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 high severity events.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, some of the more suspicious activities included “logon attempts using explicit credentials”, “attempts to reset account passwords”, and “user accounts locked out”.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, the report showed an increase in failed login attempts.

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

There were 35 failed login attempts.

- When did it occur?

March 25, 2020 at 8am.

- Would your alert be triggered for this activity?

Yes, our alert threshold was 12 failed login attempts per hour.

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

Not at this stage, the threshold worked as it should.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, the reports showed an increase in successful logins.

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

23 login attempts between 10am - 11am.
196 login attempts between 11am - 12pm.
64 login attempts between 12pm - 1pm.

- Who is the primary user logging in?

user_J.

- When did it occur?

The increase in login activity occurred between 10am and 1pm with the majority of the activity between 11am and 12pm.

- Would your alert be triggered for this activity?

Yes, the alert would have been triggered. The successful login attempts were sustained over a period of 3 hours with the majority of the logins occurring in the middle hour of that time period.

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

Based on these attack logs the threshold for login alerts our threshold was set to 25 and worked as intended.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

No, we did not detect any suspicious increase in the volume of deleted accounts and subsequently our alert did not get triggered.

With up to 22 accounts being deleted each hour in normal conditions, we think it is important to check the accounts that are being deleted regardless of the numbers to ensure accounts are not being maliciously deleted.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, we noticed suspicious activity with regard to the signatures.

- What signatures stand out?

The signature that stood out described “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?

```
A user account was locked out between 1:40AM to 2:40AM.
An attempt was made to reset an account password between 9:10AM to 11AM.
```

- What is the peak count of the different signatures?

```
The peak count for “user account was locked out” was 785.
The peak count for “an attempt was made to reset an account's password” was
397.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Our dashboard showed suspicious activity by 2 users.
```

- Which users stand out?

```
User_A & User_K.
```

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

```
There was suspicious activity for User_A between 1:40AM to 2:40AM.
There was suspicious activity for User_K between 9:10AM to 11:00AM.
```

- What is the peak count of the different users?

```
The peak count for User_A was 785.
The peak count for User_K was 397.
```

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

- Does anything stand out as suspicious?

```
Yes.
```

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

Yes, the same suspicious activity relating to signatures.

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, the same suspicious activity for the two users.

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 advantage of statistical charts is that they provide for easy visual cues relating to abnormal activity.

The disadvantage of statistical charts is that the detail relating to time and duration of an attack can only be observed on the line graph.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, our report showed a substantial increase in POST requests from 1.06% to 29.44%.

- What is that method used for?

The POST request method is used to send data to a web server to create or update a resource on the server. GET method is primarily used for retrieving data and resources from web servers.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No, we did not detect any suspicious referrer domains.

Report Analysis for HTTP Response Codes

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

Yes, our report showed a suspicious increase in 404 status codes between 5:00PM and 7:000PM on March 25, 2020. The 404 status code indicates that the HTTP request method used was not able to retrieve the resource form the web server.

The report also showed a suspicious increase in 200 status codes between 7:00PM and 9:00PM on the same day. The 200 status code indicates that the HTTP request method was successful in retrieving the requested resource from the web server.

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes, our report showed suspicious activity from different countries.

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

Our report showed 432 events between 8:00PM and 9:00PM on March 25,2020.

- Would your alert be triggered for this activity?

Yes, our threshold to trigger this alert was 11 international web visits per hour.

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

We would not change our alert threshold, the alert worked as intended for this attack.

Alert Analysis for HTTP POST Activity

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

Yes, we detected a suspicious volume of HTTP POST activity.

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

Our alert identified 1,296 HTTP POST requests which is a suspiciously high number.

- When did it occur?

March 25, 2020 between 7:00PM and 8:00PM.

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

We would not change our alert threshold of 7 per hour, the alert worked as intended for this attack.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, our dashboard indicates a suspicious increase of HTTP activity.

- Which method seems to be used in the attack?

The attack logs show GET and POST request methods were used the most.

- At what times did the attack start and stop?

There was an increase in GET requests between 5:00PM and 7:00PM while there was an increase in POST requests between 7:00PM and 9:000PM.

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

The peak count for GET requests was 729 and for POST requests it was 1,296.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Yes, our dashboard indicates an increase in web traffic from a country outside of the United States.

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

Our dashboard is showing the cities of Kiev and Kharkiv in the country Ukraine as a source of increased web traffic to the https://vsi-corporation.azurewebsites.net domain.

- What is the count of that city?

There was 439 web visits from Kiev while there was 433 web visits from Kharkiv.

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, our dashboard identifies a suspicious increase in web visits to one URI.

- What URI is hit the most?

Our dashboard showed the following URI https://vsi-corporation.azurewebsites.net/VSI_Account_logon.php was visited 1,323 times.

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

The attacker could potentially be attempting a brute force attack by gaining unauthorized access to user accounts.