Cybersecurity

Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.

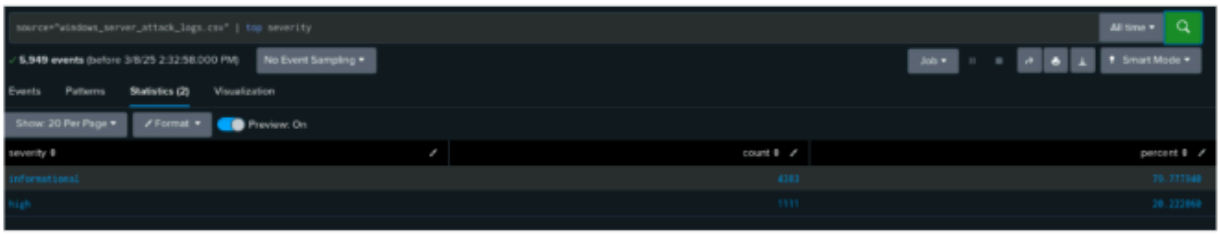
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Pre Attack

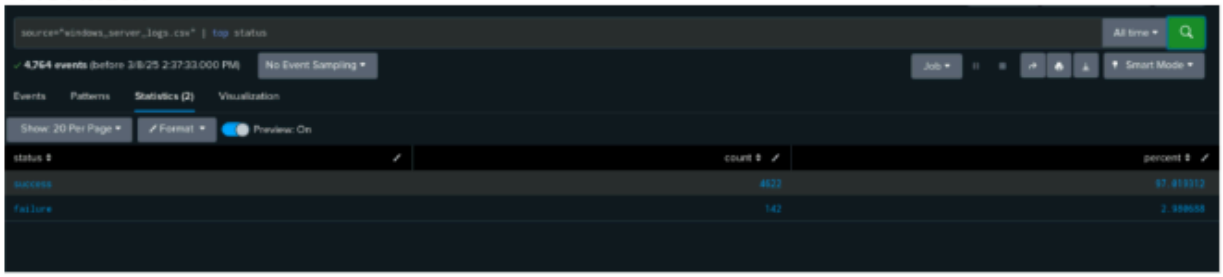
Post Attack



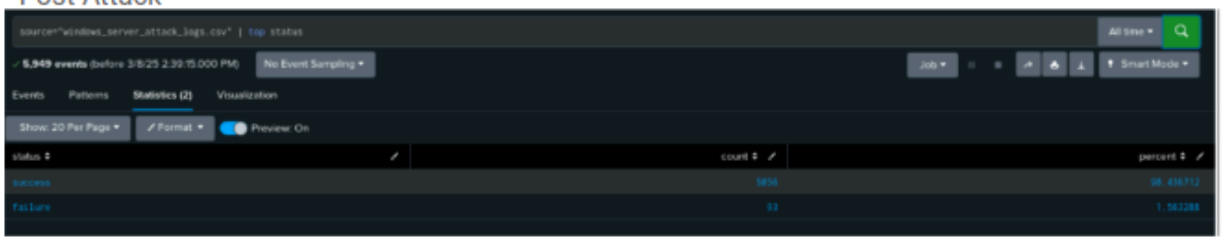
Yes, our report did detect changes in severity, the biggest being for high severity events. They increased from roughly 7% to 20.22% during the attack.

Report Analysis for Failed Activities

Pre Attack



Post Attack



- Did you detect any suspicious changes in failed activities?

```
Yes failed went from 142 to 93 and success went from 4622 to 5856
Yes, we did see changes in our report on the status of activities between
normal logs and the attack logs. From our analysis we can see that the
number of successful activities increased and the number of failed
activities decreased.
```

Alert Analysis for Failed Windows Activity

Pre Attack

Post Attack

- Did you detect a suspicious volume of failed activity?

```
Yes we detected suspicious volume of failed activity
```

- If so, what was the count of events in the hour(s) it occurred?

```
The count of suspicious volume of Failed activities was 35
```

- When did it occur?

```
March 25th at 8:00AM
```

- Would your alert be triggered for this activity?

```
Yes our Alert Threshold was set to 15 so the alert was successfully
triggered
```

- After reviewing, would you change your threshold from what you previously selected?

```
Reviewing the side by side screenshot, 15 still is an appropriate threshold
```

Alert Analysis for Successful Logins

Pre Attack

Post Attack

- Did you detect a suspicious volume of successful logins?

```
Yes there was a suspicious amount of activity on March 25th at 11:00AM and
at 12:00PM
```

- If so, what was the count of events in the hour(s) it occurred?

```
March 25th 11:00AM 196 events March 25th 12:00OM 77 Events
```

- Who is the primary user logging in?

```
User _J
```

- When did it occur?

```
March 25th 11:00AM 196 events March 25th 12:00OM 77 Events
```

- Would your alert be triggered for this activity?

```
Yes, Alert threshold was set to 30, so the alert threshold was sufficient
```

- After reviewing, would you change your threshold from what you previously selected?

```
No, the alert threshold set to 30 was sufficient to be triggered
```

Alert Analysis for Deleted Accounts

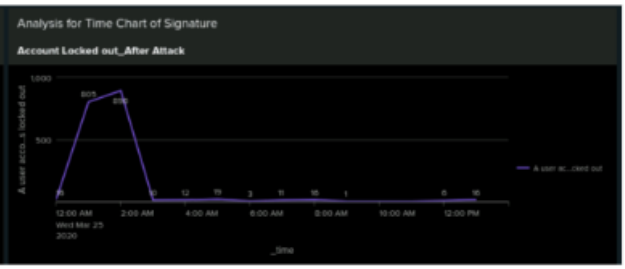
- Did you detect a suspicious volume of deleted accounts?

```
No suspicious activity
```

Dashboard Analysis for Time Chart of Signatures

Pre Attack

Post Attack



- Does anything stand out as suspicious?

```
Yes the time char signatures for the attack logs, some events stood out form
the windows activity logs
```

- What signatures stand out?

```
The two signatures that stood out were
   1. Attempts made to reset account password
   2. Account locked out
```

- What time did it begin and stop for each signature?

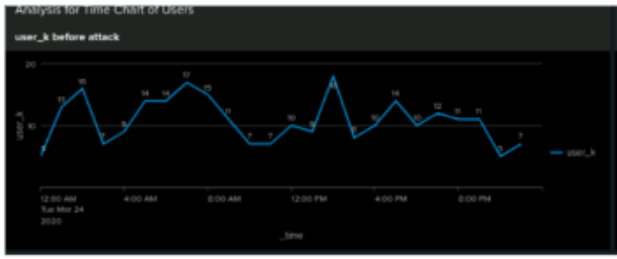
```
   1. Attempts made to reset account password: 9:00AM - 11:00AM
   2. Account locked out: 1:00AM - 3:00AM
```

- What is the peak count of the different signatures?

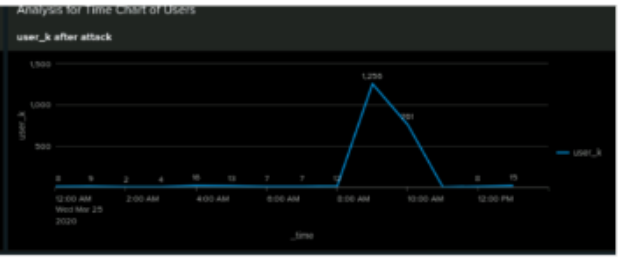
```
      Attempts made to reset account password: 1258
      Account locked out: 896
```

Dashboard Analysis for Users

Pre Attack



Post Attack



- Does anything stand out as suspicious?

```
Yes suspicious activity with two users
```

- Which users stand out?

```
User_k and User_a
```

- What time did it begin and stop for each user?

```
User_k: 9:00AM-11:00AM
User_a: 1:00AM-2:00AM
```

- What is the peak count of the different users?

```
User_k: 1256
User_a: 984
```

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Yes there is a significant increase in two signature types: An attempt was
made to reset an account password and A user account was locked out
```

- Do the results match your findings in your time chart for signatures?

```
Yes they do match
```

Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Yes, there is a noticeable increase in user_a and user_k activity
```

- Do the results match your findings in your time chart for users?

```
Yes the results match the time chart
```

Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

```
The advantage of using statistical time charts for signatures and users is
that they allow for a quick determination of event counts or user activity
per hour. However, a drawback compared to bar graphs and pie charts is that
changes in activity are not as immediately noticeable. Visualizations like
bar graphs highlight spikes and declines in events over time, while pie
```

```
charts provide a clear snapshot of which events or users have experienced increased activity
```

Apache Web Server Log Questions

Report Analysis for Methods

REPORT ANALYSIS FOR METHODS

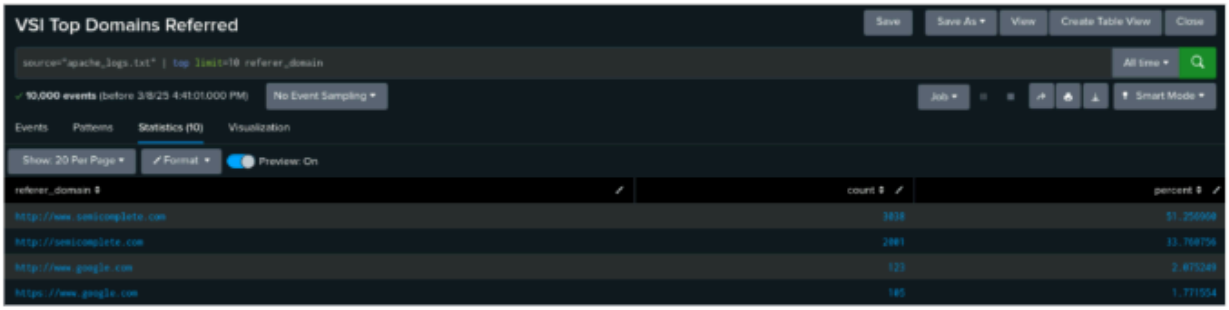
- Did you detect any suspicious changes in HTTP methods? If so, which one?

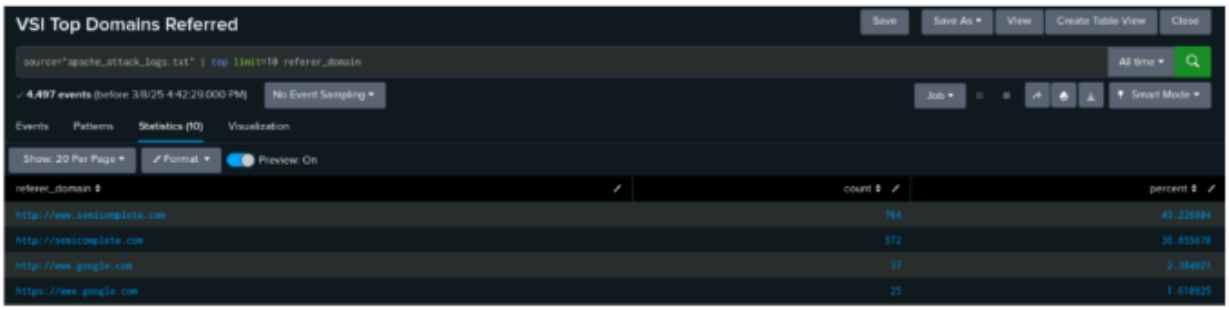
```
Yes we detected suspicious changes in the HTTP methods, notably POST
```

- What is that method used for?

```
POST: used to send data to the server from the HTTP client
```

Report Analysis for Referrer Domains

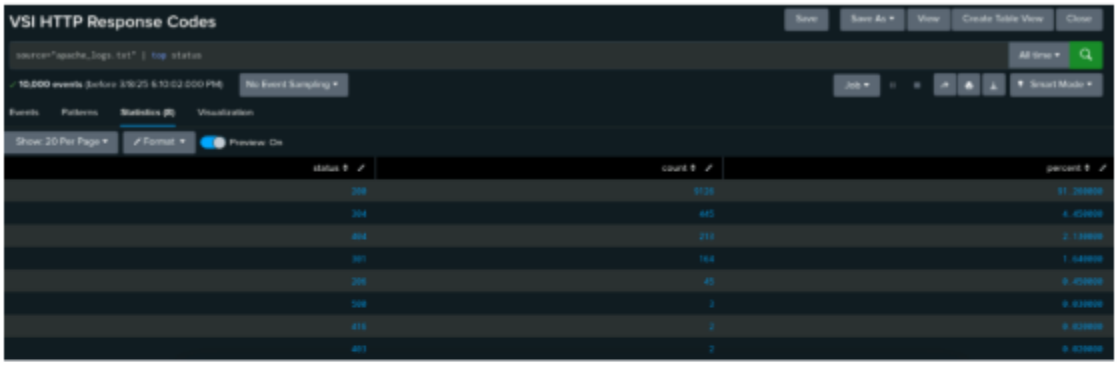




- Did you detect any suspicious changes in referrer domains?

```
Yes some suspicious activity did present itself in the top 10 referrer
domains.
```

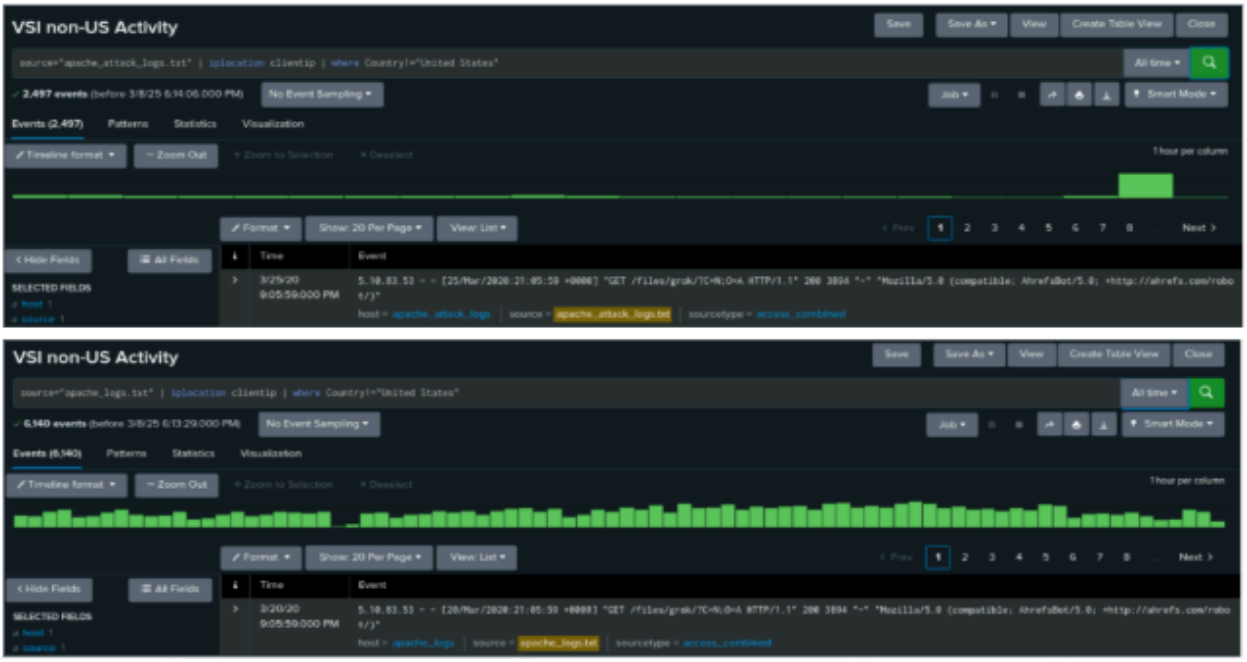
Report Analysis for HTTP Response Codes



- Did you detect any suspicious changes in HTTP response codes?

```
We did detect a suspicious change in HTTP response codes, specifically with response code 200 and 404. Response code 200 saw a decrease in amount and 404 saw an increase.
```

Alert Analysis for International Activity



- Did you detect a suspicious volume of international activity?

```
Yes we did detect a suspicious volume of international activity
```

- If so, what was the count of the hour(s) it occurred in?

```
939 at 08:00 PM
```

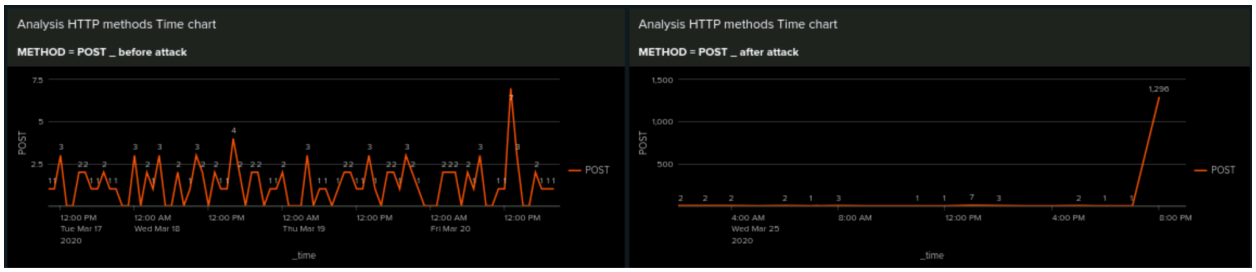
- Would your alert be triggered for this activity?

```
Yes threshold was set to 150 and hour
```

- After reviewing, would you change the threshold that you previously selected?

```
No the threshold of 150 was sufficient to set off the alert
```

Alert Analysis for HTTP POST Activity



- Did you detect any suspicious volume of HTTP POST activity?

```
Yes we detected suspicious volume of HTTP POST Activity
```

- If so, what was the count of the hour(s) it occurred in?

```
The count was 1296
```

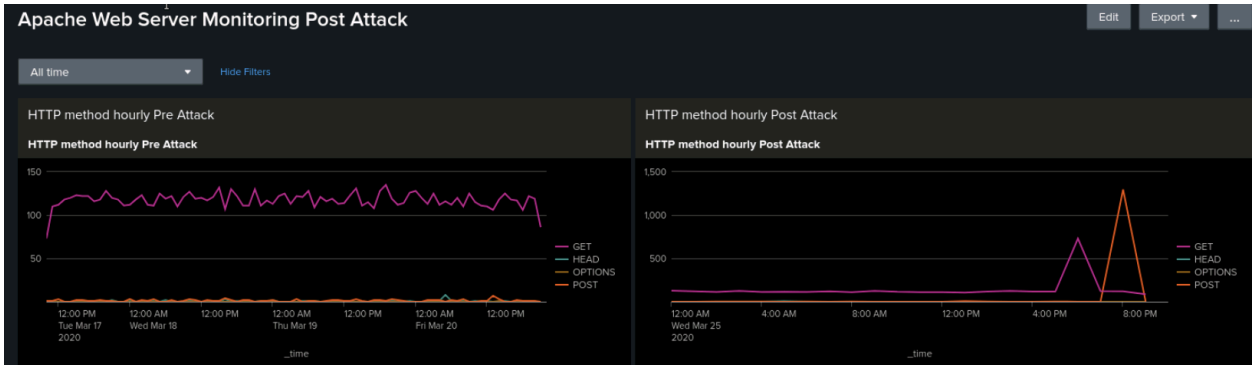
- When did it occur?

```
March 25th 8:00PM
```

- After reviewing, would you change the threshold that you previously selected?

```
The threshold of 15 was adequate for normal activity
```

Dashboard Analysis for Time Chart of HTTP Methods



- Does anything stand out as suspicious?

```
Yes there was a notable difference in the HTTP method time chart from the two logs
```

- Which method seems to be used in the attack?

```
POST
```

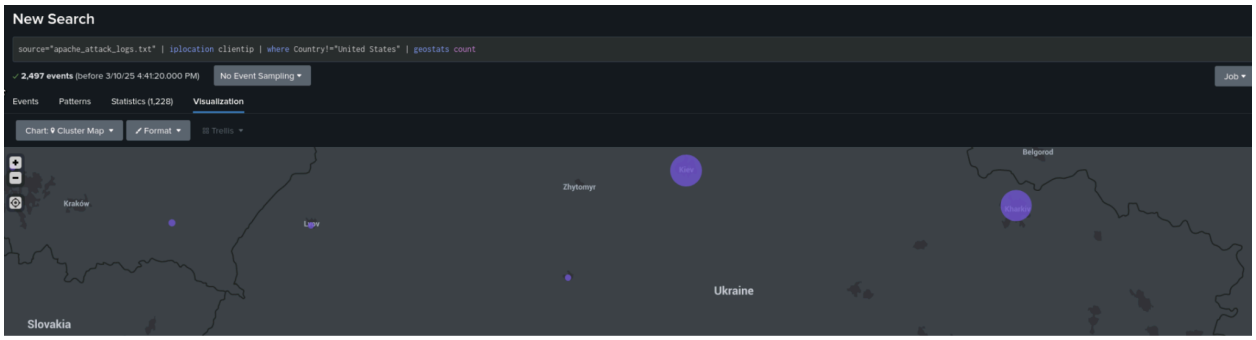
- At what times did the attack start and stop?

```
Attacks took place between 7:00PM and 9:00PM
```

- What is the peak count of the top method during the attack?

```
1296
```

Dashboard Analysis for Cluster Map



- Does anything stand out as suspicious?

```
Yes, high level of international logins from a specific area
```

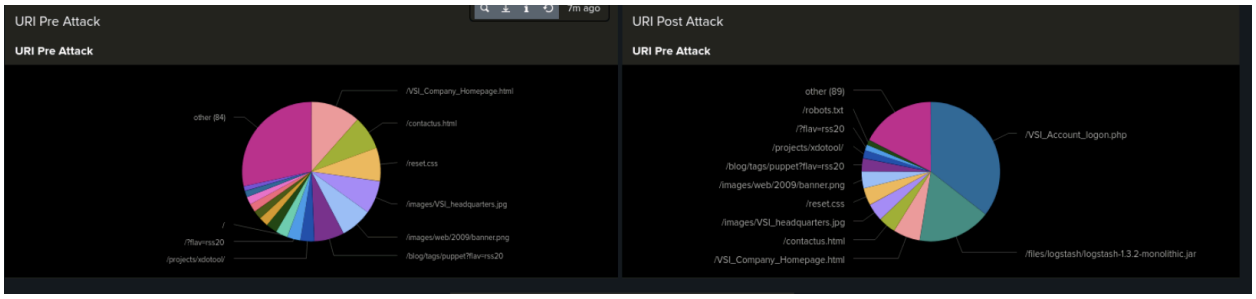
- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

```
Kiev Ukraine and Kharkiv Ukraine/Russia (depending on when you are reading this )
```

- What is the count of that city?

```
Kiev = 439
Kharkiv = 433
```

Dashboard Analysis for URI Data



- Does anything stand out as suspicious?

```
Yes the URI Chart does show suspicious activity
```

- What URI is hit the most?

```
VSI_Account _logon.php
```

- Based on the URI being accessed, what could the attacker potentially be doing?

```
Based on the URI attackers are likely using a Bruntforce attack
```

Presentation:
https://docs.google.com/presentation/d/1dzwNEUBLfUS3sNaJXcE0a6pWYD_dl-dI3dVyYGVa348/edit?usp=sharing