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 change in high severity instances raised by approximately 13.314% from
Day 2 compared to Day 1.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
No; The amount of failed Windows activity dropped from Day 1 to Day 2 from
2.98% down to 1.564% respectively.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, on Wednesday, March 25th at 8AM there was 35 failure events compared to
an average no higher than 10 the previous day even at the highest point.
```

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

```
There were 30 counts of a failure event.
```

- When did it occur?

```
March 25th, 2020 at 8:00AM
```

- Would your alert be triggered for this activity?

```
Yes. The alert was set to go off if more than 10 events per hour occurred.
```

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

```
No, however if the company were concerned about future attacks, they could
lower the threshold and dedicate more resources to this monitoring.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
There was on Day 2 one point in the day at 2 AM with 94 successful logins,
and 70 successful logins at 9 AM. (03/25/2020)
```

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

```
94 logins at 2AM and 70 logins at 9 AM.
```

- Who is the primary user logging in?

```
“User_a” (91 attempts at 2 AM) & “user_k” (70 attempts at 9AM)
“User_k” also had 52 login attempts the next hour at 10 AM making their
combined login attempts higher than “user_a” but still lower per hour.
```

- When did it occur?

```
2 AM and 9 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?

```
I would likely change the threshold to around 20 attempts, as the baseline
from the day before rarely surpassed that and all suspicious activity was
much higher than this baseline.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
There were only 10 more events on the Day 2 event logs than there were on
Day 1 (318 compared to 338), however the majority of the events occurred in
two clusters of around 1-2am and 9-10am on Day 2 instead of spread more
thinly throughout the day on Day 1.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes.
```

- What signatures stand out?

```
There was a user that was locked out on Day 2 around midnight, until 2 AM,
followed by a large number of attempts (1,258) to reset a password.
```

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

```
The lockouts ran from midnight to 2 AM, and the attempts to change passwords ran from 8 AM to 11 AM.
```

- What is the peak count of the different signatures?

```
There were 896 instances of a user being locked out of their account, and 1,258 attempts to reset a password.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes.
```

- Which users stand out?

```
“user_a” and “user_k” stand out as suspicious. There is 984 actions from “user_a” at 2 AM and 1,256 actions from “user_k” at 9 AM.
```

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

```
“user_a”’s actions begin at midnight and end by 3 AM (based off of visualization) and “user_k”’s actions begin at 8 AM and end by 11 AM (based off of visualization).
```

- What is the peak count of the different users?

```
984 actions from “user_a” and 1,256 actions from “user_k”.
```

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?

```
The dashboard results line up with the previous dashboard for signatures we saw earlier. The different visualizations emphasize the severity and repetition of the attacks we saw previously, especially compared to the other baselines of actions taken at the same time.
```

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

- Does anything stand out as suspicious?

```
Yes. The previously mentioned suspicious activity for users shows through in this information as well.
```

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

```
Yes. The information matches what was previously observed. Much like with the signature analysis with the bar, graph, and pie charts, these visualizations illustrate just how outsized these user's actions were in comparison to every other user.
```

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?

```
If there's too many large samples of data, sometimes a visualization can become too messy to easily navigate. In that instance something like the statistics on this page can be much easier to understand. They also could be more useful when needing to find the largest number quickly in a small data set. Data in this format can also easily be copied into another format quickly if need be.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, The HTTP methods are POST and GET with a combined 2000+ requests
```

- What is that method used for?

```
This method is used for a DDOS attack. A GET request is used to retrieve standard, static content like images while POST requests are used to access dynamically generated resources
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
There were a few different domains that entered or changed spots on the top 10 list. The biggest difference was the total amount of visits per website was down by nearly 10 % for all websites. The difference can be seen most with http://semicomplete.com going from 6076 to 706 count. This could be due to the flood of HTTP POST and GET requests.
```

Report Analysis for HTTP Response Codes

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

```
The 1 Day activity had significantly more 200 status compared to the the day2 logs. Also the amount of 404 errors rose significantly from day 1 to day 2 which does support the of a DDOS attack. On a side note the website had less 500 status on day 2 with 1 compared to 6.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes the amount of visits from Ukraine jump into the top 10 being the second visited country with 20% of total users.
```

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

```
There were about 864 events at 8pm March 25 2020.
```

- Would your alert be triggered for this activity?

```
The alert would not be triggered because it was not set to Ukraine
```

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

```
I would change the threshold to about 20.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, the alert would have detected the HTTP POST Activity
```

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

```
1296
```

- When did it occur?

```
8pm
```

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

```
Yes and no, to my understanding from the last activity the events are way
down so maybe I would adjust the count threshold based on time of hear or
whatever would trigger higher activity for that week.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
The amount of HTTP methods GET and POST
```

- Which method seems to be used in the attack?

```
Both GET and POST though GET is a common request method.
```

- At what times did the attack start and stop?

```
The attack occurred during 6pm to 8pm and seemed to have slowed down at 7pm
```

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

```
The peak count 1296 and it was post
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
At first glance no there is nothing suspicious or different from the two
maps.
```

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

```
Difficult to see at first glance but the bubble over eastern Europe seems
lower and covers some parts of Ukraine.
```

- What is the count of that city?

```
For Kyiv it is 438 and for Kharkiv 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
The amount of /VSI_Account_logon.php went from 202 at 1% to 29.42% at 1323
count.
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
The attacker may have tried to do a brute force attack.
```