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 I did, the High severity changed from 329 (6.9%) to 1111 (20.2%)
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, the failed activities reduced from 142(2.9%) to 93(1.5%)
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes
```

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

```
35 counts of failed activity
```

- When did it occur?

```
March 25, 2020 at 8AM
```

- Would your alert be triggered for this activity?

```
Yes our baseline was 12
```

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

```
No we would not change it
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
No
```

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

```
N/A
```

- Who is the primary user logging in?

```
N/A
```

- When did it occur?

```
N/A
```

- Would your alert be triggered for this activity?

```
No
```

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

```
No
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
no
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, we observed suspicious activity
```

- What signatures stand out?

‘A user account was 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?

A user account was locked out : 12am to 3am
An attempt was made to reset an accounts password : 8am to 11am
An account was successfully logged on : 10am to 12pm

- What is the peak count of the different signatures?

A user account was locked out : 895 counts
An attempt was made to reset an accounts password : 1258 counts
An account was successfully logged on : 196 counts

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, we observed some suspicious user activity
```

- Which users stand out?

```
User_a, User_k, User_j
```

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

```
User_a : 12am to 3am
User_k : 8am to 11am
User_j : 10am to 12pm
```

- What is the peak count of the different users?

```
User_a : 984
User_k : 1256
User_j : 196
```

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

- Does anything stand out as suspicious?

```
Yes, we saw a lot of suspicious activity which our alerts didn't pick up
```

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

```
Yes
```

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

- Does anything stand out as suspicious?

```
Yes
```

- 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?

```
When we created ou reports, they did not pick up on the weird user
activities but the user panels clearly show the suspicious activities of the
users that were attacking the server.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
HTTP Post went from 106 to 1324
```

- What is that method used for?

```
HTTP Post Upload data to the webserver
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No
```

Report Analysis for HTTP Response Codes

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

```
Yes code 404 increased 213 to 679.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes
```

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

```
937 events
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No.
```

Alert Analysis for HTTP POST Activity

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

```
Yes it went from 106 to 1324
```

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

```
1296 events
```

- When did it occur?

```
March 25, 2020 at 8pm
```

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

```
No, we had our baseline at 10
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes
```

- Which method seems to be used in the attack?

```
GET and POST
```

- At what times did the attack start and stop?

```
GET method : 5pm to 7pm
POST method : 7pm to 9pm
```

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

```
GET method : 729
POST method : 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes
```

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

```
The US had the top 2 Cities, Ashburn and New York but the second highest was Ukraine with Kyiv and Kharkiv
```

- What is the count of that city?

```
Kyiv has 438
Kharkiv has 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes
```

- 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 was trying to login to the webpage. Possibly a brute force
attack.
```