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, “High” severity jumped by about 14%
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
No, failed activities actually dropped while successful activities increased
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, there was a suspicious volume of failed activity
```

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

```
35 events
```

- When did it occur?

```
8am 3/25/2020
```

- 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?

```
Yes, there was a suspicious amount of successful logins
```

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

```
196 events at 11am on 3/25/2020 and then 77 events at 12pm on the same date
```

- Who is the primary user logging in?

```
[Enter answer here]
```

- When did it occur?

```
[Enter answer here]
```

- 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 Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No, it seemed on par with the threshold of what the average account deletion is.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, there is some suspicious activity
```

- What signatures stand out?

```
“A user account was locked out” and “An attempt was made to reset an accounts password”
```

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

```
12am to 3am for “A user account was locked out” and 8am to 11am for “An attempt was made to reset an accounts password”
```

- What is the peak count of the different signatures?

```
896 for account lockout and 1,258 for account password reset
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes the events for two of the users have drastically increased
```

- Which users stand out?

```
User_a: and user_k: are the two accounts that stand out
```

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

```
User_a: started at 12am and went to 3am and user_k: started at 8:00am and
went until 11am
```

- What is the peak count of the different users?

```
User_a: had a peak count of 984 and user_k: had a count of 1,256
```

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

- Does anything stand out as suspicious?

```
Yes “A user account was locked out” and “An attempt was made to reset an
accounts password” signatures both drastically increased
```

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

```
They match in the sense that both the signatures increased but their count
is different
```

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

- Does anything stand out as suspicious?

```
Yes, user_a: and user_k: events both drastically increased
```

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

```
Somewhat. The users are the same but the event counts are different
```

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?

```
[Enter answer here]
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, the POST method drastically increased
```

- What is that method used for?

```
For sending user submitted data to the web server
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes, the two top referrer domains dropped drastically.
```

Report Analysis for HTTP Response Codes

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

```
Yes, the response code 200 for success drastically dropped
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there was suspicious international activity detected
```

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

```
939 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, there was suspicious activity detected
```

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

```
1,296 events
```

- When did it occur?

```
At 8pm on 3/25/2020
```

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

```
No
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, the HTTP POST method is being used a lot more
```

- Which method seems to be used in the attack?

```
POST
```

- At what times did the attack start and stop?

```
It started at 7pm and ended at 9pm on 3/25/2020
```

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

```
1,296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
[Enter answer here]
```

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

```
[Enter answer here]
```

- What is the count of that city?

```
[Enter answer here]
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, the logon page is being visited way more
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
Brute Force attack
```