| 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?

| There were over 1000 “high” severity cases compared to the baseline of 320ish “high” severity cases. The additional attacks seem to have occurred between 1am-3am and 9am-11am. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| There were a significant number of failed activities between 8am-9am. About 5-6 times the normal expected numbers. |
| --- |

**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 events |
| --- |

* When did it occur?

| 8am-9am |
| --- |

* Would your alert be triggered for this activity?

| Yes, our alert was 28 in an hour |
| --- |

* 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 |
| --- |

* 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?

| Yes, significantly less accounts deleted. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Significant user account lockouts at 12am-3am. Reset passwords were up from 8am-11am. |
| --- |

* What signatures stand out?

| User account lockouts and reset password requests |
| --- |

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

| 12am-3am for user lockouts and 8am-11am for reset password requests |
| --- |

* What is the peak count of the different signatures?

| 896 events for user lockouts and 1258 reset password requests. |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes |
| --- |

* Which users stand out?

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

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

| 12am-3am for User\_A and User\_K is 8am-11am |
| --- |

* What is the peak count of the different users?

| 984 events for User\_A and User\_K is 1256 |
| --- |

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

* Does anything stand out as suspicious?

| Yes, there were accounts locked out between 1-2am and the password request count was at 9am-10am. |
| --- |

* 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, User\_A and User\_K have significantly more events. |
| --- |

* 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?

| The advantages are showing the total event amounts for each suspicious user and giving a general timeline for their attempts. This allows future planning of when attacks may occur. This also allows you to find specific users that are carrying out the attacks. Disadvantages would be the report not being sent every hour, as the attacks tend to take several hours and you normally get a report every day or once a week. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| POST |
| --- |

* What is that method used for?

| 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?

| 404 error code had a significant increase. |
| --- |

**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?

| 939 events between 8pm-9pm |
| --- |

* Would your alert be triggered for this activity?

| Yes, the threshold was set at >140. |
| --- |

* 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?

| 1296 events |
| --- |

* When did it occur?

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

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

| No, Charles is too op for this class. |
| --- |

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

* Does anything stand out as suspicious?

| GET at 6pm and POST at 8pm |
| --- |

* Which method seems to be used in the attack?

| GET and POST |
| --- |

* At what times did the attack start and stop?

| The attack started at 5pm and ended at 9pm |
| --- |

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

| POST count was 1296. |
| --- |

**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.)

| Kiev, Ukraine & Kharkiv, Ukraine |
| --- |

* What is the count of that city?

| 433 for Kharkiv and 439 for Kiev |
| --- |

**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?

| Brute Force Attack. |
| --- |

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