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 severity levels changed with informational level events going from 4435(93.1%) to 4383 events (79.8%), while high level events went from 329(6.9%) to 1111 events (20.2%), revealing a large increase of high level severity events.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

The original report had the success rate at 97.019312% and the failure rate at 2.980688%, now it has changed to 98.436712% success rate and 1.563288% failure rate, showing there to be an increase in successful activity and decrease in failed activity. Then there was an increase of total activity as well, with there being 5856 successful events and 56 failed events.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

There were a total of 93 failed activity events, a decrease of volume from the total of 142 in the original log.

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

There were 93 total events.

- When did it occur?

6 events at 12AM, 8 events at 1AM, 2 events at 2AM, 3 events at 3AM, 7 events at 4AM, 6 events at 5 AM, 7 events at 6AM, 8 events at 7AM, 35 events at 8AM, 3 events at 12PM, and 8 events at 1PM.

- Would your alert be triggered for this activity?

Our alert would only be triggered for the outlier of 35 events at 8AM.

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

Yes, our threshold of 10 is a bit too high and would only alert for one of the many hours.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes there was an increase in volume by over 100 events compared to the original log.

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

The total count of events was 432 events.

- Who is the primary user logging in?

```
User_j accounted for 302 of these events.
```

- When did it occur?

```
11 events at 12AM, 15 events at 1AM, 14 events at 2AM, 14 events at 3AM, 12
events at 4AM, 9 events at 5 AM, 11 events at 6AM, 15 events at 7AM, 16
events at 8AM, 4 events at 9AM, 23 events at 10AM, 196 events at 11AM, 77
events at 12PM, and 15 events at 1PM.
```

- Would your alert be triggered for this activity?

```
Our alert would be triggered for the consecutive 3 hours of 10AM-12PM.
```

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

```
I believe the threshold of 20 should be slightly lowered to at least 15 to
attest for the other hours.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
The volume of deleted accounts went down from 318 events in the original log
to 130 events in the attack log.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
There were two signature fields that stood out as extremely suspicious when
compared its immense volume to the volume of the other fields.
```

- What signatures stand out?

“A user account was locked out” , “An attempt was made to reset an accounts password”, were the two signature fields that stood out the most by far. Then there was “an account successfully logged on” field as well that had some numbers, but still paled in comparison.

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

From about 12AM-3AM was the timespan of the “a user account was locked out” signature field, then about 8AM-11AM was the timespan of the “An attempt was made to reset an accounts password” signature field, and about 10AM-1PM was the time span of the “an account successfully logged on” signature field

- What is the peak count of the different signatures?

The peak counts for “a user account was locked out” signature field was 896 events at 2AM, for the “An attempt was made to reset an accounts password” signature field it was 1258 events at 9AM, and for the “an account successfully logged on” signature field it was 196 events at 11AM.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

It matches the previous time chart for the signature fields, essentially revealing the user responsible for the spike in certain signature fields.

- Which users stand out?

User_a, user_k, & user_j were the users that stood out.

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

User_a stood out from 12AM-3AM, user_k stood out from 8AM-11AM, and user_j stood out from 10AM-1PM.

- What is the peak count of the different users?

User_a peak count was 984 events at 2AM, user_k peak count was 1256 events at 9 AM, user_j peak count was 196 events at 11AM.

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

- Does anything stand out as suspicious?

The two signature fields from before, “A user account was locked out” & “An attempt was made to reset an accounts password”, dominated the pie chart accounting for 65% of all signatures, the other 35% being dispersed with 9 other various signatures.

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

Yes the results within the pie chart matched the signature time chart, confirming our findings.

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

- Does anything stand out as suspicious?

User_a and user_k account for nearly 70% of all user activity within the pie chart.

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

Yes the results within the pie chart matched the user field time chart, confirming our 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?

They provide a better insight on pinpointing specific totals and percentages but don't represent the time spans like the time charts.

Apache Web Server Log Questions

Report Analysis for Methods

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

The volume decreased from 10,000 to 4,497. The GET method went from 98.5% to 70.2%, POST method went from 1.1% to 29.4%, HEAD method went from 0.4% to .3%, and lastly OPTIONS method stayed the same with a count of 1. Overall, the methods that were significantly impacted were GET & POST methods.

- What is that method used for?

POST method is usually used to send and store data within a server, while the GET method is used to request data from the server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Once again, the total count went down by over 5000 in the attack logs, but although the volume decreased drastically the splits remained fairly similar.

Report Analysis for HTTP Response Codes

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

Decreased volume and the three major changes were response codes 200 went from a count of 9126(91.26%) to 3746(83.3%), 304 went from 445(4.45%) to 36(.8%), and 404 went from 213(2.13%) to 679 (15.1%).

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

The international activity volume decreased and was mainly concentrated in the hour of 8AM.

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

120 events at 12AM, 108 events at 1AM, 88 events at 2AM, 95 events at 3AM, 81 events at 4AM, 85 events at 5 AM, 74 events at 6AM, 90 events at 7AM, 79 events at 8AM, 107 events at 9AM, 98 events at 10AM, 46 events at 11AM, 61 events at 12PM, 66 events at 1PM, 58 events at 2PM, 70 events at 3PM, 53 events at 4PM, 33 events at 5PM, 39 events at 6PM, 81 events at 7PM, 937 events at 8PM, and 28 events at 9PM.

- Would your alert be triggered for this activity?

The threshold of 50 would be triggered for most of the hours.

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

No, I believe the threshold of 50 to be adequate enough to address the issue.

Alert Analysis for HTTP POST Activity

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

The volume of this activity increased drastically going from a count of 106 to 1324.

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

Nearly all the volume occurred in the hour of 8PM, with it accounting for 1296 hourly events.

- When did it occur?

8PM- 1296 events, rest of the hours combined for 28 hourly events.

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

THe threshold of 15 would only catch the outlier hour of 8PM, outside of that no other hour exceeded 7 hourly events, so probably lower it to 5 would be a better fit for the dataset.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

There are some very suspicious spikes associated with the POST and GET method.

- Which method seems to be used in the attack?

POST and GET methods.

- At what times did the attack start and stop?

From 5PM-7PM there was unusual activity associated with the GET method and 7PM-9PM there was unusual activity associated with the POST method, these two separate time ranges indicate an attack.

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

THe peak count of the POST method was 1296 events.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Outside of the high volume in the east coast of the USA, there is an unusually high volume of activity throughout 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 were the two cities in Ukraine with
unusually high volume.
```

- What is the count of that city?

```
There was a count of 439 in Kiev and 432 in Kharkiv.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
The URI data count for the company’s login info has a suspiciously high
volume.
```

- What URI is hit the most?

```
The /VSI_Account_logon.php URI has the highest count by far with a count of
1323.
```

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

```
The attacker could be accessing employee accounts and manipulating their
credentials through brute force attacks or another credential-based attack.
```