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

## Windows Server Log Questions

**Report Analysis for Severity**

source="windows\_server\_attack\_logs.csv" | top severity

* Did you detect any suspicious changes in severity?

|  |
| --- |
| Informational: went from 93% to 80%, resulting in a 13% decrease. Severity went from 7% to 20%, resulting in a 13% decrease. These results suggest there are suspicious changes in activity deemed as high severity. Such activities could include unauthorized access attempts, brute force attacks, malware detection and possible configuration changes. |

**Report Analysis for Failed Activities**

source="windows\_server\_attack\_logs.csv” | top status

* Did you detect any suspicious changes in failed activities?

|  |
| --- |
| Successful activities went from 97% to 98%, resulting in a 1% decrease. Failed activities went from 3% to 2%, resulting in a 1% decrease. These results suggest there were no major changes in failed activities. |

**Alert Analysis for Failed Windows Activity**

source="windows\_server\_attack\_logs.csv” status=failure

* Did you detect a suspicious volume of failed activity?

|  |
| --- |
| There was a suspicious volume of failed activity at 8am on March 25. Failed activities could include failed logons due to incorrect credentials, denied access to files / folders and windows service failing to start. |

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

|  |
| --- |
| The count of activity was 35 events during this hour. |

* When did it occur?

|  |
| --- |
| March 25 at 8am. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes. The alert threshold was set at 15, therefore the alert would be triggered. |

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

|  |
| --- |
| No change in the alert threshold is required. |

**Alert Analysis for Successful Logins**

source="windows\_server\_attack\_logs.csv" signature="An account was successfully logged on"

* Did you detect a suspicious volume of successful logins?

|  |
| --- |
| There was suspicious activity at 11am and 12pm on March 25. |

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

|  |
| --- |
| The count of activity is 196 events at 11am and 77 events at 12pm. |

* Who is the primary user logging in?

|  |
| --- |
| The primary user logging in was user j. |

* When did it occur?

|  |
| --- |
| The suspicious activities occurred at 11am and 12pm on March 25. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes. The alert threshold was set at 30, therefore the alert would be triggered. |

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

|  |
| --- |
| No change in alert threshold is necessary. |

**Alert Analysis for Deleted Accounts**

source="windows\_server\_attack\_logs.csv" signature=”A user account was deleted” OR USE

source="windows\_server\_attack\_logs.csv" signature\_id=4726

* Did you detect a suspicious volume of deleted accounts?

|  |
| --- |
| There were no signs of suspicious volumes of deleted accounts.  The alert threshold was set at 50, therefore the alert would be not triggered and the threshold was successful. |

**Dashboard Analysis for Time Chart of Signatures**

source="windows\_server\_attack\_logs.csv" signature="A user account was locked out" | timechart span=1h count by signature

source="windows\_server\_attack\_logs.csv" signature="An attempt was made to reset an accounts password" | timechart span=1h count by signature

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity within the signature “An account was locked out” from 1am to 3am on March 25.  There was suspicious activity within the signature “An attempt was made to reset an account password” from 9am to 11am on March 25. |

* What signatures stand out?

|  |
| --- |
| “A user account was locked out” stands out for high volume, which is suspicious activity.  “An attempt was made to reset an account password” stands out for high volume, which is suspicious activity. |

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

|  |
| --- |
| “A user account was locked out”: started at 1am on March 25 and stopped at 3am on March 25.  “An attempt was made to reset an account password”: started at 9am on March 25 and stopped at 11am on March 25. |

* What is the peak count of the different signatures?

|  |
| --- |
| “A user account was locked out”: peak count during the attack was at 896, at 2am.  “An attempt was made to reset an account password”: peak count during the attack was at 1258, at 9am. |

**Dashboard Analysis for Users**

source="windows\_server\_attack\_logs.csv" user=user\_a | timechart span=1h count by user

source="windows\_server\_attack\_logs.csv" user=user\_k | timechart span=1h count by user

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity from user\_a starting just after 12am and ending just before 3am on March 25.  There was suspicious activity from user\_k starting just after 8am and ending just before 11am on March 25. |

* Which users stand out?

|  |
| --- |
| user\_a: suspicious volume of activity; pre-attack total count of 282 events, post-attack total count of 1878. User\_a is responsible for the signature “An account was locked out”.  user\_k: suspicious volume of activity; pre-attack total count of 260 events, post-attack total count of 2118. User\_k is responsible for the signature “An attempt was made to reset an account password”  Post-attack stats and visualizations support this. |

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

|  |
| --- |
| user\_a starting just after 12am and ending just before 3am on March 25.  user\_k starting just after 8am and ending just before 11am on March 25. |

* What is the peak count of the different users?

|  |
| --- |
| user\_a: peak count was 984 at 2am.  user\_k: peak count was 1256 at 9am. |

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

source="windows\_server\_attack\_logs.csv" | top limit=20 signature

source="windows\_server\_attack\_logs.csv" signature="A user account was locked out" | timechart span=1h count by signature

source="windows\_server\_attack\_logs.csv" signature="An attempt was made to reset an accounts password" | timechart span=1h count by signature

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity within the signature “An account was locked out” for high volume. Pre-attack total was 309 which represented 7% of the total count, post-attack total was 1811 which represented 30% of the total count, an increase of 23%.  There was suspicious activity within the signature “An attempt was made to reset an account password” for high volume. Pre-attack total was 295 which represented 6% of the total count, post-attack total was 2128 which represented 36% of the total count, an increase of 30%. |

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

|  |
| --- |
| Yes, the results match the findings in the time chart for signatures. |

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

source="windows\_server\_attack\_logs.csv" | top limit=50 user

source="windows\_server\_attack\_logs.csv" user=user\_a | | timechart span=1h count by user

source="windows\_server\_attack\_logs.csv" user=user\_k | | timechart span=1h count by user

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity for user\_a for high volume. Pre-attack total was 282 which represented 6% of the total count; post-attack total was 1878 which represented 32% of the total count, increase of 26%.  There was suspicious activity for user\_k for high volume. Pre-attack total was 260 which represented 5% of the total count; post-attack total was 2118 which represented 36% of the total count, increase of 31%. |

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

|  |
| --- |
| Yes, the results match the findings in the time chart for signatures. |

**Dashboard Analysis for Users with Statistical Charts**

source="windows\_server\_attack\_logs.csv" | top limit=20 user

* What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

|  |
| --- |
| An advantage of a statistical chart is that it provides a concise list of the top users accused of suspicious activity. A disadvantage of the statistical chart is that it shows a cumulative perspective data while other approaches to data representation show a shorter, more specific perspective of data. |

## Apache Web Server Log Questions

**Report Analysis for Methods**

source="apache\_attack\_logs.txt" | top method

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

|  |
| --- |
| GET method: there was a suspicious decrease in GET activity by 29%.  POST method: there was a suspicious increase in POST activity by 29%.  This is suspicious as an attacker could be using credential stuffing or brute force attack to gain login credentials; malicious payloads are often sent using command line injection and / or RCE through the POST method. |

* What is that method used for?

|  |
| --- |
| POST: used to submit or update information to a web server. |

**Report Analysis for Referrer Domains**

source="apache\_attack\_logs.txt" | top limit=10 referer\_domain

* Did you detect any suspicious changes in referrer domains?

|  |
| --- |
| There were no suspicious referrer domains during the attack. |

**Report Analysis for HTTP Response Codes**

source="apache\_attack\_logs.txt" | top status

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

|  |
| --- |
| There are several small changes overall, but the most suspicious change detected was the HTTP 404 response code, increasing from 2% to 15%. This could be due to malicious users or automated bots attempting reconnaissance, scanning for vulnerabilities.  \*\*\*Post presentation observation in HTTP 200 response code (successful requests): Pre-attack count was 9126 or 91% of total requests; Post-attack count was 3746 or 83% of total requests. Although the absolute number of successful requests declined significantly, the percentage overall reduced only 8%. In the context of HTTP 400 increasing at the same time, this could lead us to conclude suspicious activity. |

**Alert Analysis for International Activity**

source="apache\_attack\_logs.txt" | iplocation clientip | where Country!="United States"

* Did you detect a suspicious volume of international activity?

|  |
| --- |
| There was a suspicious volume of activity in Ukraine at 8pm on March 25. |

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

|  |
| --- |
| Ukraine had a count of 937 events during the 8pm attack. |

* Would your alert be triggered for this activity?

|  |
| --- |
| Yes. The alert threshold was set at 170, therefore the alert would be triggered. |

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

|  |
| --- |
| No change in alert threshold is necessary. |

**Alert Analysis for HTTP POST Activity**

source="apache\_attack\_logs.txt" method=POST

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

|  |
| --- |
| There was a suspicious increase of POST method activity. |

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

|  |
| --- |
| There was a total count of 1296 events at 8pm. |

* When did it occur?

|  |
| --- |
| The event occurred at 8pm on March 25. |

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

|  |  |
| --- | --- |
| The alert threshold was set at 12, therefore the alert would be triggered and was successful.  No change in alert threshold is necessary. |  |

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

source="apache\_attack\_logs.txt" method=GET | timechart span=1h count by method

source="apache\_attack\_logs.txt" method=POST | timechart span=1h count by method

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity with the GET method between 5pm and 7pm on March 25.  There was suspicious activity with the POST method between 7pm and 9pm on March 25. |

* Which method seems to be used in the attack?

|  |
| --- |
| Both, GET and POST methods seem to be used in the attack. |

* At what times did the attack start and stop?

|  |
| --- |
| GET: started at 5pm on March 25 and stopped at 7pm on March 25.  POST: started at 7pm on March 25 and stopped at 9pm on March 25. |

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

|  |
| --- |
| GET: peak count during the attack was 729.  POST: peak count during the attack was 1296. |

**Dashboard Analysis for Cluster Map**

source="apache\_attack\_logs.txt" | iplocation clientip | where Country!="United States" | geostats count

source="apache\_attack\_logs.txt" | iplocation clientip | where Country!="United States" | stats count as “Activity Count” by Country

source="apache\_attack\_logs.txt" | iplocation clientip | where Country!="United States" | stats count as “Activity Count” by City

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity in the country of Ukraine, with an activity count of 937; specific cities of Kiev with a count of 438 and Kharkiv with a count of 432  Ukraine pre-attack total was 89 which represented 2% of the total count; post-attack total was 937 which represented 38% of the total count, increase of 36%. |

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

|  |
| --- |
| The city of Dnipropetrovsk, Ukraine is a new city that showed activity.  The city of Kiev, Ukraine and the city of Kharkiv, Ukraine had significantly higher volumes of activity during the post-attack review. |

* What is the count of that city?

|  |
| --- |
| Dnipropetrovsk: 1  Kiev: 438  Kharkiv: 432 |

**Dashboard Analysis for URI Data**

source="apache\_attack\_logs.txt" uri="/files/logstash/logstash-1.3.2-monolithic.jar" | timechart span=1h count by uri

source="apache\_attack\_logs.txt" uri="/VSI\_Account\_logon.php" | timechart span=1h count by uri

* Does anything stand out as suspicious?

|  |
| --- |
| There was suspicious activity with the URI ”/files/logstash/logstash-1.3.2-monolithic.jar” from 5pm to 7pm on March 25.  There was suspicious activity with the URI “/VSI.Account\_logon.php” from 7pm to 9pm on March 25. |

* What URI is hit the most?

|  |
| --- |
| The URI “/VSI.Account\_logon.php” was hit the most with 1323 events. |

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

|  |
| --- |
| Based on the URI “/VSI.Account\_logon.php” being accessed, the attacker is attempting a Brute Force attack on the VSI logon page. |

ADDITIONAL RESOURCES:

1. ChatGpt
2. Splunk
3. Google
4. Mitre

© 2024 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.