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

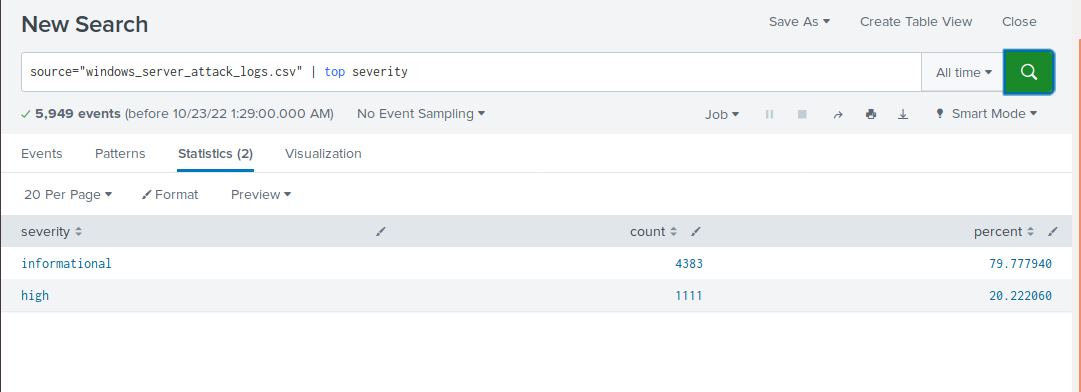
Make a copy of this document before you begin. Place your answers below each question.

## Windows Server Log Questions

**Report Analysis for Severity**

* Did you detect any suspicious changes in severity?

|  |
| --- |
| [Yes, looking at the logs, we can see changes in both **Informational** and **High** severity categories. High went from 7 percent to 20 percent, which shows a 13 percent increase. These changes in severity are suspicious. Please see the screenshots below for reference.] |



**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| [Success rate went from 97 percent to 98 percent, and failure went from 3 percent to 2 percent. I do not consider this change suspicious. Please see the screenshots below for reference.      ] |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

|  |
| --- |
| [Looks like there is a large volume of suspicious activity on March 25 at 8 am in the Windows attack logs. Please see the screenshots below for reference.    ] |

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

|  |
| --- |
| [35 events during that hour] |

* When did it occur?

|  |
| --- |
| [At 8 am] |

* Would your alert be triggered for this activity?

|  |
| --- |
| [Yes, the alert would be activated.] |

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

|  |
| --- |
| [No.] |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

|  |
| --- |
| [At 11 am on March 25, 2020, multiple successful logons] |

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

|  |
| --- |
| [196 at 11 am] |

* Who is the primary user logging in?

|  |
| --- |
| [**user\_j**  ] |

* When did it occur?

|  |
| --- |
| [at 11 am on March 25] |

* Would your alert be triggered for this activity?

|  |
| --- |
| [Yes, the alert would be triggered] |

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

|  |
| --- |
| [No.] |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

|  |
| --- |
| [The number of deleted accounts went from 318 to 131, I do not consider it suspicious.    ] |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

|  |
| --- |
| [We see two suspicious spikes in activities on March 25th.      One of the spikes shows user account being locked out multiple times.  ] |

* What signatures stand out?

|  |
| --- |
| [Signatures are: user account locked out, see the screenshot above, and an attempt to reset the account password] |

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

|  |
| --- |
| [Account was locked out from 12 am to 3 am on March 25, and an attempt was made to reset the account password between 8 am and 11 am on the same day.] |

* What is the peak count of the different signatures?

|  |
| --- |
| [896 for user account locked out, and ,258 for the attempt to reset the account password] |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

|  |
| --- |
| [Both these activities look suspicious.] |

* Which users stand out?

|  |
| --- |
| [**user\_k** looks suspicious for the 1,255 attempts to reset the account password, and **user\_a** looks suspicious for 896 cases of a user account being locked out. Please see the screenshots below.    ] |

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

|  |
| --- |
| [**user\_a** activity started at 12 am and ended at 3 am on March 25, 2020  **user\_k** activity started at 8 am and ended at 11 am on the same day] |

* What is the peak count of the different users?

|  |
| --- |
| [user\_a peak count is 896, user\_k count is 1,258] |

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

* Does anything stand out as suspicious?

|  |
| --- |
| [There was suspicious activity from 12 am to 3 am on March 25, 2020, and again from 8 am to 11 am on the same day.    here] |

* 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?

|  |
| --- |
| [We see spikes of suspicious activity at 1 am and then at 2 am for user\_a; then we see spikes of suspicious activity at 9 and 10 am for user\_k.  ] |

* 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?

|  |
| --- |
| [The advantage is a complete list of users with the numbers signifying the activity their accounts engaged in. The disadvantage is that it does not readily display the type of activities/events associated with the user account.  ] |

## 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 suspicious drop in GET requests, by 29 percent. And there was a suspicious increase in POST requests, by 29 percent. Please see screenshots below for reference.    ] |

* What is that method used for?

|  |
| --- |
| [POST requests are used to create or update a resource on the server.] |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| [No suspicious changes in referrer domains found. Please see the screenshots below.    ] |

**Report Analysis for HTTP Response Codes**

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

|  |
| --- |
| [There were some small changes, but the increase in 404 (Not Found) response code from 2 percent to 15 percent is worriesome.    ] |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

|  |
| --- |
| [Yes, there were 939 events at 8 pm on March 25.    answer here] |

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

|  |
| --- |
| [939 events.] |

* Would your alert be triggered for this activity?

|  |
| --- |
| [Yes.] |

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

|  |
| --- |
| [No] |

**Alert Analysis for HTTP POST Activity**

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

|  |
| --- |
| [Yes, there were 1,296 POST requests at 8 pm on March 25, which is suspicious.    ] |

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

|  |
| --- |
| [There were 1,296 requests] |

* When did it occur?

|  |
| --- |
| [At 8 pm on March 25, 2020] |

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

|  |
| --- |
| [No] |

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

* Does anything stand out as suspicious?

|  |
| --- |
| [There is suspicious activity with GET request from 5 pm to 7 pm on March 25, 2020, and POST request from 7 pm to 8 pm on the same day.      ] |

* Which method seems to be used in the attack?

|  |
| --- |
| [GET and POST requests seem to be used in these attacks.] |

* At what times did the attack start and stop?

|  |
| --- |
| [GET request attack started at 5 pm on March 25 and stopped at 7 pm on the same day; POST request attack started at 7 pm on March 25 and ended at 8 pm on the same day.] |

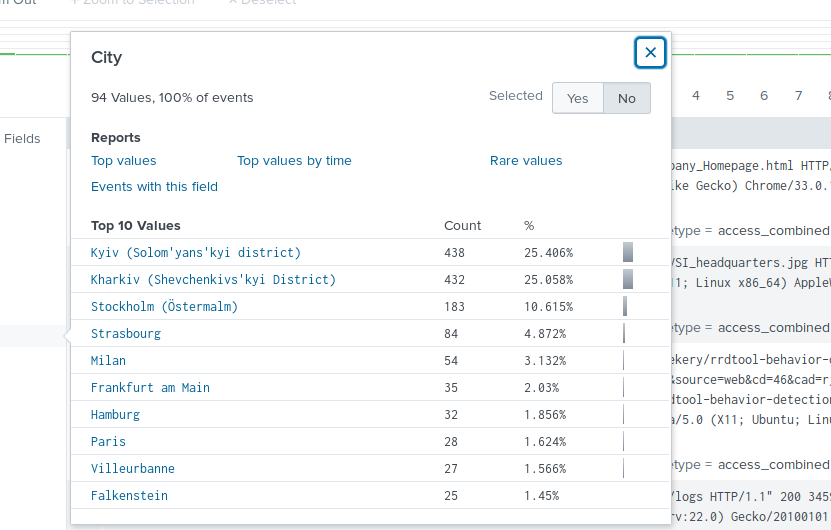
* What is the peak count of the top method during the attack?

|  |
| --- |
| [POST request peak count was 1,296 and GET request peak count was 729] |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

|  |
| --- |
| [There was suspicious activity in Ukraine, in the two cities, Kiev and Kharkiv.    ] |



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

|  |
| --- |
| [Ukraine, two cities: Kiev and Kharkiv] |

* What is the count of that city?

|  |
| --- |
| [Kiev – 438, Kharkiv - 432] |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

|  |
| --- |
| [First we need to check which URI are present and analyze how the patterns change between two Apache logs. We see that two URI, “/files/logstash/logstash-1.3.2-monolithic.jar”, and “/VSI\_Account\_logon.php”, have the most number of requests. Then we analyze these two URI and see that there was suspicious activity with the URI “/files/logstash/logstash-1.3.2-monolithic.jar” from 6 pm to 7 pm on March 25, and the URI “/VSI\_Account\_logon.php” on the same day from 8 pm to 9 pm.                ] |

* What URI is hit the most?

|  |
| --- |
| [URI “/VSI\_Account\_logon.php” was hit the most, with 1,296 requests] |

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

|  |
| --- |
| [The attacker might be using the brute force attack against the logon page of the company.] |

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