| 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 normal server logs had an informational percentage of 93.085330 and a high percentage of 6.914670. The attack logs had an informational percentage of 79.770575 and a high percentage of 20.229425 |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| There was an uptick in more successful events in the attack logs compared to the normal logs. In the normal logs there was 4616 successful activities compared to the 142 failed activities whilst on the attack logs there were 5854 successful activities compared to the 93 failed activities |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes at 8am |
| --- |

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

| 70 failed activities |
| --- |

* When did it occur?

| 8am |
| --- |

* Would your alert be triggered for this activity?

| Yes as my threshold was set to 15 |
| --- |

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

| No I would not |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes |
| --- |

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

| 294 successful logins between 10:00am and 12:00pm |
| --- |

* Who is the primary user logging in?

| user\_j |
| --- |

* When did it occur?

| 10am-12pm |
| --- |

* Would your alert be triggered for this activity?

| Yes as my threshold was set to 30 |
| --- |

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

| No my threshold is still good |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| Yes at 5am there was 34 deleted accounts |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes |
| --- |

* What signatures stand out?

| A user account was locked out and an attempt was made to reset an account password |
| --- |

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

| A user account was locked out ID started at 12:00 am Wed Mar 25 2020 and stopped around 3:00 am of the same day. An attempt to reset an accounts password ID started around 8:00 am Wed Mar 25 2020 and stopped around 11:00 am that same day. |
| --- |

* What is the peak count of the different signatures?

| A user account was locked out peaked at 896 IDS whilst An attempt was made to reset an accounts password peaked at 1258 IDS |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which users stand out?

| user\_k and user\_a |
| --- |

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

| user\_a started around 12:00 am Wed Mar 25 2020 and stopped at 3:00 am that same day. user\_k started around 8:00 am Wed Mar 25 2020 and ended at 11:00 am that same day. |
| --- |

* What is the peak count of the different users?

| user\_a peaked at 984 events whilst user\_k peaked around 1256 |
| --- |

**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 |
| --- |

**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?

| Statistical charts can be sorted to easily see how many activities have occurred with a certain user but it doesn’t do a good job of showing a visualization of all of the users. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| There was a massive increase in the POST method from 100 to 1300 different POST attempts. |
| --- |

* What is that method used for?

| The POST method is an essential part (HTTP) used in web development. It's employed to send data from a client to a server. The data is included in the request body and is processed by the server, which then sends a response. While the POST method itself is not suspicious, it can be misused by cybercriminals for malicious activities such as unauthorized data access, breaches, and attacks. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| There was significantly less activity coming from referrals with the main referrer dropping from 3000 to 764. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| The code 200 (successful) stayed pretty steady until 8pm when we saw it increase by about 400%. 2 hours prior to this anomaly there was a massive amount of 404 error codes that were reported. However during this time we did not see a decrease in 200 successful codes. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| We lost all activity from Australia and saw a decrease in both west coast USA and Europe however there was an increase in the East coast USA. There doesn’t seem to be any influx of foreign countries. |
| --- |

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

| The increase in activity on the east coast occurred around 5pm which is 1 hour before the massive amounts of 404 error codes |
| --- |

* Would your alert be triggered for this activity?

| No, The alert would not be triggered because it did not include the USA as a potential threat. |
| --- |

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

| It could be considered to create an alternate alert for the USA or adjusting the current one to include abnormally low activity from other countries. |
| --- |

**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?

| 1296 |
| --- |

* When did it occur?

| 8pm |
| --- |

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

| No, Anything over 4 Post requests should be reported. |
| --- |

**Dashboard Analysis for Time Chart of HTTP Methods**

* Does anything stand out as suspicious?

| The only anomaly seems to be the aforementioned POST requests. |
| --- |

* Which method seems to be used in the attack?

| POST |
| --- |

* At what times did the attack start and stop?

| 8pm to 9pm |
| --- |

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

| 1296 |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| We lost all activity from Australia and saw a decrease in both west coast USA and Europe however there was an increase in the East coast USA. There doesn’t seem to be any influx of foreign countries aside from Kyiv. |
| --- |

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

| Kyiv, Ukraine |
| --- |

* What is the count of that city?

| 438 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes |
| --- |

* What URI is hit the most?

| The VSI account login php had 1323 counts of activity |
| --- |

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

| DDoS , brute force login |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.