| 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 percentage of cases with high severity rose from 6% to 20%. |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| The unsuccessful attempts got a modification. There were fewer unsuccessful attempts. The analysis showed that the assault log percent was 1.56 and the original log file percent was 2.98.Thus, it wasn't a significant change. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| There is no sign of a suspicious amount of unsuccessful activities, according to a comparison of the two log files. It wasn't a big change. |
| --- |

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

| 35 events |
| --- |

* When did it occur?

| 8:00 AM March 25, 2020 on Wednesday |
| --- |

* Would your alert be triggered for this activity?

| Yes it would have been since it was set to 13 |
| --- |

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

| Yes because it’s a little low I would rather it be around 15-16 to prevent false positives but other than that It’s fine |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes, there seemed to be a suspiciously high number of successful login attempts. There were 196 events that took place in one hour in the attack log file, with the events ranging from 11 to 20 in the original log file. |
| --- |

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

| 196 events in 1 hour |
| --- |

* Who is the primary user logging in?

| User j |
| --- |

* When did it occur?

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

* Would your alert be triggered for this activity?

| Yes since our threshold was set at 19 |
| --- |

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

| Same as before I would’ve just changed it to a higher threshold like 45-50 to prevent false positives |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| No, there weren't a lot of accounts that were removed. The overall number of deleted accounts in the attack logs is less than in the original log but is still similar. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes, the Windows server's time chart for the signature was longer. more people in the attack log file than in the original log file. In the attack log file, two signatures were identified to be questionable. |
| --- |

* 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, two users who displayed suspicious behavior had their accounts 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: Data can be shown differently in reports, and visualizations can be created to make analysis simpler. allows you to save the report and then go back and make changes as needed to gain more insights from your data.  Cons: Reports are typically cluttered visuals rather than user panels that are equally engaging.It is not possible to see the data in a multiple-time mode or to break it down according to what you want to see. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes, following the attack, there was a noticeable spike in post requests and a little decrease in get requests. |
| --- |

* What is that method used for?

| One of the HTTP protocol's many request methods is GET. It is used for getting data from a certain source. It does not carry out any additional tasks other than obtaining the data from the server.  One of the HTTP protocol's request methods is PUT.Data is sent to the server using it so that resources can be generated. Included is the data that is supplied in the body of the request. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| Yes, as new domains show up in the attack log, the percentage of the top referrers has shifted. Additionally, there was a notable decline in the count. These changes demonstrate a shift in traffic that may be related to the attack. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Yes. The number of responses has significantly decreased for 200, while the number of responses has significantly increased for 404. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes, according to both logs, there are more events than at any previous period. |
| --- |

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

| 1415 |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| definitely yes threshold is set at 0 which doesn’t make sense maybe around 150 |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes, on an hourly basis, there are more http post requests than at any other time of day. |
| --- |

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

| 1296 |
| --- |

* When did it occur?

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

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

| no it would have triggered |
| --- |

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

* Does anything stand out as suspicious?

| Yes, a large portion of the attack involves the use of the HTTP post. 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?

| On March 25, 2020, the attack began at 7:00 p.m. and ended at 9:00 p.m. |
| --- |

* 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 are large amounts in both Ukraine and the United States |
| --- |

* 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 suggests that the user is making an effort to log into the account. a brute force attack, in which the user attempts to guess the target's password. A large volume of Post requests indicates that the user wishes to communicate information to the server. |
| --- |

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