| 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. High severity went from 329 to 1111. Informational did not have any suspicious 4435 to 4483 changes.

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Failed = 142 to 93 (2.98% to 1.56% )  Success = 4622 to 5856 (1.4%)  Percentage of Failed activity was cut in half as percentage of total activities. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Threshold > 10  The number of failed windows activity events increased to 35 events at 8 am. |
| --- |

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

| There were 35 failed events in the hour it occurred (8:00 am) |
| --- |

* When did it occur?

| 8:00 am on Wednesday March 25 |
| --- |

* Would your alert be triggered for this activity?

| Yes, our threshold is greater than 10. |
| --- |

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

| No, our threshold was set correctly. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes we had a suspicious increase in volume of successful logins. |
| --- |

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

| 1293 |
| --- |

* Who is the primary user logging in?

| User\_k had 1256 logins and accounted for 97.138% of the successful logins at this time. The next highest was user\_c at 5 logins. |
| --- |

* When did it occur?

| 9 am on March 25 |
| --- |

* Would your alert be triggered for this activity?

| Yes. |
| --- |

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

| No, our alert would trigger for this event. |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| Threshold (>20) There was a suspicious drop in deleted accounts around 2 am, and a definite flatline from 9:15 am to 11:30 pm, one account showed deleted at 11:45 am, drop to zero and back to normal at noon. |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| Yes there were dramatic increases in attempts to reset an account password from 8:30 to 11:00 am. User accounts were locked out from 1 am to 2:30 am. Starting at 9 am on March 25.An account was successfully logged on at 11 am (count=100) |
| --- |

* What signatures stand out?

| A user account was locked out. An attempt was made to reset an accounts password. An account was successfully logged on. |
| --- |

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

| A user account was locked out. 1:30 am to 2:00 am  An attempt was made to reset an account’s password. 9:00 am to 10:30 am  An account was successfully logged on. 10:30 am to 12:00 pm |
| --- |

* What is the peak count of the different signatures?

| A user account was locked out (4740) - 795 events (1:30 am) preattack had a range of only 3 to 13.  An attempt was made to reset an accounts password (4726) - 1046 (9:30 am) preattack only had 2-11 attempts.  An account was successfully logged on (- 100 events (11:00 am) preattack had only 1-13 events. |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| Yes. User\_a and User\_k both had peaks above the normal range of all others. |
| --- |

* Which users stand out?

| User\_a and User\_k |
| --- |

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

| User\_a began at 1:30 am to 2:30 am. User\_k began at 9:00 am to 10:30 am. |
| --- |

* What is the peak count of the different users?

| User\_a: 796 (preattack peak was 12 at 6 am)  User\_k: 1046 (preattack peak was 12 at 2 am) |
| --- |

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

* Does anything stand out as suspicious?

| Yes. There are three areas that stand out: A user account was locked out (count=1811), An account was successfully logged on (count=432), An attempt was made to reset an accounts password (count=2128). |
| --- |

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

| Yes. The results match. |
| --- |

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

* Does anything stand out as suspicious?

| User\_a preattack count = 282; attack count = 1878  User\_k preattack count = 260; attack count = 2118 |
| --- |

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

| Yes, these finding match our time chart for users results. |
| --- |

**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?

| The dashboard visualizations help to highlight changes in the data, and the timeline allows us to view the trends and data anomalies. The statistical chart gives the underlying data to support what the visualization and trend lines are showing. The advantage is the statistical chart allows the build of the dashboard visualizations and viewing the granular user data; the disadvantage is it is hard to analyze the raw data. |
| --- |

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| There was a large increase in POST (from 106 pre-attack to 1324 during attack). GET decreased from 9851 to 3157. HEAD decreased from 42 to 15. OPTIONS stayed the same at 1. There were three attacker clientip addresses that showed even distribution of events (432) 79.171.127.34; 194.146.132.138; 194.105.145.147 |
| --- |

* What is that method used for?

| POST is used to send data to a server to create or update a resource. There were VSI\_Account\_logon.php POSTs 1323 times. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| One of the attacker clientip addresses also had 5 GET requests at 4:05 am on March 25, 2020 (194.105.145.147). |
| --- |

**Report Analysis for HTTP Response Codes**

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

| Code 404 tripled from 213 to 679. Most of that change was driven by client IP 208.91.156.11 with GET requests for log files. Also Code 200 showed VSI\_Account\_logon.php with 1322 attempts. It appears that the attacker was able to inject a .php file. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| During the attack, Ukraine was the highest 877 (34.774%). 864 was the peak. Pre-attack Ukraine was 1.464% (count=90). The United States had a peak of 691 (1975 was total for the entire day for the US). |
| --- |

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

| Peak: Ukraine March 25 at 7:30 to 8:30 pm ; United States March 25 5:30 - 6:30 |
| --- |

* Would your alert be triggered for this activity?

| Yes, it would have triggered. |
| --- |

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

| The threshold of 110 was fine; no need to change. |
| --- |

**Alert Analysis for HTTP POST Activity**

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

| Yes. |
| --- |

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

| There were 1296 POST activities |
| --- |

* When did it occur?

| March 25, 8:05:59 pm |
| --- |

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

Yes. We can increase our threshold slightly (from 7 to 10).

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

* Does anything stand out as suspicious?

| There was a large increase in GET (from 135 pre-attack max to 729 attack max (6:00 pm); POST increase pre-attack max was 7 to 1296 attack max (8:00 pm). |
| --- |

* Which method seems to be used in the attack?

| POST was the main method used in the attack, but there was also suspicious GET activity. |
| --- |

* At what times did the attack start and stop?

| GET 6:05:59 pm to POST 8:05:59 pm |
| --- |

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

| POST - 1296 |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| Ukraine showed up on the map, and there was an increase in activity in New York, NY. |
| --- |

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

| Ukraine was a new location, and had two cities with activity - Kyiv 194.105.145.147 (438) and Kharkiv 79.178.127.34 (432). |
| --- |

* What is the count of that city?

| Ukraine: Kyiv 194.105.145.147 (438) and Kharkiv 79.17.127.34 (432); United States: New York 194.146.132.138 (432) |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| Yes, the main files have changed. |
| --- |

* What URI is hit the most?

| /VSIAccount\_logon.php (1323 hits, 29.42%) |
| --- |

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

| The attacker is trying to inject a file. |
| --- |

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