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?

The percentage for “high” severity went from 6.905% to 20.222%. The percentage for “informational” severity went from 93.094% to 79.777%

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

There was an increase in “success” events (4622 to 5856) (97.01% to 98.43%) as well as a decrease in “failure” events (142 to 93) (2.98 to 1.56)

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

There was a drop in usual “failed” activity according to the attack logs. Then, there was a sharp increase of “failed” activity around 8 AM followed by 0 failed activity for the next 3 hours.

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

From 12 AM, March 2020, there was an unusual decrease in “failed” activity (6 events) until 8 AM which showed a sharp increase (35). From 9 AM to 11 AM there was 0 “failed” activity, which is a deviation from the “windows_logs” (not the “attack” logs)

- When did it occur?

12 AM (6 events), 8 AM (35 events), 9 AM to 11 AM (0 events)

- Would your alert be triggered for this activity?

For the decrease around 12 AM no but the alert would have triggered at 8 AM, capturing the highly unusual activity.

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

No.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, there was a sudden dropoff at 9 AM, March 25. From there, there was 0 activity for 2 hours. This type of dropoff is not seen in the “windows_server” logs. Also, user_a had a spike in successful logins at 2 AM, March 25.

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

9 AM (4 events), 10 AM - 11 AM (0 events), user_a (11 events @ 2 AM)

- Who is the primary user logging in?

user_a

- When did it occur?

2 AM, March 25

- Would your alert be triggered for this activity?

No, our threshold was set at 30+ successful login attempts.

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

No, as setting the threshold any lower to what it is currently set at would increase the likelihood of false positives.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes, there was a drop in the volume of deleted accounts ranging from 9 AM to 11 AM. The “windows_server” logs do not show any such dropoff but rather shows a fairly consistent volume throughout the given time range.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, there is a total decrease in all signatures except for the “An attempt was made to reset an accounts password” signature as well as the “A user account was locked out” signature.

- What signatures stand out?

The “An attempt was made to reset an accounts password” signature as well as the “A user account was locked out” signature.

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

```
8-11 AM for the “An attempt was made to reset an accounts password”
signature as well as the 12-3 AM for the “A user account was locked out”
signature.
```

- What is the peak count of the different signatures?

```
“A user account was locked out” signature - 896
“An attempt was made to reset an accounts password” signature -1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, user_a had a sudden increase as well as user_k. There was a minor drop
in all other user activity.
```

- Which users stand out?

```
User_a and user_k
```

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

```
User_a - 12-3 AM
User_k - 8-11 AM
```

- What is the peak count of the different users?

```
User_a - 984
User_k - 1256
```

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

- Does anything stand out as suspicious?

Yes, there was a significant increase in signatures for the “An attempt was made to reset an accounts password” signature as well as the “A user account was locked out” signature.

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

While I had used a bar chart and a line chart, the results in both matches.

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

- Does anything stand out as suspicious?

Yes, user_a had a sudden increase as well as user_k. There was a minor drop in all other user activity.

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

While I had used a pie chart and a line graph, the results for both match.

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 pie chart is beneficial in representing the shares of each user’s activity of the total user activity. The disadvantage of the pie chart is that it does not represent changes over time. The line chart is beneficial in showing the increase and decrease of user activity over time. The disadvantage to the line chart is that it does not clearly show the shares of each user’s activity within the total share of all user activity.

Apache Web Server Log Questions

Report Analysis for Methods

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

There was a downtick in the GET method (9851 to 3175) and an uptick in the POST method (186 to 1324)

- What is that method used for?

The GET method is used to retrieve data from a server. The POST method is used for creating resources, modifying data, and submitting forms.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There was an increase in all referrer domains.

Report Analysis for HTTP Response Codes

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

There was a significant drop in the count of status code 200 (9126 to 3746), and an increase in the counts of status codes 304 (36 to 213) and 301 (29 to 164).

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

There was an abnormal uptick in activity at 8PM.

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

The count was 937 at 8 PM.

- Would your alert be triggered for this activity?

Yes, the threshold that was set was at 180.

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

No, the threshold that was established was based on the logs prior to the attack which was representative of regular activity. The threshold that was used would have triggered the alert.

Alert Analysis for HTTP POST Activity

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

Yes, there was a sharp increase in HTTP POST activity at 8 PM, March 25

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

8 PM - 1296

- When did it occur?

8 PM, March 25

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

No. The “apache_logs”, which represents regular activity, does not show any POST method counts higher to the threshold that was established for the alert. In the event of this attack, being the “apache_attack_logs”, the alert would have triggered.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, there was a significant increase in the count of POST methods between 7 PM and 9 PM.

- Which method seems to be used in the attack?

```
The POST method.
```

- At what times did the attack start and stop?

```
It seems to have started at 7 PM and ended at 9 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?

```
Yes, there was an increase in activity from Ukraine.
```

- 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
```

- What is the count of that city?

```
Kiev, Ukraine - 440
Kharkiv, Ukraine - 433
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there was an increase in the count for /VSI_Account_logon.php.
```

- 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 type of URI being accessed, an assumption could be made that the attacker is using either a SQL injection or is trying to perform a brute force attack on user accounts.