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, there was an increase in ‘high’ severity events from 6.9% to 20.2% and
a decrease in ‘informational’ events dropped from 93.1% to 79.8%
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
While the increase in failed activities was minimal, at approximately 1%,
the distribution and volume of successful activities were notably
suspicious. Specifically, the baseline for successful activities was around
200 per hour, but on the day of the attack, there was a surge up to 1674
successful events within just two hours. This deviation from the norm is
highly suspicious and could indicate a potential breach.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, at one of the hours there was a huge spike to 35 events.
```

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

```
Peaked at 35 events.
```

- When did it occur?

```
It occurred 8am-9am on Wednesday, 25th March, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, my alert would have been triggered, as the activity exceeded the set
threshold of 7 events, suggesting a potential attack.
```

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

```
In our observations, alongside the peak of 35 events, there were several
hours with 8 events for which alerts will be generated. So, most of these
could be false positives. However, there is a chance that some of them are
real attacks with a low failed activity rate. Therefore, if too many alerts
are being generated, I would suggest increasing the threshold to 9 to reduce
the number of false positive alerts, as the likelihood of a potential attack
with 9 events per hour is extremely slim.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, there were several hours exceeding the threshold of 18 events.
```

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

```
Significant spikes observed at four different hours were 25, 92, 70 and 54
events.
```

- Who is the primary user logging in?

```
The most active users during these times was ‘user_k’ with 126 successful logins, closely followed by ‘user_a’ with 110 logins.
```

- When did it occur?

```
In the significant spikes observed:
   ● First  spike occurred during 1-3am (25+92=117 events), and
   ● Second spike occurred during 9-11am (70+54=124 events)
on Wednesday, 25th March, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, my alert threshold was set 18 so, it would even be triggered for the whole duration of the attack.
```

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

```
I would increase the threshold to 20, as 18 seems a bit low and could potentially generate false positives, especially after observing the large numbers from the attack logs. Initially, the attack started with 25 events and peaked at 92 events in an hour.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
The observations in the Deleted Accounts alert are similar to the successful logins. Once again, there was a significant increase above the threshold in the deletion of user accounts at the same timings.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, there were multiple spikes of different signatures occurring during the
times of the attack.
```

- What signatures stand out?

```
The signatures that stand out:
   ● A user account was locked out,
   ● An attempt was made to reset an account's password, and
   ● An account was successfully logged on.
```

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

```
On Wednesday, 25th March, 2020:
   ● A user account was locked out - began at 12am and stopped at 3am,
   ● An attempt was made to reset an account's password - began at 8am and
     stopped at 11am, and
   ● An account was successfully logged on - began at 10am and stopped at
     1pm.
```

- What is the peak count of the different signatures?

```
Peak counts for different signatures:
   ● ‘A user account was locked out’ - 896 events,
   ● ‘An attempt was made to reset an account's password’ - 1258 events,
     and
   ● ‘An account was successfully logged on’- 196 events.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, there were multiple spikes of different users occurring during the
times of the attack.
```

- Which users stand out?

```
The signatures that stand out:
```

```
   - User_k,
   - User_a, and
   - User_j.
```

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

```
On Wednesday, 25th March, 2020.
   - User_k - began at 8am and stopped at 11am,
   - User_a - began at 12am and stopped at 3am, and
   - User_j - began at 10am and stopped at 1pm.
```

- What is the peak count of the different users?

```
Peak counts for different users:
   - User_k - 1256 events,
   - User_a - 984 events, and
   - User_j - 196 events.
```

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

- Does anything stand out as suspicious?

```
Yes, three signatures appear suspicious due to their elevated presence in
bar graphs and line graphs: 'user was locked out,' 'account successfully
logged on,' and 'attempt made to reset account password.'
```

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

```
Yes, they match with my findings.
```

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

- Does anything stand out as suspicious?

```
Yes, three users, user_k, user_a and user_j, appear suspicious due to their
disproportionately high counts (above baseline and threshold) and
significant presence in the pie chart.
```

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

```
Yes, they match with my findings.
```

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?

```
Advantages:
   ● Comprehensive Overview: Statistical charts give a full picture of what
     users are doing, helping you understand the data better.
   ● Spotting Unusual Patterns: They make it easy to see anything out of
     the ordinary, as these points will look different from the usual data
     pattern.
   ● Better Comparisons: They offer detailed ways to compare how users
     behave, showing things like averages and distributions that you don't
     get from other charts.
Disadvantages:
   ● Hard to Understand: If you're not used to statistical terms and ideas,
     these charts can be tough to figure out.
   ● No Time Information: They don't show how things change over.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, there is a notable shift in HTTP methods. The frequency of GET requests
has significantly decreased, while the number of POST requests have surged
dramatically following the attack.
```

- What is that method used for?

```
GET is an HTTP request method used to retrieve data from a specified resource. It retrieves information from the server and has no other side effects. POST, on the other hand, is an HTTP request method used to send data to a server for the purpose of creating or altering a resource. Moreover, the increase in POST requests can even mean the input of credentials many times in logins to gain access.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Nothing much. Some minimal changes in terms of percentages of different domains in the top 10. There are newer domains in the top 10 - can’t assume they are attackers domains. However, the counts for certain previously prominent referrers have noticeably declined. These shifts indicate a change in traffic source or type, potentially linked to the attack.
```

Report Analysis for HTTP Response Codes

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

```
Yes, there are notable anomalies in HTTP response codes. The frequency of 200 (OK) responses has notably dropped, whereas the occurrences of 404 (Not Found) responses have surged post-attack. This pattern implies that the attacker may have been probing for non-existent resources on the server, potentially entering incorrect credentials.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there is a clear spike in international traffic, predominantly to Ukraine.
```

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

```
The spike occurred for only one hour, 8pm-9pm on Wednesday, the 25th March, 2020.
```

- Would your alert be triggered for this activity?

```
The threshold set for inbound traffic from outside of the US was initially set at 100. As the spike exceeded this threshold, the alert would have been triggered.
```

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

```
After reviewing the International Activity, I have decided to slightly adjust the threshold and increase it by 10 events. The small increase to 110 would more effectively avoid creating alerts for minor increases in international activity while still protecting from major attack spikes. This decision was mainly influenced by noticing one event with 107 occurrences, which was not linked to the attack.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, there is a suspicious volume of HTTP POST activity. The count of HTTP POST requests are significantly higher than any other hour.
```

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

```
It was only one hour with a peak of 1296. Which is significantly higher than the threshold set.
```

- When did it occur?

```
The time of the spike was 8pm on Wednesday the 25th March, 2020.
```

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

```
The threshold that was set for POST requests was 4 events per hour, and I believe that is sufficient, as I noticed no hour other than the attack hour
```

```
had more than 3 events. However, I would suggest increasing it to 5 because most of the hours' events are close to the threshold.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
The dashboard showed a small spike in GET requests and a large spike in POST requests.
```

- Which method seems to be used in the attack?

```
HTTP POST would seem to be used in the attack, as there is an increase from our visual data.
```

- At what times did the attack start and stop?

```
The start of the POST request spike is at 7pm and ends at 9pm, on Wednesday the 25th March, 2020.
```

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

```
The peak count of the top method: POST was 1296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, there is a high volume of activity coming from Ukraine,
which stands out as suspicious.
```

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

```
Kharkiv, Ukraine on the map has a high volume of activity.
```

- What is the count of that city?

```
432 is the count of that city.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, the URI ‘VSI_Account_logon.php’ with 1323 events and
‘files/logstash/logstash-1.3.2-monolithic.jar’ with 638 events stand out.
```

- What URI is hit the most?

```
The URI that is hit the most is ‘VSI_Account_logon.php’.
```

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

```
The ‘VSI_Account_logon.php’ URI suggests that the attacker is attempting to
log in to an account. This could indicate a brute force attack where the
attacker is trying to guess the password of an account. The high number of
POST requests supports this, as POST is typically used to send data (like a
password) to a server. The http status code also adds on as 404 can be
triggered by the failed login attempts by the brute force attack.
```