| 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 a very large change in two specific signatures raising the severity of the situation very quickly. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Yes, there was a suspicious amount of failed activities in a 1 hr window early in the morning |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes, the alert threshold was triggered for a 1 hr span of time. |
| --- |

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

| There were 35 failed events in the 1 hr time period. |
| --- |

* When did it occur?

| These activities took place some time between 8am and 9am. |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| I believe the threshold that was set to be adequate for the situation. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes there was a suspicious level of successful logins. |
| --- |

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

| Two different 1 hr time spans yielded suspicious counts. One at 196, the other at 77. |
| --- |

* Who is the primary user logging in?

| User J |
| --- |

* When did it occur?

| The two hours in which suspicious levels of logins occurred were between 11:00 am and 1:00 pm. |
| --- |

* Would your alert be triggered for this activity?

| Yes. |
| --- |

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

| I believe the threshold we chose was adequate for the situation. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| No |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes, there seem to be several signatures that stand out as suspicious activity. |
| --- |

* What signatures stand out?

| The signatures for a user account being locked out, and attempts made to reset a password were both suspicious. |
| --- |

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

| The account lockouts occurred between 1:00 am and 3:00 am. The password reset attempts occurred between 9:00 am and 11:00 am. |
| --- |

* What is the peak count of the different signatures?

| The account lockouts peaked at 896, and the password resets peaked at 1,258. |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| OTHER user had the most events logged (95) before the attack log. After the attack log user\_k had the most events logged (1,256). |
| --- |

* Which users stand out?

| user\_a, user\_k adn user\_j |
| --- |

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

| user\_a: Begin - 12:00 a.m. Stop - 3:00 a.m.  user\_k: Begin - 8:00 a.m. Stop - 11:00 a.m.  user\_j: Begin - 10:00 a.m. Stop - 1:00 p.m. |
| --- |

* What is the peak count of the different users?

| 1,256 |
| --- |

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

* Does anything stand out as suspicious?

| Yes, a user account was locked out at 1:00 a.m. - 805 events, at 2:00 a.m. - 896 events. An attempt was made to reset an accounts password at 9:00 a.m. - 1,258 events and 10:00 a.m. - 761 events. After that, an account was successfully logged on at 11:00 a.m. - 196 events and at 12:00 a.m. - 77 events. |
| --- |

* 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?

| Some advantages are that they can point out specific anomalies in the data in a way that is more visually apparent. A disadvantage would be that it is more difficult to plot that data on a coherent timeline in one smooth graphic. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes, there was a suspicious amount of GET requests, while the POST requests were abnormally small in comparison to GET requests. |
| --- |

* What is that method used for?

| GET requests are for fetching data. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Nothing that seemed suspicious or out of the ordinary. There were insignificant changes. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| There was a significant increase for the HTTP response codes 301, 304, and 404. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes there was 1 IP address that contributed a large amount of traffic. |
| --- |

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

| At 8:00 PM |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| Maybe lower it, otherwise the current threshold is fine. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes on 03/25/2020 there was a large amount of POST requests well over the threshold that would be set. |
| --- |

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

| This occurred on 03/25/2020 at 8:00 PM |
| --- |

* When did it occur?

| 03/25/2020 |
| --- |

* 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?

| Yes, on 3/25/2020 at 6:00pm there was a large increase in GET responses, and at 8:00pm on the same day there was a large increase in POST responses. |
| --- |

* Which method seems to be used in the attack?

| SQL Injection |
| --- |

* At what times did the attack start and stop?

| Between 8:00pm and 9:00pm |
| --- |

* 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?

| Yes there was a spike in GET requests at 6:00PM and A spike in POST requests at 8:00PM |
| --- |

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

| Kiev, Ukraine and Kharkiv, Ukraine. |
| --- |

* What is the count of that city?

| Kiev - 439 Kharkiv - 433 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes, there are a couple of URI’s with suspicious counts. |
| --- |

* What URI is hit the most?

| The /VSI\_Account\_logon.php is hit the most with 1,296 times accessed at 8:00pm. |
| --- |

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

| This could potentially be a brute force attack. |
| --- |

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