Cybersecurity

Alert Analysis for HTTP POST Activity

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, activity  was at a higher percentage at 20.229425.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
No suspicious changes were detected in failed activities.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes , when set to all time.
```

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

```
35 events
```

- When did it occur?

```
March, 25th, 2020
```

- Would your alert be triggered for this activity?

```
Yes, this activity would trigger our alert, as count is over the threshold.
```

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

```
The threshold would not be changed, as the uptick in count triggered alerts properly.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, suspicious volumes of successful logins were detected.
```

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

```
1,293 successful logins within the hour.
```

- Who is the primary user logging in?

```
User_k was the primary user.
```

- When did it occur?

```
March 25th, 2020 at 9 AM
```

- Would your alert be triggered for this activity?

```
This activity would’ve appropriately triggered for this activity.
```

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

```
No, as the threshold was set at a point where alerts would trigger
effectively.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, 17 events on March 25th, 2020 at 5 AM.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
On March 25th 2020 at 9:00 am an attempt was made to reset an accounts
password (1,258 events noted).
```

- What signatures stand out?

```
The signatures that cause alarm are password reset attempt and user account
lockouts.
```

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

```
March 25th 2020 1:00am-account lockout ends around 3:00 am, Password reset
attempt on an account, began on  March 25th, 2020 9:00am, Ends 11:00am.
```

- What is the peak count of the different signatures?

```
Peak for account lockout is 896, Password reset attempt 1,258.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
More suspicious activity in the early morning hours.
```

- Which users stand out?

```
user_a and user_k were user accounts that were most concerning.
```

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

```
User_a began at 1:00 am and stopped at 3:00am, user_k began at 9:00am and
ended after 10am right before 11am.
```

- What is the peak count of the different users?

```
User_a 984, user_k 1,258
```

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

- Does anything stand out as suspicious?

```
Password resets signature had the highest count at 2,128 with a count
percentage of 35.783. Account lockout was the second highest signature with
a count of 1,811 with a count percentage of 30.452.
```

- 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?

```
User K count 2,118 and count percentage 37.086% is the highest among the users for attempted password resets, user_a count for account lockout was highest among users with the count being 1,878 and count percentage at 32.884.
```

- 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?

```
Advantages using this report is it shows more detail with the charts, graphs ect. Reports give the full analysis, and provide information. Dashboards are used more for monitoring through use of a single view.
Disadvantages of a dashboard is it may become cluttered and typically will not include explanations of the results, whereas a report is more likely to give a detailed explanation of the data.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes there were far more “Post” requests by about 1100.
```

- What is that method used for?

```
Post methods are used to write and/or create
 resource on the server.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
There were not any suspicious changes in the referrer domains.
```

Report Analysis for HTTP Response Codes

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

```
The 404 response codes had 400 more than previous.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
There was a suspicious volume of international activity.
```

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

```
8pm and 10pm.
```

- Would your alert be triggered for this activity?

```
Our alert would be triggered.
```

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

```
No. Our alert is set to go off at 80 but the amount recorded during those
hours was 938.
```

Alert Analysis for HTTP POST Activity

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

```
Yes there was some suspicious POST activity
```

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

```
2 hours
```

- When did it occur?

```
25/Mar/2020 20:05:59
```

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

```
Yes I would increase the threshold.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Post requests rapidly increase at 8PM and continuing until 10PM.
```

- Which method seems to be used in the attack?

```
HTTP POST requests were the method used.
```

- At what times did the attack start and stop?

```
The attack begins at 8pm and ends at 10pm.
```

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

```
1,296 POST requests.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
The amount of POST request from Ukraine
```

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

```
Kiev, Ukraine
```

- What is the count of that city?

```
877
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes. There is a URI hit more often than before.
```

- What URI is hit the most?

```
/reference/android/graphics/Path.html
```

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

```
Crafting a malicious URL that could be embedded in a website or sent as in
HTML email. This would run when the requested URI is loaded. From there an
attacker can retrieve user's information and other confidential information.
```