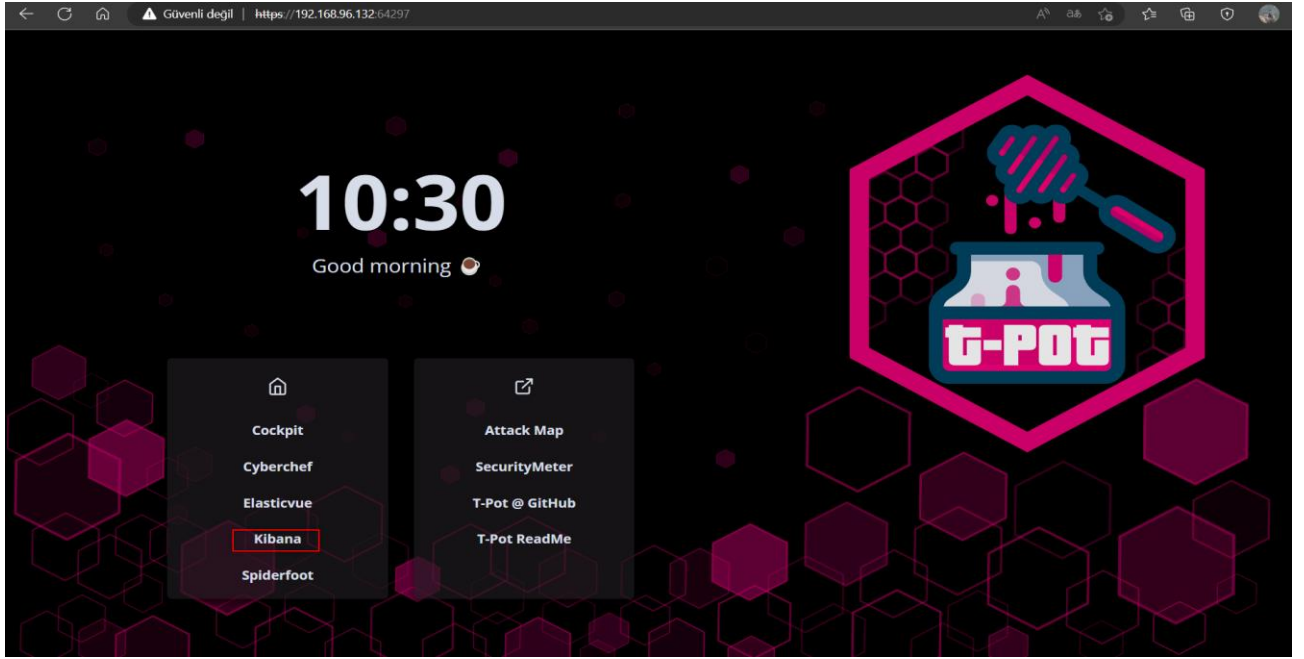
---- [ deadsnuggle ] [ Mon Nov 7 2022 ] [ 07:24:08 ]
|
| IP: 192.168.96.132 (193.255.125.93)
| SSH: ssh -l tsec -p 64295 192.168.96.132
| WEB: https://192.168.96.132:64297
| ADMIN: https://192.168.96.132:64294
| BLACKHOLE: [ DISABLED ]
|
----

deadsnuggle login: tsec
Password:
Linux deadsnuggle 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64
Last login: Mon Nov 7 06:40:25 UTC 2022 from ::ffff:192.168.96.1 on web console
[tsec@deadsnuggle:~]$
```

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.

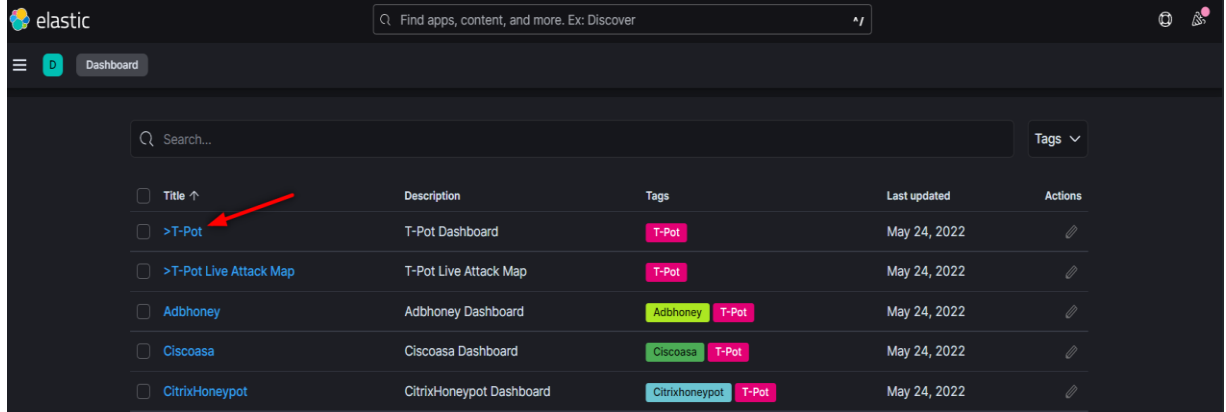
Cyberchef: Şifreleme ve verilerin analizi için kullanılan bir web terminalidir.

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

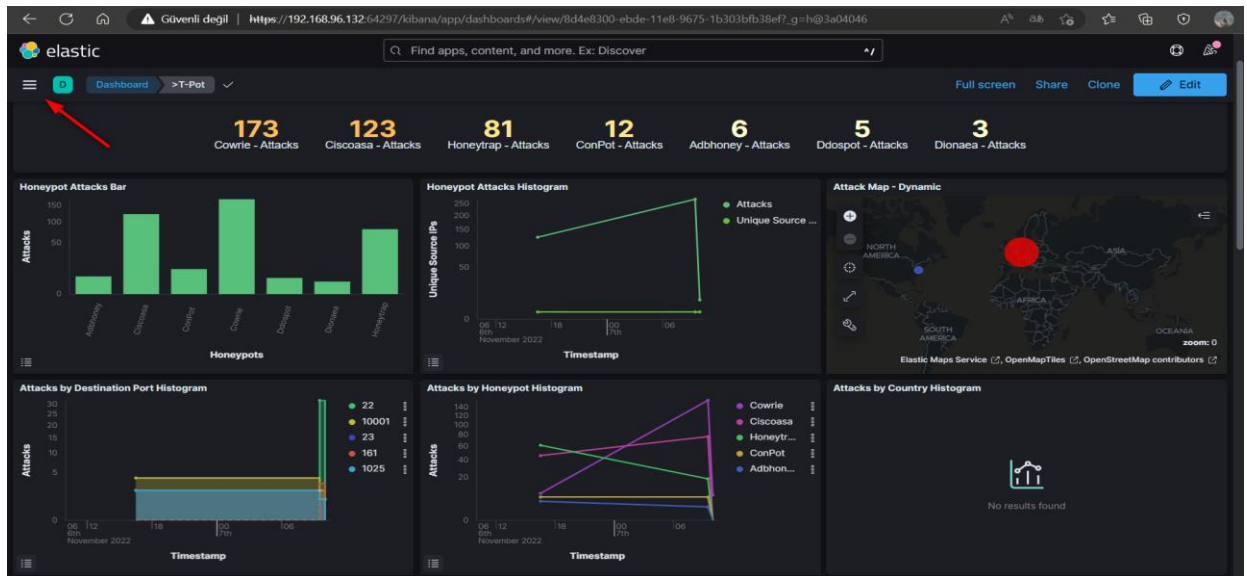
Kibana: Elasticsearch'ün üstünde çalışan ve kullanıcılara verileri analiz etme ve görselleştirme olanağı sağlayan bir görselleştirme katmanıdır.

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

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

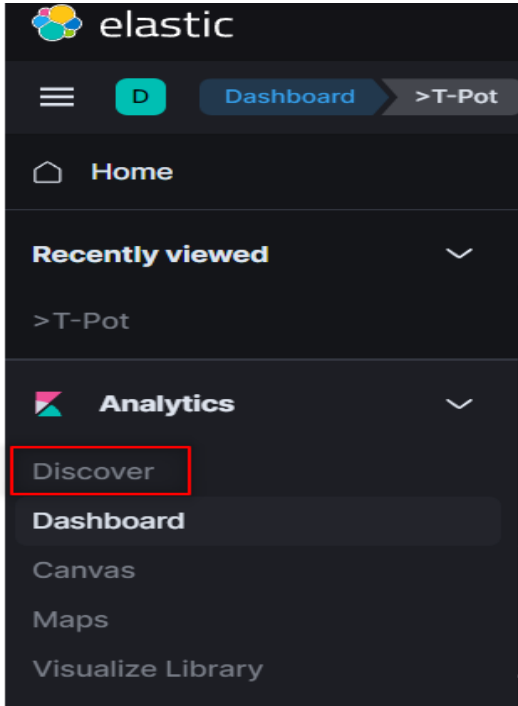


Yukarıda gösterdiği gibi karşımıza gelen seçeneklerden T-Pot seçerek Kibananın arayüzüne erişim sağlıyoruz.



Kibananın görsel arayüzü görselleştirilmiş bir şekilde şekildeki gibi karşımıza geliyor.

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



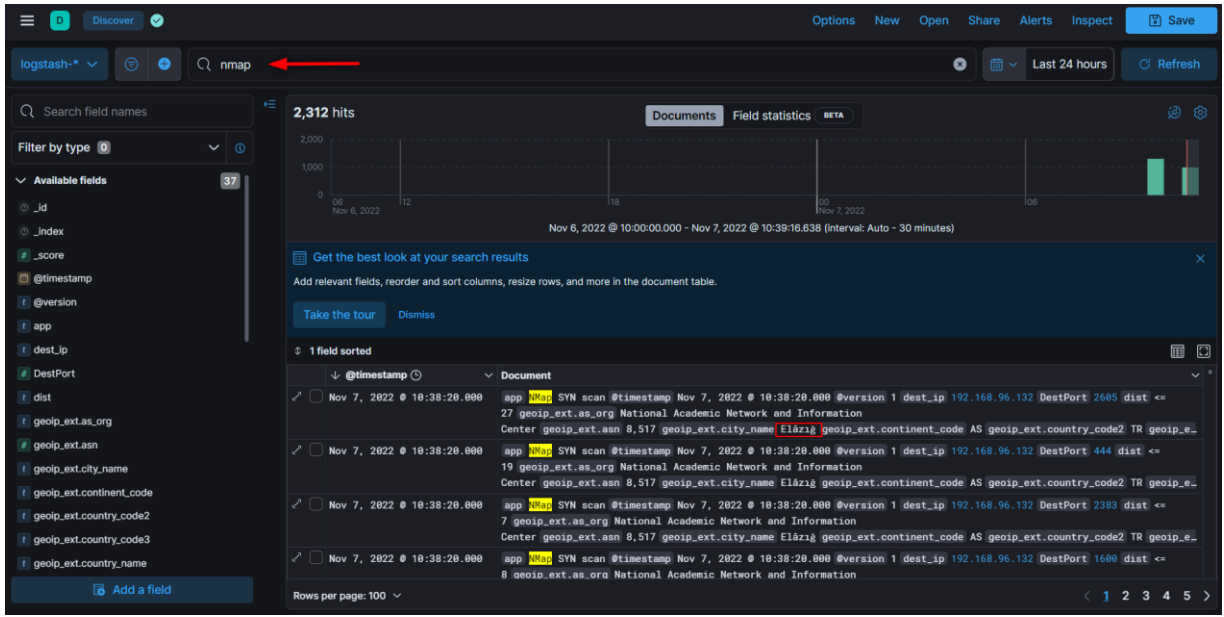
Daha sonra karşımıza açılan pencereden **Discover** seçeneğini seçerek işlemimize devam ediyoruz.

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

```
(root@yusuf)-[/home/kali]
# nmap 192.168.96.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 02:38 EST
```

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 inceleme yaparsak eğer aşağıda gösterildiği gibi saldırgan cihazın ip adresi gibi bilgilere de ulaşıyoruz.

```
},
"t-pot_ip_ext": [
  "193.255.125.93"
],
"src_ip": [
  "192.168.96.128"
],
"geoip_ext.country_code3.keyword": [
  "TR"
],

```

Copy to clipboard

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.

```
(root@yusuf)-[/home/kali]
# hydra -l yusuf -P /usr/share/wordlists/rockyou.txt ssh://192.168.96.132 -V -t30
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-07 02:44:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[ATTEMPT] target 192.168.96.132 - login "yusuf" - pass "soccer" - 29 of 14344399 [child 28] (0/0)
[ATTEMPT] target 192.168.96.132 - login "yusuf" - pass "anthony" - 30 of 14344399 [child 29] (0/0)
[22][ssh] host: 192.168.96.132 login: yusuf password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-07 02:44:33
```

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

```
(root@yusuf)-[/home/kali]
# ssh yusuf@192.168.96.132
The authenticity of host '192.168.96.132 (192.168.96.132)' can't be established.
ED25519 key fingerprint is SHA256:SRo3D3t2FLs5I5IlqXoH3ykaN8q7oLB/HyRSUY00rv0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.96.132' (ED25519) to the list of known hosts.
(yusuf@192.168.96.132) Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

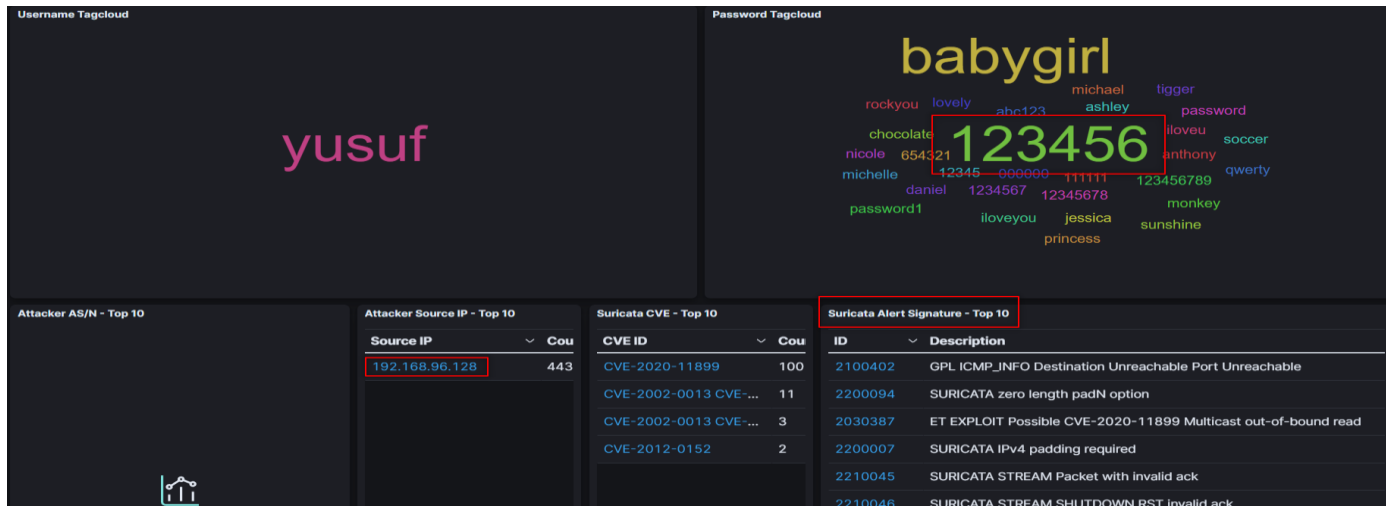
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
yusuf@ubuntu:~$
```


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

1 field sorted		
	@timestamp	Document
Nov 7, 2022 @ 10:46:02.682		event_type ssh @timestamp Nov 7, 2022 @ 10:46:02.682 @version 1 dest_ip 192.168.96.132 DestPort 22 flow_id 70,169,963,066,094 geoip_ext.as.org National Academic Network and Information...
Nov 7, 2022 @ 10:46:00.218		keyAlgs ssh-ed25519-cert-v01@openssh.com ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com sk-ssh-ed25519-cert-v01@openssh.com sk-ecdsa-sha2-nistp256-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ssh-ed25519...
Nov 7, 2022 @ 10:46:00.212		fatt_ssh.client SSH-2.0-OpenSSH_9.0p1 Debian-1+b1 fatt_ssh.cshka ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,sk-ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa...
Nov 7, 2022 @ 10:46:00.211		fatt_ssh.server SSH-2.0-OpenSSH_7.9p1 fatt_ssh.sshka ssh-rsa,ssh-dss,ecdsa-sha2-nistp256,ssh-ed25519 protocol ssh @timestamp Nov 7, 2022 @

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

Kibananın görselleştirilmiş arayüzüne geri döndüğümüzde ise aşağıdaki gibi bilgilerle karşılaşyoruz.



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