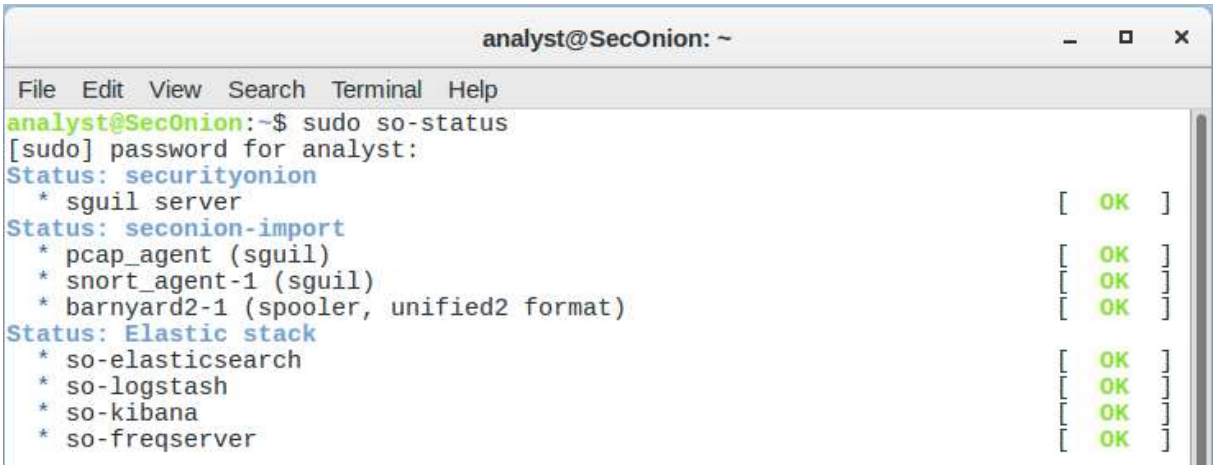
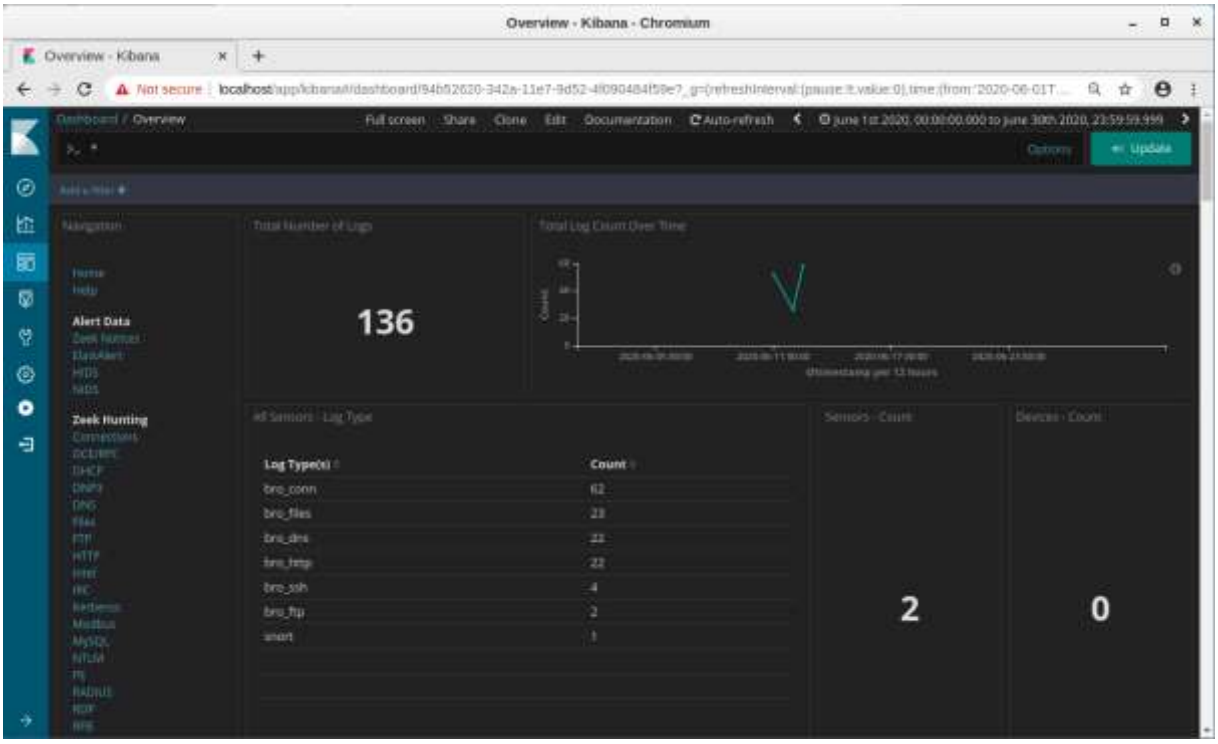
Mateusz Łapieś (mateusz.lapies@student.pk.edu.pl)

Sprawozdanie – lab1

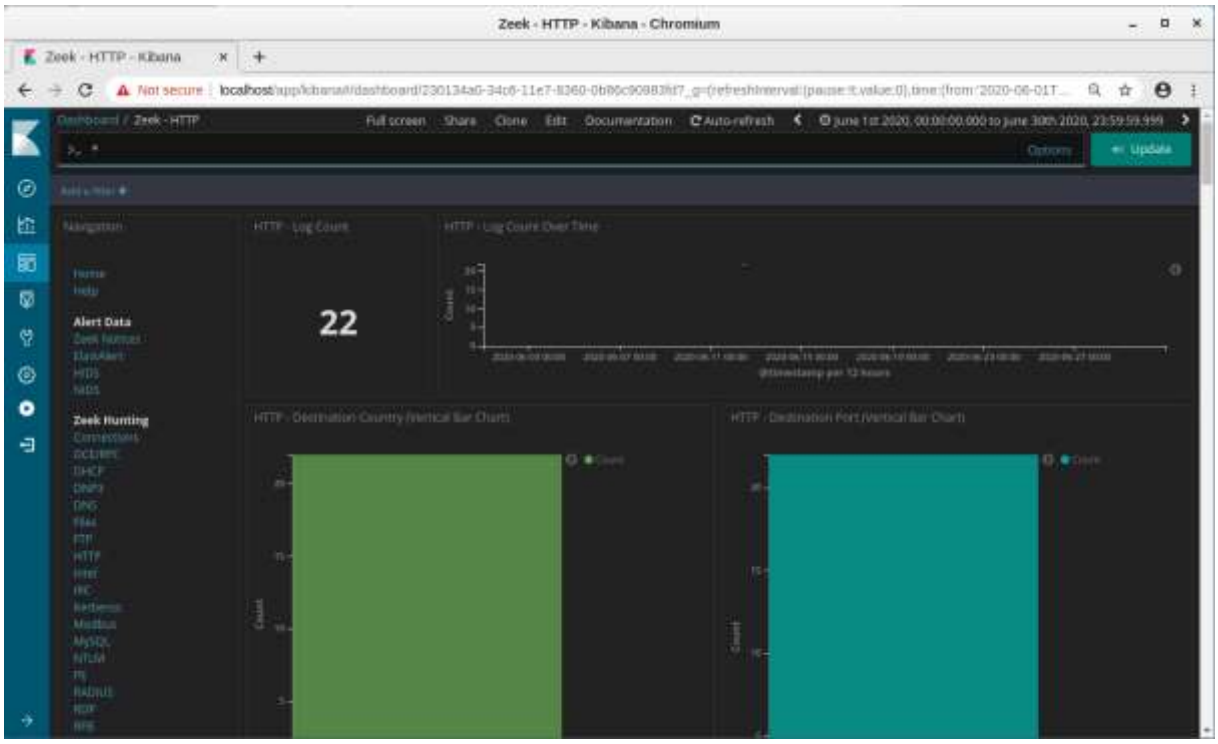
1. Start
    a. –
    b.



    c. –
    d. –
    e.



2. HTTP traffic
    a.



What is the source IP address?

209.165.200.227

What is the destination IP address?

209.165.200.235

What is the destination port numer?

22

b. –

c.

What is the timestamp of the first result?

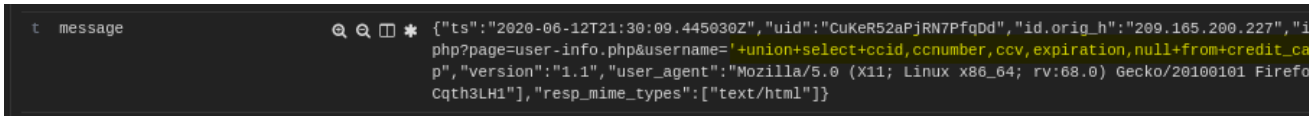
June 12th 2020, 21:30:09.445

What is the event type?

bro_http

What is included in the message field? These are details about the HTTP GET request that was made by the client to the server. Focus especially on the uri field in the message text.

Zawiera timestamp zapytania, uid, adres ip zapytania, port z którego przyszło zapytanie, adres ip odpowiedzi, port odpowiedzi, metoda zapytania, ip hosta, uri, które w tym przypadku zawiera również SQL Incection



What is the significance of this information?

Jest możliwość stwierdzenia, że doszło do ataku

d.

What do you see later in the transcript as regards usernames?

Liczba zawarta po tytule Username to cc id, numer cc, ccv, termin wygaśnięcia karty kredytowej z tabeli cedit_cards.

Give some examples of a username, password, and signature that was exfiltrated.

1234567812345678, 627, 2018-11-01

7725653200487633, 230, 2017-06-01

3. DNS
Client
192.168.0.11
Server
209.165.200.235

Were the subdomains from the DNS queries subdomains? If not, what is the text?

```
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

What does this result imply about these particular DNS requests? What is the larger significance?

Fragmenty poufnego dokumentu są przesyłane w postaci subdomen. Cały dokument mógł zostać w ten sposób przesłany, lub ich większa ilość.

What may have created these encoded DNS queries and why was DNS selected as the means to exfiltrate data?

Takie zapytania mogły zostać stworzone przez osobę mającą dostęp do sieci i poufnego pliku, która chciał wyprowadzić go poza lokalną sieć. Takie zapytania z reguły byłyby ignorowane, nie podlegały by podejrzeniom.