Cybersecurity

Project 3 Review Questions

Make a copy of this document before you begin. Place your answers below each question.
Group: Danielle Gutierrez, Daniel Garrett, Heather Cooley, Jaycee Shin, Eric Colbert

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
Yes, we did. The informational level severity alerts percentage dropped from
93% at our normal levels to 79.8% during the attack. More importantly, the
high level severity percentage rose from 7% during normal traffic to 20.2%
during the attack. This is a significant increase in high severity levels.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
There was actually a decrease in failed activities during the attack. Before
the attack, we had 2.98% failed activities on our Windows server. During the
attack, we had 1.56% failed activities on our Windows server. This could be
because their attack was successful and created more successful activities.
However, it wasn't a significant change in percentage. The traffic was
increased during the attack (5856 successes during the attack vs 4622
successes during normal times), which is more significant of a change.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, during the hour 8am-9am on Wednesday, March 25, 2020, we had a large
increase in failed activities.
```

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

```
There were 35 failed events during that hour.
```

- When did it occur?

```
Wednesday, March 25, 2020 during 8am-9am.
```

- Would your alert be triggered for this activity?

```
Yes, the threshold was set for 15 failed events before our alert gets
triggered.
```

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

```
No, because it didn’t give us any false positives but also alerted us to the
suspicious activity.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?0

```
 Yes at 10 am on Wednesday March 25, 2020 there were no logins.
```

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

```
There were only 4 logins during 9am-10am, then 0 logins during the hours
between 11am and 12pm, and again only 4 logins during 12pm-1pm.
```

- Who is the primary user logging in?

```
User_a logged in 14.29% of the time.
```

- When did it occur?

```
Wednesday March 25 at 9 am and went till 12 pm.
```

- Would your alert be triggered for this activity?

```
No, we set up our alert for an unusually high number of logins. We set to be alerted for over 35 successful logins in one hour.
```

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

```
Yes, looking at the attack, we are really looking for unusually low logins. We could change our alert to alert us whenever successful logins is less than 7 in one hour. This could alert us to a system being off.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, there was an unusually low amount of deleted accounts between 9am and 12pm on March 25, 2020. We would change our alert to also have a floor to alert us, for example, when deleted accounts is less than 5, send an alert. This would show if the servers were offline.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
There are three signatures (A user account was locked out, An attempt was made to reset an accounts password, and An account was successfully logged in) that have significant spikes in activity.
```

- What signatures stand out?

```
A user account was locked out, An attempt was made to reset an accounts password, and An account was successfully logged in were all substantially higher than other activities and had large spikes at different times.
```

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

```
March 25th “User account was locked out” signature started at 12 am and stops at 3 am. March 25th “An attempt was made to reset an accounts password” signature happened between 8am and 11am. March 25 “An account was successfully logged on” signature happened between 10am to 1pm.
```

- What is the peak count of the different signatures?

```
An attempt was made to reset an accounts password (1,258/hr)
A user account was locked out (896/hr)
An account was successfully logged in (196/hr)
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
User A got locked out of accounts, user K attempted to reset account passwords and user J successfully logged on to an account a suspicious amount of times.
```

- Which users stand out?

```
User A, user J and user K.
```

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

```
User A started at 12 am and stopped at 3 am. User J started at 10:00 am and stopped at 1:00 pm. User K started at 8:00 am and stopped at 11:00 am
```

- What is the peak count of the different users?

```
User A (984/hr), User K (1,256/hr), User J (196/hr)
```

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

- Does anything stand out as suspicious?

```
A user account was locked out (1811 activities), An attempt was made to reset an accounts password (2128 activities), and An account was successfully logged in (432 activities) were all substantially higher than other activities.
```

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

```
Yes, these are the same findings from our signatures time chart.
```

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

- Does anything stand out as suspicious?

```
User K is responsible for 35.6% of activities, User A is responsible for 31.6% of activities, and User J is responsible for 6.7% of activities during the attack. These are a lot higher than other users.
```

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

```
Yes, these are the same findings from our users time chart.
```

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?

```
It was easier to see total events that happened when we used the bar chart and the pie chart. Some disadvantages are that we weren't able to see the time of the events, we could only see the amount of events that occurred.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, there was a significant drop in GET methods (98.51% to 70.20% during
the attack) and the POST increased substantially (1.06% to 29.44% during the
attack).
```

- What is that method used for?

```
POST method is used to send or upload any data to the server.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
The referrer domains dropped by about 75%
```

Report Analysis for HTTP Response Codes

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

```
Response code 200 dropped about 8%. Response code 404 increased
significantly (213 preattack to 679 during the attack).
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
At 8:00 pm on March 25th, 2020 there were 939 events from other countries.
This was much higher than our usual activity.
```

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

```
Between 8pm and 9pm on March 25, 2020, there were 939 events from Non-US countries.
```

- Would your alert be triggered for this activity?

```
Yes, we set the alert to trigger at anything over 100 Non-US clients. We would have also had 3 false positives with that number.
```

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

```
Yes, we would increase our threshold to 135 Non-US clients per hour. This will decrease the number of false positives while also catching attacks.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, on March 25, 2020 at 8pm there was an extremely large spike in HTTP POST activity.
```

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

```
During the attack there were 1296 HTTP POST activities.
```

- When did it occur?

```
March 25, 2020 from 8 pm to 9 pm.
```

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

```
No, we wouldn't change our threshold. We didn't catch any false positives, but we definitely caught the attack.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There are two large spikes in activity with the GET method and the POST method.
```

- Which method seems to be used in the attack?

```
The HTTP methods GET and POST were used.
```

- At what times did the attack start and stop?

```
There was a spike in GET requests between 5pm and 7pm. The spike in POST requests was between 7pm and 9pm.
```

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

```
The peak count of POST during the attack was 1,296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Ukraine had a large number of client ip connections.
```

- 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 had 439 and Kharkiv had 433
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
/VSI_Account_logon.php and /files/logstash-1.3.2-monolithic.jar increased
substantially.
```

- 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 is trying to log in to the web server.
```