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?

```
For high severity, we detected a jump from 7% to 20%.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
The original failed activities were about 3 percent. The attack logs states
that failed activities is now about 1.5 percent
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

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

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

```
It was a count of 70 events at 8:00AM.
```

- When did it occur?

```
It occurred on March 25, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, our alert would be triggered for the spike of failed events.
```

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

```
No, our threshold of 20 was a good threshold. The average of failed activity
was a count of 16.
```

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?

```
Ranged from 784 to 1293
```

- Who is the primary user logging in?

```
User_k
```

- When did it occur?

```
From 1 AM to 2 AM and 9 AM to 10 AM on March 25th, 2020
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
Yes, should increase the threshold to 400 successful attempts
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes we detected two spikes of deleted accounts at 2:00AM and at 9:00AM
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Two major data spikes
```

- What signatures stand out?

```
“A user account was locked out” and “An attempt was made to reset an accounts password”
```

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

```
“User account locked out” was around 12 AM to 3 AM and “An attempt was made to reset an account’s password” was around 8 AM to 11 AM
```

- What is the peak count of the different signatures?

```
“User account locked out” peaked at 896, and “An attempt was made to reset an account’s password” peaked at 1258.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Both charts from “signature” and “user” fields are matching
```

- Which users stand out?

```
Users “a” and “k”
```

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

```
“User A” was around 12 AM to 3 AM and “User K” was around 8 AM to 11 AM
```

- What is the peak count of the different users?

```
“User A” peaked at 984, and “User K” peaked at 1256.
```

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

- Does anything stand out as suspicious?

```
“A user account was locked out” and “An attempt was made to reset an
accounts password” take up the majority of data
```

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

```
Yes
```

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

- Does anything stand out as suspicious?

```
Users “A” and “K” take up the majority of data
```

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

```
Yes
```

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: Shows potential attacks from select fields and users.

Disadvantages: There are a lot of fields, and it could be harder to read if there is more attack data to be filled into the charts.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes. There were two significant changes in request methods. GET requests decreased by about 28.3% and POST requests increased by about 28.3%
```

- What is that method used for?

```
GET is used to request information from the source and POST is used to send or update information to a web server
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
There seemed to be no signs of suspicious changes regarding the referrer domains
```

Report Analysis for HTTP Response Codes

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

```
There was a decrease in 200 response codes by about 8% and an increase in 404 response codes by about 13%. The increase in 404 errors is slight but can still be seen as suspicious
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there was a suspicious volume of activity in Ukraine at 8:00 p.m. on March 25th.
```

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

```
Ukraine had a count of 1,369 events during the 8:00 p.m. attack.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would be triggered as it falls within the threshold.
```

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

```
No change in the threshold is necessary.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, there was a suspicious increase in HTTP POST activities.
```

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

```
There was a count of 1,296 events at 8:00 p.m.
```

- When did it occur?

```
The event occurred at 8:00 p.m. on Wednesday, March 25th.
```

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

```
No change in the threshold is necessary.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There is a suspicious increase in activity for both GET and POST requests.
GET requests had an increase surge from 5 pm to 7pm while POST requests had
their increase from 7pm to 9pm. Both surges occurred on Wednesday March 25th
```

- Which method seems to be used in the attack?

```
Both the GET and the POST method seemed to have been used in the attack
```

- At what times did the attack start and stop?

```
The GET attack started at 5pm and stopped at 7pm on Wednesday March 25.

The POST attack started at 7pm and stopped at 9pm on Wednesday March 25.
```

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

```
Peak count for GET Requests: 729
Peak count for POST Requests: 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
There was a significant increase in activity in Ukraine. The cities of Kiev
and Kharkiv showed the most signs of activity
```

- 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 have high volumes of activity
```

- What is the count of that city?

```
Count for Kiev: 440
Count for Kharkiv: 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
[EThere was a significant and suspicious increase in activity for
/VSI_Account_logon.php as well as
/files/logstash/logstash-1.3.2-monolithic.jar
```

- What URI is hit the most?

```
/VSI_Account_logon.php was hit the most with a count of 1323
```

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

```
It seems the attacker is trying to access the logon page via a brute force
attack
```