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 count of ‘high’ severity level events rose from 329 events to 1111
(6.9% to 20.2%).
‘Informational’ severity levels saw a decrease of 4435 to 4383 events (93%
to 79.7%).
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Success count of windows activities rose from 4622 events to 5856, with an
increase of 1.42% (97.01% to 98.43%)
Failed windows activities count decreased by 1.42% from 142 events to 93
(2.98% to 1.56%)
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, identified a spike in event counts for the given search query
```

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

```
We identified a peak count of 35 events
```

- When did it occur?

```
This occurred between 8am and 9am on March 2020
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
There was a max event reduction of 7 identified. Normal logs indicated successful logins ranging between 9 and 21 per hour, whereas our attacks showed results of 0 to 16 events per hour.
```

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

```
8 events were counted over a 3 hour period, with a maximum count of 4 events each hour
```

- Who is the primary user logging in?

```
user_a
```

- When did it occur?

```
Between 9am and 1pm on 25 March 2020
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
Not necessary to change the threshold.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, we identified that the new baseline within the attack logs shows us a value of 9, compared to a baseline of 15 within the initial server logs. This shows a decrease in deleted account signature events
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
From the results we can identify a possible brute-force attack due to the high level of events in relation to user logins and failed logins within a short period of time.
Attempts and change of password requests subsided once there was an incline in account successful logins, possibly indicating attackers had successfully gained access.
```

- What signatures stand out?

```
The following signatures stood out:
   -  “User account locked out”
   -  “An attempt was made to reset an accounts password”
   -  “An account was successfully logged on”
```

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

```
We identified a spike between 12am and 2:30am for “user account locked out”. For “an attempt was made to reset an account's password” we identified a spike between 8am and 11am. There was a spike between 10am and 12:30pm for the signature “an account was successfully logged on”.
```

- What is the peak count of the different signatures?

```
“User account locked out” had a peak count of 896
“An attempt was made to reset an account's password” had a peak count of 1258 events.
“An account was successfully logged on” had a peak count of 196 events.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
There was suspicious activity from 8am to 11am on Wednesday, March 25th and between 4pm and 7pm on the same day.
```

- Which users stand out?

```
Users user_a and user_k stand out as suspicious
```

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

```
User_a: Started at 12:00am on 25th March and stopped at 3:00am on 25th March.
User_k: Started at 8:00am on 25th March and stopped at 11:00am on 25th March.
```

- What is the peak count of the different users?

```
User_a had a peak count of 984 and user_k had a peak count of 1256.
```

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

- Does anything stand out as suspicious?

```
Identified an increase in user count from 354 to 1256 and no domain users were listed when viewing ‘top’ results in the attack logs. Suspicious activity started at 8am-11am and 4pm-7pm, all on the 25th of March.
```

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

```
Yes, the results were synonymous with the findings
```

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

- Does anything stand out as suspicious?

```
We identified users user_a and user_k to be identified as having increases in their activity.
```

- 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?

```
Statistical charts allow you to view data points and values quickly and efficiently,however it becomes difficult to compare data over time or analyze multiple variables within a field.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
We identified an increase in POST HTTP methods of 28%, with an increase from
1% to 29% (count of 9852 pre attack to 3157 post attack). GET request
activity decreased by 28.5%, from 98.5% before the attack down to 70% post
attack (count of 106 pre attack to 1324 post attack).
```

- What is that method used for?

```
GET response is used to request data from a server, whereas POST is used to
send data to a server to create or update a resource.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Various new domains identified such as:
   - http://turxradar.com
   - https://www.google.com.br
   - http://kufli.blogspot.com

Google domain is especially suspicious, as it is disguising itself as the
official domain of Google.
```

Report Analysis for HTTP Response Codes

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

```
There was a significant increase in 404 (not found responses) and an
decrease in 200, 206,301 and 304 requests.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there was a suspicious volume of activity in Ukraine at 4am on March 26th.
```

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

```
We identified a count of 864 events during the hour of 4am.
```

- Would your alert be triggered for this activity?

```
Yes, as the threshold was set at 170.
```

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

```
No change in threshold necessary
```

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?

```
We identified a total count of 1296 events
```

- When did it occur?

```
This occurred at 4am on 26th March 2020
```

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

```
No change in threshold necessary
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There was suspicious activity with the GET method from 1am to 3am on 26th March 2020. We identified suspicious POST activity from 3am to 5am on 26th March 2020.
```

- Which method seems to be used in the attack?

```
POST method was the primary method used in the attack
```

- At what times did the attack start and stop?

```
GET attack commenced at 1am on 26th March 2020 and concluded at 3am on 26th March 2020.
POST attack occurred from 3am to 5am on 26th March 2020.
```

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

```
GET requests had a peak count of 729, whereas POST requests had a peak count of 1296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
We identified increased levels of traffic coming out of Ukraine
```

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

```
From the results we identified the city of Kharkiv  in Ukraine having a high volume of activity. Another noticeable location is the town of Kiev as well.
```

- What is the count of that city?

```
Kharkiv showed a total count of 432 events.
Kiev showed a total count of 440
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
There was suspicious activity with the URI
“/files/logstash/logstash-1.3.2-monolithic.jar” with 638 counts at 21% total
and URI “/VSI_Account_logon.php” with 1323 counts at 43.6%.
```

- What URI is hit the most?

```
“/VSI_Account_logon.php” was hit the most, with 1323 total events recorded.
```

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

```
The data shown indicates that the attacker was attempting to execute a brute
force attack against the VSI logon page.
```