| Cybersecurity |
| --- |
| Project 3 Review Questions |

Make a copy of this document before you begin. Place your answers below each question.

## By: Matthew Forrest, Runa Frye, Miranda Bergman, Gary Oligschlaeger, Christopher Lexow, Joshua Bernstein

## 

## Windows Server Log Questions

### Report Analysis for Severity

* Did you detect any suspicious changes in severity?

| Yes, the High severity amount of events had nearly tripled from 6.91% to 20.22%  Before:    After: |
| --- |

### Report Analysis for Failed Activities

* Did you detect any suspicious changes in failed activities?

| Yes, failures dropped from 142 to 93(34.51% drop) while success increased from 4622 to 5856(26.73%) indicating a brute force attacker was successful in gaining access. |
| --- |

### 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?

| We had 35 counts of failed activity in one hour |
| --- |

* When did it occur?

| 8AM, March 25, 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes it would trigger the threshold |
| --- |

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

| We would change it from 7 to 10, this would limit the amount of false positives but still be able to trigger for suspicious activity. |
| --- |

### 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?

| The count levels were 23, 196, 77 |
| --- |

* Who is the primary user logging in?

| The primary user logging in was User\_j |
| --- |

* When did it occur?

| March 25 2020 10pm-12am |
| --- |

* Would your alert be triggered for this activity?

| Yes |
| --- |

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

| No, it is set at a good threshold |
| --- |

### Alert Analysis for Deleted Accounts

* Did you detect a suspicious volume of deleted accounts?

| No, it peaked at 17 at 5 am, March 25, 2020 but didn’t not cross the threshold or seem suspicious |
| --- |

### Dashboard Analysis for Time Chart of Signatures

* Does anything stand out as suspicious?

| There was a large increase in two Signatures: Attempt to reset account passwords and user account was locked out. |
| --- |

* What signatures stand out?

| The two Signatures that stood out were “Attempt to reset an account password” and “user account was locked out”. |
| --- |

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

| The attempt to reset account passwords occurred from 8:00AM-11:00AM and peaked at 9:00AM  The user account was locked out occurred from 12:00AM-3:00AM and peaked at 2:00AM  Both occurred March 25, 2020 |
| --- |

* What is the peak count of the different signatures?

| The peak count for attempt to reset account passwords was 1258. The peak count for user account was locked out 896 |
| --- |

### Dashboard Analysis for Users

* Does anything stand out as suspicious?

| There were two users that had an increase in activity. |
| --- |

* Which users stand out?

| User\_K and user\_A stood out among the other users. |
| --- |

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

| User\_K’s activity began at 8:00am and ended at approximately 11:00am.  User\_A’s activity began at 12:00am and ended at approximately 3:00am. |
| --- |

* What is the peak count of the different users?

| The peak activity for User\_k was 1256.  The peak activity for User\_a was 984. |
| --- |

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

* Does anything stand out as suspicious?

| Yes, the pie chart that was used to graph the Signatures shows an increase in two signatures. |
| --- |

* 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, the pie chart used to display the users shows an increase in two users |
| --- |

* 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?

| A statistical chart for Users would display the raw numbers corresponding with each user. It is an easy way to compare each value. The disadvantage of the statistical chart is it can be difficult to understand the significance of each number in relation to each other without a visual. |
| --- |

## 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 activity with the POST activity and GET activity. There was an increase in POST and a decrease in GET. |
| --- |

* What is that method used for?

| POST is typically used for username and password fields on a website.  GET is used to try and retrieve data |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| The count for the referer domain <http://semicomplete.com> and <http://www.semicomplete.com> dropped by a couple thousand. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| There was a significant decrease in HTTP response code 200 and an increase in response code 404. |
| --- |



**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?

| The count was 937 at 8:00pm March 25, 2020 |
| --- |

* Would your alert be triggered for this activity?

| Yes, the threshold for the alert was 120. |
| --- |

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

| No, the threshold limited the amount of false positives and remained effective. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes, there was a high volume of HTTP POST activity at 8PM on March 25, 202 |
| --- |

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

| 1296 |
| --- |

* When did it occur?

| 8:00pm on March 25, 2020 |
| --- |

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

| No, the threshold was low enough to catch suspicious activity but high enough to avoid false positives. |
| --- |

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

* Does anything stand out as suspicious?

| Significantly less HTTP GET activity, and dramatic increase in POST activity |
| --- |

* Which method seems to be used in the attack?

| POST activity, indicating a DDoS or Brute Force Attack |
| --- |

* At what times did the attack start and stop?

| The attack began at 7:00pm and ended at 9:00pm. |
| --- |

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

| The peak count of POST activity was 1296. |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| There was an increase in global access from Kharkiv, Ukraine. |
| --- |

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

| A high volume of activity was found in Kharkiv, Ukraine |
| --- |

* What is the count of that city?

| The count for Kharkiv was 432 |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| There was a large increase in VSI\_Account\_logon\_php |
| --- |

* 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 potentially be using a PHP code injection to attack VSI. |
| --- |

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