Cybersecurity

Project 3 Review Questions

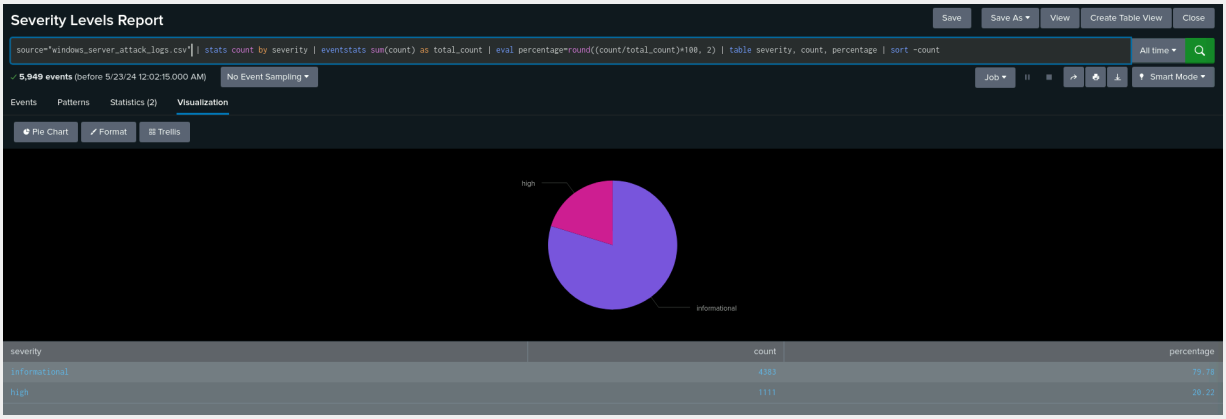
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, the ratio of severity went from informational severity of 4435/93.09% to 4383/79.78%, and high severity of 329/6.91% to 1111/20.22%.



Report Analysis for Failed Activities

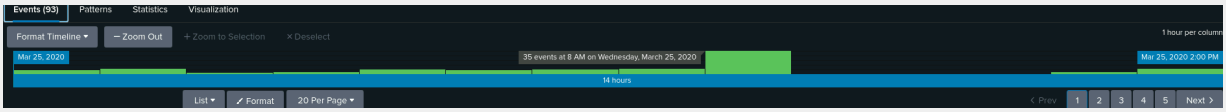
- Did you detect any suspicious changes in failed activities?

```
Yes, the ratio of failed activities to successful activities went from
142/4622 failure/success (2.98%/97.02%) to 93/5856 failure/success
(1.56%/98.44%).
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, there were 35 events logged at 8:00AM.
```



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

```
The count of events in the 8:00AM hour was 35.
```

- When did it occur?

```
It occurred at 8:00AM.
```

- Would your alert be triggered for this activity?

```
Yes, it would have been triggered due to it being over 11 events in a one
hour period.
```

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

```
No, the threshold of 11 events triggering an alert was appropriate.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes
```

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

```
At 11 AM on Wednesday, March 25, 2020 there were 196 successful logins,
followed by 77 successful logins at 12 AM
```

- Who is the primary user logging in?

```
User_j was responsible for the vast majority of logins during this time
period.
```

- When did it occur?

```
11:00 AM to 1:00 PM
```

- Would your alert be triggered for this activity?

```
Yes, the threshold for the alert to be triggered was >22 successful logins
in one hour.
```

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

```
No, the threshold of 22 events triggering an alert was appropriate.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

No, we did not detect a suspicious volume of deleted accounts. The alert threshold was set for 22 deletions or higher, and the average volume was not out of the norm based on our established baseline.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, on March 25, 2020, at 1:00AM, “A user account was locked out” spiked to 805 events, and at 2:00AM, that number spiked to 896. Additionally, at 9:00AM, “An attempt was made to reset an accounts password” spiked to 1258 events. At 11:00AM, “An account was successfully logged on” spiked to 196 events which occurred after the previously mentioned suspicious activity.

- What signatures stand out?

The signatures that stand out are the following:
“A user account was locked out,”
“An attempt was made to reset an accounts password,” and
“An account was successfully logged on.”

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

“A user account was locked out” began at 12:00AM and ended at 3:00AM.
“An attempt was made to reset an accounts password” began at 8:00AM and ended at 11:00AM.
“An account was successfully logged on” began at 10:00AM and ended at 1:00PM.

- What is the peak count of the different signatures?

“A user account was locked out” peaked at 896 events at 2:00AM.
“An attempt was made to reset an accounts password” peaked at 1258 events at 9:00AM.
“An account was successfully logged on” peaked at 196 events at 11:00AM.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, 3 different users had significant spikes in activity
```

- Which users stand out?

```
The users that stand out are users A, K and J.
```

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

```
User A spike started at 12:00AM and ended at 3:00AM.
User K spike started at 8:00AM and ended at 11:00AM.
User J spike started at 10:00AM and ended at 1:00PM.
```

- What is the peak count of the different users?

```
User A peaked at 984
User K peaked at 1,256
User J peaked at 196
```

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

- Does anything stand out as suspicious?

```
Yes, there was a large spike in three categories being “An attempt was made
to reset an accounts password,” “A user account was locked out,” and “An
account was successfully logged on.”
```

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

```
Yes, the results match our findings in our time chart for signatures.
```

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

- Does anything stand out as suspicious?

```
Yes, User K and User A both had a significantly greater amount of activity compared with other users, with User J also having a greater amount of activity, although to a lesser extent.
```

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

```
Yes, this matches the significant spikes in activity for Users K, A, and J
```

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?

```
Utilizing a bar chart, the advantages were that you can see which users had the most activity over a 24 hour period, but the disadvantage would be that we don't see their activity over an hourly period which can show which suspicious activities it correlated with.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, there was a significant increase in the number of POST requests. Under normal conditions, POST requests were just 1% of the total events captured from the four methods (GET, HEAD, OPTIONS, POST). During the attack, POST methods rose to 29.4% of the total events captured.
```

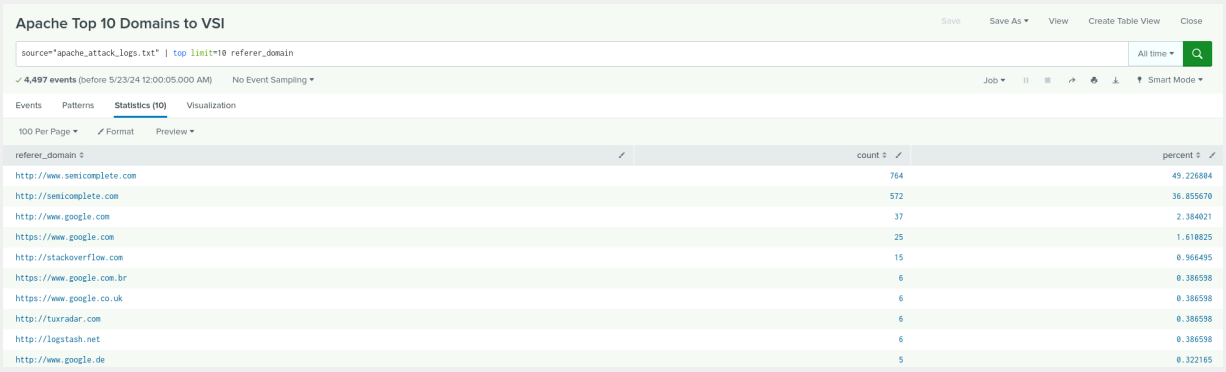
- What is that method used for?

```
The POST method requests that a web server accept data enclosed in the body of a message, usually for storage.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

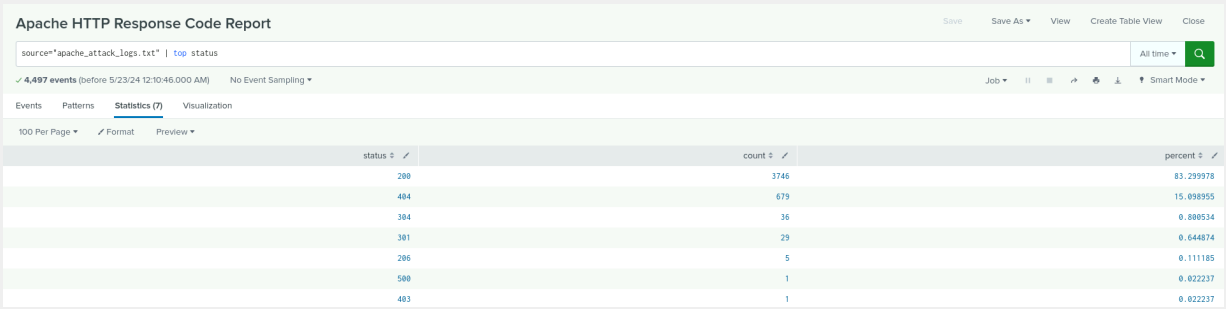
No, there were no suspicious changes in referrer domains. Any new domains in the top 10 were also not suspicious.



Report Analysis for HTTP Response Codes

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

There was a noticeable increase in 404 response codes. The percentage increased from 2% before the attack to 15% durings the attack. This caused a decrease in 200 (OK) response codes (91% to 83%). Less clients are getting successful HTTP requests.



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

No, the number of events per hour during the attack was less than the baseline established for China by the apache_logs.txt events.

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

N/A

- Would your alert be triggered for this activity?

No, an alert would not have been triggered. The alert was designed with a threshold of greater than 40 events to account for normal activity for IP addresses from China.

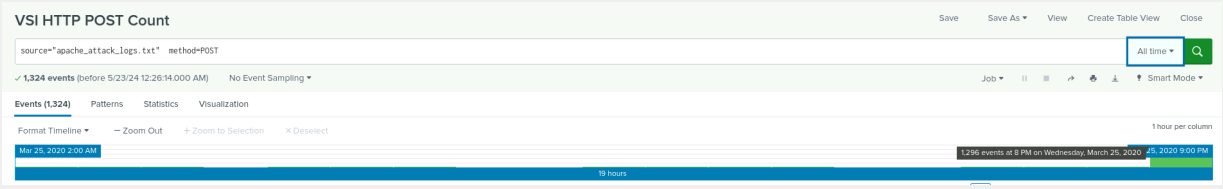
- After reviewing, would you change the threshold that you previously selected?

After reviewing, we would not change the threshold selected. We would however set a second alert for IP addresses in Ukraine or adjust this international alert to include both China and Ukraine. Adjusting this alert would require establishing a new baseline and threshold given the addition of Ukraine.

Alert Analysis for HTTP POST Activity

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

There was a suspicious increase in the HTTP POST activities.



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

1,296 at 8PM.

- When did it occur?

Wednesday at 8PM on March 25th, 2020.

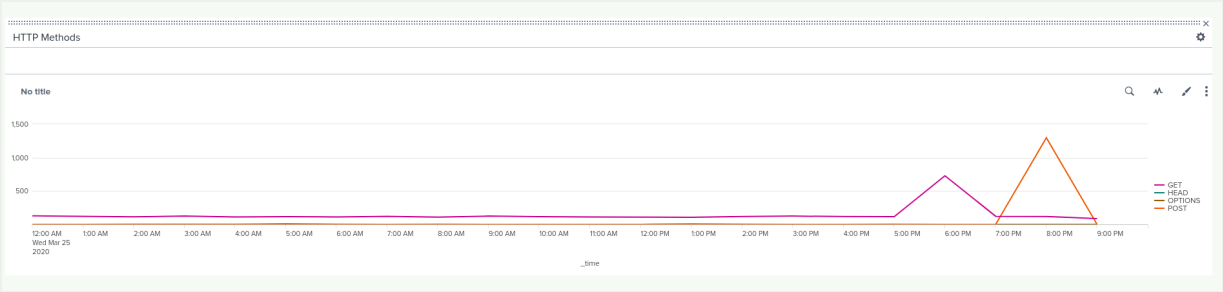
- After reviewing, would you change the threshold that you previously selected?

No, since there is at most 1 event occurring at a time besides this abnormality. Generally if there is a significant increase in events the threshold we selected should be a good indicator of suspicious activity happening.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, there was a spike in GET HTTP requests at 6:00 PM on March 25, 2020, (up from 117 events at 5:00 PM to 729 at 6:00 PM) followed by a spike in POST events at 8:00 PM (up from 1 event at 7:00 PM to 1,296 at 8:00 PM).



- Which method seems to be used in the attack?

Both the GET and POST HTTP methods seem to have been used in the attack

- At what times did the attack start and stop?

The attack started at 5:00 PM on March 25th when the number of GET requests began to climb. The attack continued with the POST method until 9:00 PM.

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

1296

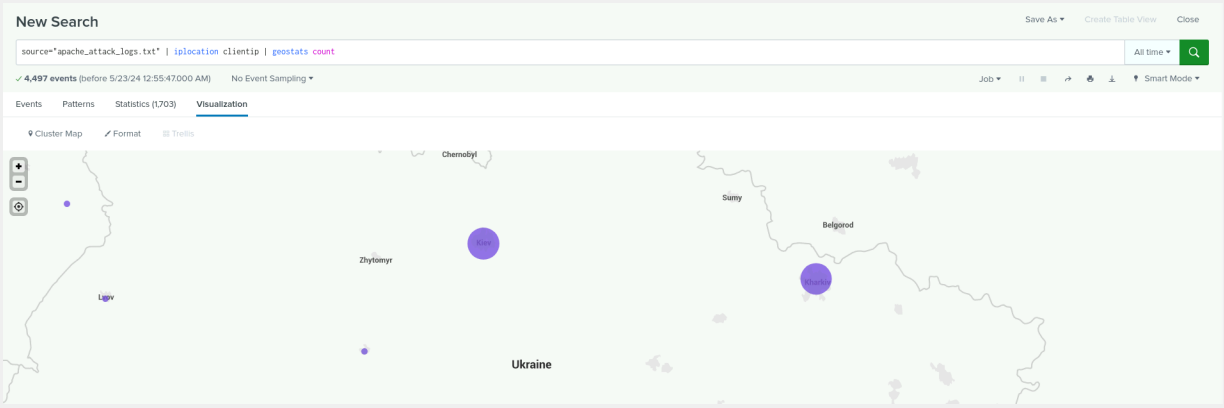
Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Ukraine had an increase in activity in 2 major cities being Kiev and
Kharkiv.
```

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

```
In Ukraine, the cities Kiev and Kharkiv had a large increase in activity.
```

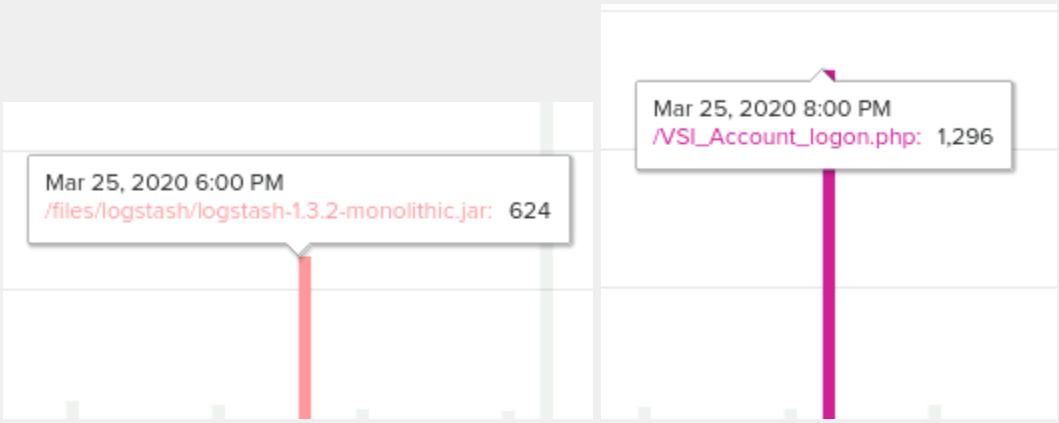


- What is the count of that city?

```
Kiev - 440, Kharkiv - 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

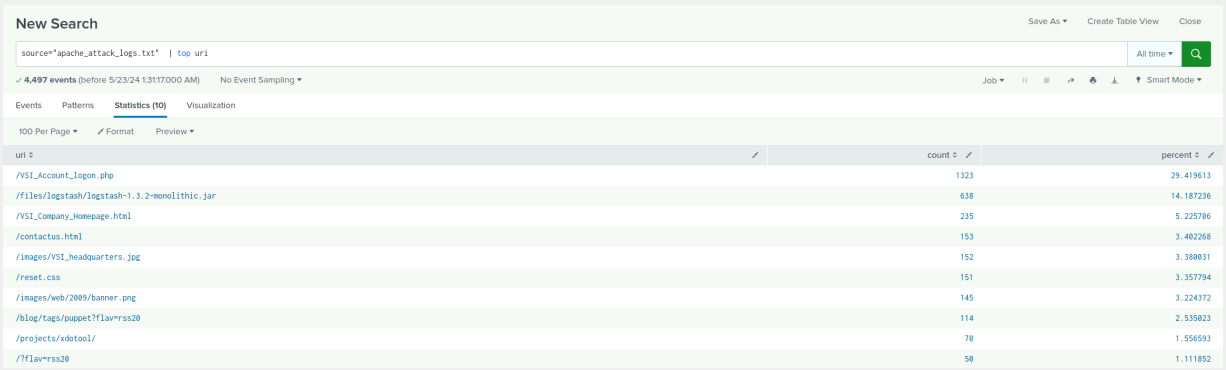



```
source="apache_attack_logs.txt"  | timechart span=1h count by uri
```

The URI /files/logstash/logstash-1.3.2-monolithic.jar had suspicious activity at 6PM on Wednesday, March 25th

The URI /VSI_Account_logon.php had suspicious activity at 8PM on Wednesday, March 25th

- What URI is hit the most?



/VSI_Account_logon.php was hit the most with a count of 1323 events. The number of events that occurred during the attack was 1296 as shown in the previous question.

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

The attacker could be attempting to gain initial access to our web server by brute forcing their way in from the logon.php page. Or based on the increase in POST requests, the attacker may be using automated tools to test and exploit SQL injection vulnerabilities.

Logstash is a free and open-source data processing pipeline tool designed to collect data from various sources, like a web server, transform and process it, and then send it to a destination for further analysis or storage. The attacker may have used Logstash's data processing capabilities in an attempt to exfiltrate web server data, maintain persistence, or set up command and control channels all while blending in with legitimate server operations.