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

## Windows Server Log Questions

**Report Analysis for Severity**

* Did you detect any suspicious changes in severity?

Server log severity levels indicate the importance and urgency of logged

events. When analyzing Windows Server logs, a change in severity levels can signal significant shifts in the system's security status.

| * Informational: from 93% to 80% ⇒ 13% decrease. * High: from 7% to 20% ⇒ 13% increase.   The increase in high-severity logs suggests that the server is experiencing more critical issues or security threats. These could be due to malicious activities, system failures, or significant vulnerabilities that require immediate attention.  A decrease in informational logs, which typically include routine system information and non-critical events, might indicate that there is less routine or benign activity being logged. This could mean the system is under stress, or there might be a focus shift towards logging more critical events |
| --- |

**Report Analysis for Failed Activities**

* Did you detect any suspicious changes in failed activities?

| Small changes (<2%) in failed activities in Windows Server logs generally indicate minor fluctuations that may not be immediately alarming but should still be monitored.   * Success: from 97% to 98% ⇒ 1% increase. * Failure: from 3% to 1.5% ⇒ 1.5% decrease. |
| --- |

**Alert Analysis for Failed Windows Activity**

* Did you detect a suspicious volume of failed activity?

| Yes there was a suspicious volume of failed activity.  An increase in failed Windows activity in server logs typically indicates that there are more unsuccessful attempts to access or interact with the system, which could be due to user errors, incorrect credentials, or potential security threats.  This uptick might suggest either legitimate issues requiring user or administrative intervention or possible malicious activities, such as brute-force attacks, that need further investigation. |
| --- |

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

| 35 events occurred in the timeframe. |
| --- |

* When did it occur?

| Between 8am and 9am on 25th March 2020. |
| --- |

* 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, after reviewing the data we are comfortable to keep the current threshold. |
| --- |

**Alert Analysis for Successful Logins**

* Did you detect a suspicious volume of successful logins?

| Yes, normal logs indicate a 9-21 success logins per hour whereas attack logs show events between 0 and 16.  A decrease in successful logins in Windows Server logs typically indicates that fewer users are successfully accessing the system, which could be due to authentication issues, credential problems, or potential security concerns.  This drop might suggest issues with user accounts or access controls, or it could signal an attempted attack or unauthorized access that needs to be investigated further. |
| --- |

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

| 8 events between 9am and 1pm, max of 4 events per hour |
| --- |

* Who is the primary user logging in?

| User\_a |
| --- |

* When did it occur?

| 9am to 1pm on 25 March 2020 |
| --- |

* Would your alert be triggered for this activity?

| NO, alert was misconfigured for ‘greater than’ instead of ‘less than’ |
| --- |

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

| YES, threshold would be changed to trigger when events fall under 6 each hour |
| --- |

**Alert Analysis for Deleted Accounts**

* Did you detect a suspicious volume of deleted accounts?

| Activity of deleted account has decreased, normal logs had an average baseline of 15 whereas attack logs indicate an average baseline of 9 |
| --- |

**Dashboard Analysis for Time Chart of Signatures**

* Does anything stand out as suspicious?

| From the results, we can identify a possible brute-force attack due to the high number of login attempts and failed logins in a short period.  The number of attempts and password change requests decreased once there was a rise in successful logins, possibly indicating that attackers had gained access. |
| --- |

* What signatures stand out?

| “user account locked out”  “an attempt was made to reset an account's password”  “an account was successfully logged on” |
| --- |

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

| Spike in “user account locked out” between 12am and 2:30am  Spike in “an attempt was made to reset an accounts password” between 8am and 11am  Spike in “an account was successfully logged on” between 10am and 12:30pm |
| --- |

* What is the peak count of the different signatures?

| “user account locked out” peak count = 896 events  “an attempt was made to reset an accounts password” peak count = 1258 events  “an account was successfully logged on” peak count = 196 events |
| --- |

**Dashboard Analysis for Users**

* Does anything stand out as suspicious?

| There was suspicious activity at 8am and 11am on Wednesday, March 25th and at 4pm and 7pm on Wednesday, March 25th. |
| --- |

* Which users stand out?

| user\_k and user\_a stand out for suspicious activity. |
| --- |

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

| user\_a: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.  user\_k: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th. |
| --- |

* What is the peak count of the different users?

| user\_a: Peak count was at 984.  user\_k: Peak count was at 1,256. |
| --- |

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

* Does anything stand out as suspicious?

| There was suspicious activity starting at 8am and 11am on Wednesday, March 25th and at 4pm and 7pm on Wednesday, March 25th. |
| --- |

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

| Yes, the results were synonymous with the findings |
| --- |

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

* Does anything stand out as suspicious?

| Max user count increased from 354 to 1256  No domain users listed in top 10 after when viewing attack logs |
| --- |

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

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

**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:**   * Provides a visual representation of data, making it easier to identify trends and anomalies quickly. * Offers a comprehensive overview of user activity through statistical charts, aiding in more informed decision-making.   **Disadvantages:**   * May require more time to interpret compared to simpler, text-based reports. * Can be overwhelming if too many charts are included, potentially leading to information overload. |
| --- |

## 

## 

## Apache Web Server Log Questions

**Report Analysis for Methods**

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

| Yes. Before the attack: 98.5% GET and 1% POST; after the attack: 70% GET and 29% POST.  There is a suspicious 29% decrease in GET activity and a 28% increase in POST activity. |
| --- |

* What is that method used for?

| The POST HTTP method is used to send data to a server to create or update a resource. It is typically employed when submitting form data, uploading files, or performing operations that result in changes on the server.  Unlike the GET method, which retrieves data without side effects, POST can alter the state of the server and its resources.  This makes it a preferred method for transactions, user input handling, and any action where data needs to be securely sent to the server for processing. |
| --- |

**Report Analysis for Referrer Domains**

* Did you detect any suspicious changes in referrer domains?

| No suspicious activity detected during the attack. |
| --- |

**Report Analysis for HTTP Response Codes**

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

| There are several small changes overall, but the most suspicious change detected was the 404 response code increasing from 2% to 15%.  An increase in 404 responses indicates that there are more requests for resources that cannot be found on the server.  This can suggest broken links, removed content, or incorrect URLs being accessed, and may point to user navigation issues or potential security probing by malicious actors. |
| --- |

**Alert Analysis for International Activity**

* Did you detect a suspicious volume of international activity?

| Yes, there was a suspicious volume of activity in Ukraine at 4am on March 26th. |
| --- |

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

| Ukraine had a count of 864 events during the 4am attack. |
| --- |

* Would your alert be triggered for this activity?

| Yes, the alert would have been triggered as the threshold was set at 170. |
| --- |

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

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

**Alert Analysis for HTTP POST Activity**

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

| Yes, there was a suspicious increase of POST method activities.  An increase in HTTP POST method activity indicates a higher volume of data being sent to the server, which could involve submitting forms, uploading files, or other actions that modify server resources.  This uptick might suggest legitimate user interactions or potentially suspicious activity, such as an attempted attack or abuse of the server's functionality. |
| --- |

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

| There was a total count of 1,296 events at 4am |
| --- |

* When did it occur?

| The event occurred at 4am Thursday 26th March 2020 |
| --- |

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

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

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

* Does anything stand out as suspicious?

| There was suspicious activity with the method “GET” from 1am to 3am on Thursday 26th March 2020 and with the method “POST” from 3am to 5am on Thursday 26th March 2020. |
| --- |

* Which method seems to be used in the attack?

| * The “GET” method seemed to be used in the attack. * The “POST” method seemed to be used in the attack. |
| --- |

* At what times did the attack start and stop?

| * GET: Started at 1am on Thursday 26th March 2020 and stopped at 3am on Thursday 26th March 2020. * POST: Started at 3am on Thursday 26th March 2020 and stopped at 5am on Thursday 26th March 2020. |
| --- |

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

| * GET: Peak count during the attack was 729 events. * POST: Peak count during the attack was 1296 events. |
| --- |

**Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious?

| There was suspicious activity in the country of Ukraine, specifically in the cities of Kiev and Kharkiv. |
| --- |

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

| * The city of Kiev, Ukraine had a high volume of activity. * The city of Kharkiv, Ukraine had a high volume of activity. |
| --- |

* What is the count of that city?

| * Kiev: Count of 440 events. * Kharkiv: Count of 432 events. |
| --- |

**Dashboard Analysis for URI Data**

* Does anything stand out as suspicious?

| There was suspicious activity with the following URIs:   * “/files/logstash/logstash-1.3.2-monolithic.jar” 638 counts = 21% * “/VSI\_Account\_logon.php” 1323 counts = 43.6%   A significant increase in URI data in Apache logs typically indicates a surge in requests for specific resources on the server.  This could be due to heightened legitimate user activity, such as a spike in website traffic or an increase in API usage.  However, it may also suggest potential issues such as web scraping, automated scanning, or a denial-of-service (DoS) attack. |
| --- |

* What URI is hit the most?

| * URI **“/VSI\_Account\_logon.php”** was hit the most with **1,323 events**. |
| --- |

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

| URI "account\_logon.php" in Apache logs would be targeted because it typically handles user authentication processes.  Attackers may target this URI to attempt credential stuffing, brute-force attacks, or exploit vulnerabilities in the login mechanism to gain unauthorized access to user accounts. |
| --- |

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