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 most noticeable ones are from high severity events.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes. The number of failed activities decreased and the successful activities increased.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes the alert did detect some suspicious volume of failed activity.

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

35 failed windows activities

- When did it occur?

```
8 am on 3-25-2020
```

- Would your alert be triggered for this activity?

```
Yes the alert would be triggered as the threshold was set to go off if there
were more than 20 failed windows activities in an hour.
```

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

```
No I think the threshold is low enough for us not to get spammed and high
enough for us to get notified when there are more failed attempts than
usual.
```

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?

```
16 failed login attempts
```

- Who is the primary user logging in?

```
user_a
```

- When did it occur?

```
2:00am 3-25-2020
```

- Would your alert be triggered for this activity?

No as the threshold was set to 30 or more successful attempts

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

Yes we would adjust the threshold but would definitely need further observation to come up with an alert that has a threshold that;s not too low nor too high.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes

- What signatures stand out?

In the Timechart by Signatures there was a user account that was locked out and there was an attempt to reset an account password.

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

The attempt to reset an account happened between 9:00am - 10:00am
The user account was locked out between 1:00am - 2:30am

- What is the peak count of the different signatures?

Locked out account at 896
Password reset attempt at 1268

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes
```

- Which users stand out?

```
user_a and user_k
```

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

```
user_a between 1:00am - 2:30am
user_k between 9:00am - 10:00am
```

- What is the peak count of the different users?

```
user_a at 984
user_k at 1256
```

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

- Does anything stand out as suspicious?

```
Yes
```

- 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?

```
Yes an increased activity from user_a and user_k
```

- 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?

The timecharts for signatures and users makes it easy to find the count for each event or for the user per hour. One downside of this is that it;s hard to tell when there is a change in activity unless you’re closely monitoring it. The line graph easily shows the spikes and drops and the pie chart shows clearly changes in increase of activity.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes

- What is that method used for?

POST

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Yes

Report Analysis for HTTP Response Codes

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

```
Yes
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes
```

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

```
939 at 8:00pm
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

Alert Analysis for HTTP POST Activity

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

```
Yes
```

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

```
1296 at 8:00pm
```

- When did it occur?

```
8:00pm 3-25-2020
```

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

```
No
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes
```

- Which method seems to be used in the attack?

```
POST
```

- At what times did the attack start and stop?

```
7:00pm -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
```

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

```
Kiev and Kharkiv, Ukraine
```

- What is the count of that city?

```
Kiev - 439

Kharkiv - 433
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```

- What URI is hit the most?

```
VSI_account_logon.php
```

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

```
Possibly a brute force attack or SQL injection.
```