| 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 high severity increased from 6 percent to 20 percent. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| There was a change in the failed activities.The number of failed activities decreased. Based on the analysis, the original log file percent was 2.98 and the attack log percent was 1.56.As a result it wasn't a major change. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Based on the comparison of both log files there is no evidence of suspicious volume in failed activities. It wasn't a significant change. |
| --- |

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

| 35 events |
| --- |

* When did it occur?

| 8:00 am Wednesday March 25,2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes our alert would have triggered because it is set to anything greater than 15 |
| --- |

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

| I would not change the threshold as it was set low enough to be triggered by this attack and high enough that we are not getting false positives during the hours of attack resulting in an alert fatigue. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes there was a suspicious volume of successful logins that occurred. The events would range from 11 to 20 in the original log file and there was 196 events that occurred in 1 hour in the attack log file. |
| --- |

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

| There were 196 events in an hour. |
| --- |

* Who is the primary user logging in?

| User j |
| --- |

* When did it occur?

| 11:00 am Wednesday March 25,2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes, our alert would have been triggered which was anything over 25. |
| --- |

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

| Yeah I would change it to a 50 threshold instead. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| No it wasn't an excessive volume of deleted accounts. The total amount of deleted accounts in the attack logs is similar to the original log but decreased in the attack log. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes,the time chart for the windows server was higher for the signature others in the original log file than the attack log file. There was suspiciousness found in two signatures in the attack log file. |
| --- |

* What signatures stand out?

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

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

| 1.March 25,2020 Wednesday 12:00am -3:00am  2.March 25,2020 Wednesday 8:00am -11:00am |
| --- |

* What is the peak count of the different signatures?

| 1.896  2.1258 |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes there were two users that showed suspiciousness which their accounts are compromised. |
| --- |

* Which users stand out?

| 1.user\_a  2.user\_k |
| --- |

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

| 1.12:00am-3:00am  2.8:00am-11:00am |
| --- |

* What is the peak count of the different users?

| 1.984  2.1256 |
| --- |

**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?

| Advantages:The reports may be adjusted to display certain data, and visualizations can be made for easier analysis.Enables you to further improve and adjust it over time to get various insights from your data after saving the report.  Disadvantages:Reports are usually not as engaging as other user panels and are instead messy visuals.seeing the data in a multiple-time mode is not available and breaking it down the information on your preference. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes the posts requests increased significantly and Get requests decreased slightly after the attack. |
| --- |

* What is that method used for?

| GET is one of the available request methods for the HTTP protocol.It is put to use for getting information from a certain resource. It does nothing except get the data from the server and does not perform any other functions.  PUT is one of the request methods for HTTP protocol.It is used to transmit data to the server so that resources may be created.The information that is provided in the request body is also included. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Yes, the share of the top referres has changed as new domains appear in the attack log. The count also decreased significantly. These shifts showcase a change in traffic that can be connected with the attack. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes. There is a significant decrease in the number of 200 responses an significant increase in the number of 404 responses |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes the number of events is higher than any other time from both logs |
| --- |

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

| 1415 |
| --- |

* Would your alert be triggered for this activity?

| Yes my alert would've been triggered which was anything over 160. |
| --- |

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

| No, our threshold was accurate. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes, the total number of http post requests is higher than any other time of day on an hourly basis. |
| --- |

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

| 1296 |
| --- |

* When did it occur?

| The HTTP post activity occurred at 8:00pm Wednesday March 25,2020 |
| --- |

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

| No, I would not change since it triggered successfully. |
| --- |

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

* Does anything stand out as suspicious?

| Yes, the HTTP post is utilized significantly during the attack. Get was also used. |
| --- |

* Which method seems to be used in the attack?

| HTTP POST method |
| --- |

* At what times did the attack start and stop?

| The attack started at 7:00 pm and finished at 9:00pm on March 25,2020 |
| --- |

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

| 1296 |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| Yes there is a significant amount in the United States and Ukraine |
| --- |

* 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?

| 454 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| yes |
| --- |

* What URI is hit the most?

| VIS\_Account\_Logon.php |
| --- |

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

| This indicates that the user is attempting to obtain access into the account. A brute force attack which is when the user tries to guess the password of the target. A high number of requests for a Post shows that the user wants to send data to the server. |
| --- |

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.