|  |
| --- |
| 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, we did detect suspicious changes in severity.  Severity Report Attack Report |
| Informational 4429 counts / 93% à 4381 counts / 80%  High 329 counts / 7% à 1111 counts / 20%  Too dramatic increase for High counts |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| Yes, we did detect suspicious changes in failed activities. |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

|  |
| --- |
| Yes, we did detect a suspicious volume of activity. |

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

|  |
| --- |
| The event count was 35. |

* When did it occur?

|  |
| --- |
| The occurrence happened on March 25, 2022 at 8:00 am. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes, our alert would be triggered as it was set for 5 and above. |

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

|  |
| --- |
| Yes, we would increase the threshold to 12. |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

|  |
| --- |
| Yes, we did detect a suspicious volume of successful logins. |

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

|  |
| --- |
| We noticed the following counts with the associated times:  965 events @ 1:00 am  1005 events @ 2:00 am  1293 events @ 9:00 am  784 events @ 10:00 am |

* Who is the primary user logging in?

|  |
| --- |
| We noticed < User k > was the primary user logging in with 2114 counts. |

* When did it occur?

|  |
| --- |
| The occurrence happened at 9:00 am on Wed, March 25,2020. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes, our alert was triggered for this activity as it was set at 215. |

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

|  |
| --- |
| No, we would not because our alert was triggered above our threshold. |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

|  |
| --- |
| No, we did not detect a suspicious volume of deleted accounts. There were no urgent concerns with a threshold of 15 and at 5am there were 17 accounts deleted. |

**Dashboard Analysis for Time Chart of Signatures user**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes. |

* What signatures stand out?

|  |
| --- |
| Three signatures stand out:  1. an attempt was made to reset an accounts password  2. a user account was locked out  3. an account was successfully logged on |

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

|  |
| --- |
| 1. From 8:00 am to 11:00 am: an attempt was made to reset an accounts password 2. From 12:00 am to 3:00 am: a user account was locked out 3. From 10:00 am to 1:00 pm: an account was successfully logged on   An account was successfully logged on |

* What is the peak count of the different signatures?

|  |
| --- |
| 1. The peak account was at 9:00 am with 1258 an attempt was made to reset an accounts password 2. The peak account was at 2:00 am with 896 a user account was locked out 3. The peak account was at 11:00 am with 196 an account was successfully logged on |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes, something is afoot! |

* Which users stand out?

|  |
| --- |
| The following 2 Users stands out:   * User\_a * User\_k * User\_j |

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

|  |
| --- |
| The following begin and stop time for each user:   * User\_a 12:00 am to 3:00 am * User\_k 8:00 am to 11:00 am * User\_j 10:00 am to 1:00 pm |

* What is the peak count of the different users?

|  |
| --- |
| The peak count for each user is as follows:  User\_a - 984  User\_k – 1256  User\_j - 196 |

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

* Does anything stand out as suspicious?

|  |
| --- |
| Yes, we noticed:   * A user account was locked out occurred: 1811 times. * A account reset account password occurred: 2128 times. * A successfully logged on occurred: 432 time. |

* Do the results match your findings in your time chart for signatures?

|  |
| --- |
| No, they do not match but are very similar (off by approximately 100 for each one: Account was locked / Attempt was made which is equal to .05%. |

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

* Does anything stand out as suspicious?

|  |
| --- |
| Yes we did notice suspicious activity.   * User\_a was locked out 1878 times * User\_k reset account password 2118 times * And User\_j logged in 398 times. |

* Do the results match your findings in your time chart for users?

|  |
| --- |
| The results are Similar/Off by approximate 100 counts each. |

**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 with the Pie chart and Bar chart is that both provide a total number, while the lines chart does not.  The advantage of the line chart is that it provides a visual representation of the progression of the attack and when the peak occurred. |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

|  |
| --- |
| Yes, we detected suspicious changes in the HTTP methods. POST has increased from 106 to 1324 counts. |

* What is that method used for?

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

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| Yes it was suspicious as the was reduced to 1442 events from 6437 events |

**Report Analysis for HTTP Response Codes**

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

|  |
| --- |
| Yes 404 has been increased by 15% (from 207 to 679) compare to 2.12% percent |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

|  |
| --- |
| After excluding the US, we did detect suspicious volume of international activity. |

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

|  |
| --- |
| We noticed 730 counts at 6:00 pm and again 1415 counts at 8:00 pm. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes, as our alert would be triggered was set at 140. |

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

|  |
| --- |
| No we would not change the threshold we selected. |

**Alert Analysis for HTTP POST Activity**

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

|  |
| --- |
| Yes, we detected suspicious volume of HTTP POST activity. |

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

|  |
| --- |
| It occurred at 8:00 pm with 1296 counts. |

* When did it occur?

|  |
| --- |
| The suspicious volume increase of HTTP POST occurred on March 25 ,2020 at 8:00 pm. |

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

|  |
| --- |
| No, we set our threshold at 4 and the alert was triggered. |

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

* Does anything stand out as suspicious?

|  |
| --- |
| Significantly! |

* Which method seems to be used in the attack?

|  |
| --- |
| POST and GET were the methods used in this attack. |

* At what times did the attack start and stop?

|  |
| --- |
| The GET attacked occurred from 5:00 pm -7:00 pm.  The POST attacked occurred from 7:00 pm -9:00 pm. |

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

|  |
| --- |
| GET attacked peaked at 6:00 pm with 729 counts.  POST attack peaked at 8:00 pm with 1296 counts. |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

|  |
| --- |
| We noticed the increase of density change of a few countries. |

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

|  |
| --- |
| We noticed Japan, India, and El Salvadore having an increase in volume activity.  After further analisys we discovered Ukrain had high volume of activity as well. |

* What is the count of that city?

|  |
| --- |
| After diving into each country, we noticed the respective cities with their respective increase counts: Tokyo 26, New Delhi 22 (17 unknown +5 known), and with San Salvador at 34 counts.As further analysis showed Kiev- 438 and Kharkiv – 432 . |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

|  |
| --- |
| Yes. The high activity on the VSI\_Account\_logon.php page and on the /files/logstash/logstash-1.3.2-monolithic.jar |

* What URI is hit the most?

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

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

|  |
| --- |
| The attacker is potentially login onto the system and is collecting data and is piping information to them that they collected. This is realized by using pipelines, which contain input, filter and output modules. The service gets interesting when having a compromised a machine which is running Logstash as a service. |

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