|  |
| --- |
| 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 prior report had an ‘informational’ count of 4429 and a ‘high’ count of 329 whereas the new report shows ‘informational’ count at 4381 and ‘high’ at 1111 |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| Yes, there were less failed activities after the attack occurred with the prior failure count at 142 and the new count at 93 |

**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?

|  |
| --- |
| Mar 25, 2020 8:00 AM – 9:00 AM |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes |

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

|  |
| --- |
| No, the next highest event had a count of 8 and our threshold was 14 |

**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?

|  |
| --- |
| Less than 500 |

* Who is the primary user logging in?

|  |
| --- |
| User\_j |

* When did it occur?

|  |
| --- |
| Mar 25, 2020 10:00 AM – 11:00AM |

* 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?

|  |
| --- |
| No |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes |

* What signatures stand out?

|  |
| --- |
| 1. A user account was locked out and, 2. An attempt was made to reset an accounts password |

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

|  |
| --- |
| 1. 12:00 am – 3:00 am 2. 8:00 am – 11:00 am |

* What is the peak count of the different signatures?

|  |
| --- |
| 896 and 1,258 |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes, 2 users were primarily active during each suspicious activity |

* Which users stand out?

|  |
| --- |
| User\_a and User\_k |

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

|  |
| --- |
| User\_a activity was between 12:00 am – 3:00 am  User\_k activity was between 8:00 am – 11:00 am |

* What is the peak count of the different users?

|  |
| --- |
| User\_a peak count was 984  User\_k peak count was 1,256 |

**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?

|  |
| --- |
| This report provides and easy way to see the correlation between the user activity during the time of the suspicious events and while statistics can often provide us with precise numerical data it can also be hard to see the overlapping correspondence |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

|  |
| --- |
| Yes, the POST method |

* What is that method used for?

|  |
| --- |
| POST method is used for sending data to a server to create or update a resource |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| Yes, web traffic from them went down significantly |

**Report Analysis for HTTP Response Codes**

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

|  |
| --- |
| Yes, successful response code (200) numbers went down by more than half as well as the “not modified” code (304) and “moved permanently” code (301), while “not found” responses (404) went up and |

**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 |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes |

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

|  |
| --- |
| No, our threshold was >130 and the closest event was 120 |

**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 8:00 pm – 9:00 pm |

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

|  |
| --- |
| No, our threshold was set for 12 and prior to the suspicious activity there was nothing greater than 7 |

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

* Does anything stand out as suspicious?

|  |
| --- |
| Yes |

* Which method seems to be used in the attack?

|  |
| --- |
| POST |

* At what times did the attack start and stop?

|  |
| --- |
| 7:00 pm – 9:00 pm |

* 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 |

* 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?

|  |
| --- |
| Yes |

* What URI is hit the most?

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

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

|  |
| --- |
| The attacker could be launching a Brute Force Attack |

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