| 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?

| Majority are informational values, only 7% are high severity in pre attack. Post attack, there is 2222 counts of high severity, accounting for over 20% of the logs now. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| No, nothing suspicious |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| It seems like a normal amount of failures is 10 and below. |
| --- |

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

| 35 failure events |
| --- |

* When did it occur?

| 8 AM |
| --- |

* 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 |
| --- |

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

| 196, 77 |
| --- |

* Who is the primary user logging in?

| user\_j |
| --- |

* When did it occur?

| 11 AM, 12 PM |
| --- |

* 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?

|  |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

|  |
| --- |

* What signatures stand out?

| * A user account was locked out * An attempt was made to reset an account’s password |
| --- |

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

| * 1-2 AM * 9-10 AM |
| --- |

* What is the peak count of the different signatures?

| * 896 * 1,258 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |

* Which users stand out?

| * user\_a * user\_k |
| --- |

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

| * 1-2 AM * 9-10 AM |
| --- |

* What is the peak count of the different users?

| * 984 * 1,256 |
| --- |

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

* Does anything stand out as suspicious?

|  |
| --- |

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

| * 2,128 An attempt was made to reset an account’s password * 1,811 A user account was locked out |
| --- |

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

* Does anything stand out as suspicious?

| * User\_k * user\_a |
| --- |

* 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?

| Can’t see trending data to reference to determine if there is unusual activity and data trend outliers |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes - POST |
| --- |

* What is that method used for?

| POST - sending data to server |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| <http://tuxradar.com> is new and not on the previous logs raising suspicions of its activity. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| 404 Not Found error increased significantly by over 400 counts |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes, significant increase in activity out of Ukraine |
| --- |

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

| * 877 counts at 8 PM |
| --- |

* 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 |
| --- |

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

| 1,296 |
| --- |

* When did it occur?

| Mar 25,2020 8 pm |
| --- |

* 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?

| There was a large spike in POST usage. |
| --- |

* Which method seems to be used in the attack?

| POST |
| --- |

* At what times did the attack start and stop?

| 3/25/2020 from 7 pm to 9pm |
| --- |

* 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?

|  |
| --- |

* 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?

| 439 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

|  |
| --- |

* What URI is hit the most?

| VSI Account log on is significantly higher than the others |
| --- |

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

| Brute force attack |
| --- |

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