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, there was an increase in the severity of the events, from 6.9% to
20.2%.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Baseline was 4441 and the Attack log showed 5578 ‘Failure’ events an
increase of about 1,100
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, we saw server spikes twice throughout the attack log.
```

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

```
We saw about 1,600 failure events between 1&2AM and we saw 1900 more failure events between 9&10AM on March 25, 2020.
```

- When did it occur?

```
1&2am and 9&10am
```

- Would your alert be triggered for this activity?

```
My alert threshold was 500 so all four hourly event spikes would have triggered an alert.
```

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

```
Based on the Baseline data and
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
We saw that it was suspicious in that the successful logins dropped during the attack log
```

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

```
We saw network wide logons drop significantly, we also saw an astronomical rise in  “A user account was locked out” events, it accounted for 34% of the signatures during the attack log
```

- Who is the primary user logging in?

```
user_a & user_k
```

- When did it occur?

```
user_a occurred from 12:00-3:00 & user_k occurred from 8:00-11:00.
```

- Would your alert be triggered for this activity?

```
My alert would’ve caught the drop in user logins but it would not have alerted the increased user activity, though the dashboard would.
```

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

```
I'd create a threshold alert for both abnormal successful logins for specific users rather than measuring user login rate across the server.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Again we noticed a drop in the volume of deleted accounts
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
About 800 user lock outs at both 1:00 am and 2:00 am, about 1200 attempts at 9:00am and about 800 attempts at 10:00am for attempted resets for passwords, about 200 successful logins after the password reset spike starting at 11:00am
```

- What signatures stand out?

```
‘A user account was locked out’, ‘An attempt was made to reset an account password’ & ‘An account was successfully logged on’
```

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

```
‘A user account was locked out’ the spike lasted from 1:00-2:00am
```

```
‘An attempt was made to reset an account password’ the spike lasted from 9:00-10:00am
‘An account was successfully logged on’ spike at 11:00am
```

- What is the peak count of the different signatures?

```
896 for ‘A user account was locked out’ & 1258 for ‘An attempt was made to reset an account password’ & 196 for ‘An account was successfully logged on’
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
3 user’s activity spiked at different times
```

- Which users stand out?

```
user_a, user_k, & user_j
```

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

```
user_a: 12:00pm-3:00am
user_k: 8:00am-11:00am
user_j 10:00am-1:00pm
```

- What is the peak count of the different users?

```
user_a: 984
user_k: 1,256
user_j: 196
```

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

- Does anything stand out as suspicious?

```
The differences between the baseline and the attack log were pretty dramatic.
```

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

```
Yes , the results of the pie charts also coincides with the signature time chart.
```

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

- Does anything stand out as suspicious?

```
‘A user account was locked out’ & ‘An attempt was made to reset an account’s password’ had alarmingly high increases
```

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

```
Yes, they do.
```

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 signature IDs are not available, but you can see pretty easily where the signature traffic goes and changes, and the visualization aspect of the time chart and the pie graph really illustrates what an attack would look like easily without sifting through raw data.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
At 6PM on 3/25/2020 there was a 671 spike of failed GET requests. There was a lot more traffic on the attack logs at 6PM there was a spike with 729 GET requests. Then at 8PM there was a major spike in POST requests at 1,296. Which could indicate a possible DDoS attack.
```

- What is that method used for?

```
OPTIONS is what showed up on both of the logs. It's not technically dangerous by itself but used with PUT,DELETE or TRACE can be used to leak information to help plan attacks.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, there was one from logstash.net. This is a tool used to collect and process logs from different systems and websites. BUT logstash.net isn't the official domain (elastic.co/logstash). It is a deceptive way to make requests appear legitimate.
```

Report Analysis for HTTP Response Codes

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

```
On 3/25/20 at 8PM there is a major spike in 200 response codes. 1,296 were POST requests indicating a brute force attack. There was a spike at 6PM of 404 response codes.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
On 3/25/2020 at 8PM there was a spike in activity.
```

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

```
877
```

- Would your alert be triggered for this activity?

```
Yes, but it would have been later on since I originally set my threshold at
150.
```

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

  I changed the threshold to 130 instead of 150.

```
```

Alert Analysis for HTTP POST Activity

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

```
Yes there was an extremely high amount of POST requests the whole day of
3/25/20. With it peaking at 1415
```

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

```
00:00:128, 01:00:120, 02:00:115 03:00:127 04:00:115 05:00:124, 06:00:115,
07:00:122, 08:00:114, 09:00:125, 10:00:116, 11:00:116, 12:00:112, 13:00:113,
14:00:122, 15:00:126, 16:00:118, 17:00:119, 18:00:730, 19:00:123,
20:00:1415, 21:00:86.
```

- When did it occur?

```
It started at 12AM and ended at 9PM, The highest being 1415 and lowest being
86 by the end of the attack.
```

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

```
No, I set the original threshold at 10 and that would be able to catch any
further suspicious activity.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There is a high amount of GET requests and an even higher amount of POST requests.
```

- Which method seems to be used in the attack?

```
Brute Force
```

- At what times did the attack start and stop?

```
There was an uptick in POST requests at 12AM and it didn’t go back to the baseline until 10PM.
```

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

```
1415
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
There was a high volume of activity in Europe.
```

- 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?

```
In Kiev 439 and in Kharkiv 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Very high number of activity
```

- What URI is hit the most?

```
VSI_Account_logon.php
```

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

```
All signs are pointing to a brute force attack.
```