| 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 were more severity levels in the “high” category than almost 95% “informational” that was seen before the attack. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Yes, there were more successes than failures after the attack. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes |
| --- |

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

| 35 |
| --- |

* When did it occur?

| 8am - 03/25/2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes. It exceeded our threshold. |
| --- |

* 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 |
| --- |

* Who is the primary user logging in?

| user\_j |
| --- |

* When did it occur?

| 11am - 03/25/2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes. It exceeded our threshold of 10. |
| --- |

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

| Yes, we would increase our threshold from 10 to 25. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| No. We did not not because our threshold was set to >25. |
| --- |

**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 accounts password” |
| --- |

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

| “A user account…” - 1:40am to 2:40am  “An attempt…” - 9:10am to 11am |
| --- |

* What is the peak count of the different signatures?

| “A user account…” - 785  “An attempt…” - 397 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| yes |
| --- |

* Which users stand out?

| User\_A |User\_K |
| --- |

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

| User\_A 1:40am - 2:40am | User\_K 9:10am - 11:00am |
| --- |

* What is the peak count of the different users?

| User\_A 785 | User\_K 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 |
| --- |

**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?

| An advantage is that it is very easy to see outliers and which user it was right away. A disadvantage would be that we cannot see the time and how long each attack took place for on the bar graph, only 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. There were far more POSTs. |
| --- |

* What is that method used for?

| POST is used to send data to a server to create/update a resource |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| No |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes, “404” went from 2% to 15%. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes |
| --- |

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

| 8:00 pm - 9:00 pm |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| No our threshold was accurate |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes had 1296 in one hour |
| --- |

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

| 8:00 pm - 9:00 pm |
| --- |

* When did it occur?

| March 25th |
| --- |

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

| No our threshold was accurate |
| --- |

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

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which method seems to be used in the attack?

| GET | POST |
| --- |

* At what times did the attack start and stop?

| GET 5:00pm -7:00pm | POST 7:00pm - 9:00pm |
| --- |

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

| GET - 729  POST - 1,296 |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| yes |
| --- |

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

| The city of Kiev, Ukraine had a high volume of activity.  The city of Kharkiv, Ukraine had a high volume of activity.  The city of Washington D.C, United States had a high volume of activity.  The city is New York City, United States had a high volume of activity. |
| --- |

* What is the count of that city?

| Kiev - 439  Kharkiv - 433  D.C. - 714  NYC - 549 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes |
| --- |

* What URI is hit the most?

| /VSI\_Account\_logon.php |
| --- |

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

| A Brute Force Attack. |
| --- |

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