|  |
| --- |
| 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 is an increase in severity. Before now High severity was 6.91% but, it has jumped to 20.22%] |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| [Yes the percentage changed from success: 97.02%, failure: 2.98% to success: 98.44%, failure: 1.56%. Going by these changes there is no major change in overall failure of events] |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

|  |
| --- |
| [Yes, I detected some suspicious activity for failed activity between 8am and 9am on wednesday 25th March 2020] |

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

|  |
| --- |
| [35 events] |

* When did it occur?

|  |
| --- |
| [March 25 2020] |

* Would your alert be triggered for this activity?

|  |
| --- |
| [Yes because our threshold was set to alert when greater than 20] |

* 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?

|  |
| --- |
| [94 Events] |

* Who is the primary user logging in?

|  |
| --- |
| [User A] |

* When did it occur?

|  |
| --- |
| [2AM] |

* 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 suspicious was detected] |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

|  |
| --- |
| [Yes] |

* What signatures stand out?

|  |
| --- |
| [A user account lockout 34.003%  Attempt was made to reset a user password 39.955%  An account was successfully logged on 8.111%] |

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

|  |
| --- |
| [A user account lockout; from 1AM to 3AM on March 25  Account successfully logged on; from 11AM to 1PM on March 25  An attempt was made to reset a user password; from 9AM to 11AM on 25 March] |

* What is the peak count of the different signatures?

|  |
| --- |
| [Peak for a user account lockout was 896 counts  Peak for an account successfully logged on was 196 counts  Peak for an Attempt was made to reset a user password was 1258 counts ] |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |
| [Yes] |

* Which users stand out?

|  |
| --- |
| [Users A, J and K] |

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

|  |
| --- |
| [User A: 1AM to 3Am March 25  User J: 11AM to 1PM March 25  User K: 9AM to 11AM March 25] |

* What is the peak count of the different users?

|  |
| --- |
| [User A: 984  User J: 196  User k: 1265] |

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

* Does anything stand out as suspicious?

|  |
| --- |
| [No] |

* 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?

|  |
| --- |
| [No] |

* 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?

|  |
| --- |
| [Statistical chart is easier to read because it contains the total count of users activity or the percentage of the activity. However, statistical charts do not show much details when compared to other charts such as bar chart, pie chart, line chart etc] |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

|  |
| --- |
| [Yes] |

* What is that method used for?

|  |
| --- |
| [HTTP Post method] |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| [No significant changes were detected] |

**Report Analysis for HTTP Response Codes**

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

|  |
| --- |
| [Yes, 404 response code increased from 2% to 15%. On the other hand, 200 response code dropped from 91% to 83%] |

**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?

|  |
| --- |
| [Activity from Ukraine was detected between 8PM and 9PM on 25th March. Total count of event was 935] |

* Would your alert be triggered for this activity?

|  |
| --- |
| [I set my threshold at 200 so it would have triggered an alert] |

* 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, between 8PM and 9PM March 25 there was activity in the HTTP Post method ] |

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

|  |
| --- |
| [1296 Counts of events] |

* When did it occur?

|  |
| --- |
| [Between 8PM and 9PM] |

* 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] |

* Which method seems to be used in the attack?

|  |
| --- |
| [Get method and Post method] |

* At what times did the attack start and stop?

|  |
| --- |
| [Get method was used from 6PM and stopped at 7PM  Post method was used from 8PM and stopped at 9PM] |

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

|  |
| --- |
| [Get method peak was 729 counts  Post method peak was 1296] |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

|  |
| --- |
| [Yes, from Ukraine] |

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

|  |
| --- |
| [Kiev, Kharkiv and Lvov] |

* What is the count of that city?

|  |
| --- |
| [Kiev: 439 counts  Kharkiv: 433 counts  Lvov: 5 counts] |

**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?

|  |
| --- |
| [Most likely a brute force attack ] |

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