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, there is a noticeable increase in high severity events from 6.91% (329 events) to 20.22% (1,111 events). This significant rise in high severity logs suggests that there were more severe incidents during the attack period compared to normal operation times, indicating suspicious activity that aligns with an ongoing attack.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, there are notable shifts in the times of failed logins between regular and attack logs. The attack logs show increased failed login attempts during the early morning hours and at midday, which could indicate targeted brute force attempts or unauthorized access attempts coinciding with the attack timeframe.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, the attack logs show a clear spike in failed activities, particularly centered around attempts to reset passwords and manage accounts. The increase in failure volume during 8:00 am, March, 25 suggests targeted actions that may be consistent with an attack.

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

35

- When did it occur?

8:00 am, March, 25

- Would your alert be triggered for this activity?

Yes as the count is above the set threshold

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

No, my alert works perfectly in this scenario.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

There were 432 successful login events on March 25, 2020, with a significant spike at 11 AM, accounting for 196 events. This indicates a potential abnormal activity, as the large number of logins concentrated in a short time span could signify a security breach or unauthorized access. However, the regular logs show a more evenly distributed pattern of successful logins on March 24, 2020, with a total of 323 events. The peaks are much less pronounced, with the highest being only 21 events around 7 PM, suggesting normal login activity compared to the attack period.

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

The most significant spike was 196 events at 11 AM.

- Who is the primary user logging in?

user_j

- When did it occur?

11:00 am - 12:00 pm on March 25th

- Would your alert be triggered for this activity?

Yes, it would.

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

No as my alert would work perfectly

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes, the attack logs show a distinct increase in account deletions during specific hours, particularly early in the morning, which is abnormal compared to the regular pattern observed on the previous day. This behavior may suggest deliberate account removals associated with an attack.
The regular logs show a steady distribution of account deletion events on March 24, 2020, with a total of 318 events. Peaks occur around 11 AM with 22 events, but overall, the distribution suggests regular maintenance or expected deletions. The attack logs display a higher concentration of account deletions on March 25, 2020, totaling 130 events, with noticeable peaks at 5 AM with 17 events. This pattern is unusual compared to the normal logs and could indicate malicious activity, such as an attacker attempting to remove traces or disable access.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, several signatures show unusual spikes in activity during specific times, which is not seen in the regular logs. This abnormal behavior suggests that these events are directly related to an attack or malicious activity.

- What signatures stand out?

“An attempt was made to reset an account's password” shows a significant spike early in the day, indicating possible brute force or unauthorized access attempts.
“A user account was deleted” and **“A user account was created”** have spikes, suggesting that accounts were being managed in an unauthorized manner.
“Special privileges assigned to new logon” stands out, indicating potential privilege escalation attempts.

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

The **password reset attempts** and **account deletions** begin around early morning hours (1:00 AM) and continue with peaks throughout the morning, stopping by around midday.
The **privilege escalation attempts** and **security access removals** occur around 2:00 AM, showing concentrated activity at this time, indicating a coordinated attack.

- What is the peak count of the different signatures?

Password reset attempts reached a peak of around 10 attempts within an hour.
Account deletions peaked at about 7 events during a concentrated hour.
Privilege escalations had a high of approximately 500 events in a single hour, highlighting a significant unauthorized action.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes, there are unusual spikes in activity for specific users that are not consistent with normal usage patterns. The significant peaks suggest unauthorized or malicious behavior.

- Which users stand out?

user_a and **user_k** are the most notable, with sharp increases in activity at specific times, which is abnormal compared to other users.

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

user_a shows a peak at 2:00 AM on March 25, 2020, with 984 events, and then the activity drops sharply after that hour.
user_k exhibits a peak at 9:00 AM on the same day with 1,256 events, with no preceding or following significant activity, indicating a concentrated burst of actions.

- What is the peak count of the different users?

user_a: The peak count is 984 events at 2:00 AM.
user_k: The peak count is 1,256 events at 9:00 AM

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

- Does anything stand out as suspicious?

Yes, several signatures show unusual spikes in activity during specific times.

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

The spike in activity occurred from 8:00 AM to 10:00 AM on March 25, 2020, with the most notable peak at 9:00 AM.

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

- Does anything stand out as suspicious?

Yes, there was a significant increase in the number of successful logins.

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

```
Yes, user_k stands out as the primary user logging in, with a peak at 1,256
logins around 9:00 AM.
```

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?

With our main actors pinpointed, we can see the statistics more clearly in these charts. On the other hand, the disadvantage might be that we won't be able to determine the time range of these attacks when working with statistical charts.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, there were suspicious changes detected in the HTTP methods, specifically the POST method. The attack logs show a significant spike in the count of POST requests compared to the normal logs. This abnormal increase suggests potential malicious activity during the attack period.

- What is that method used for?

The POST method is used to send data to the server, typically used for submitting form data, uploading files, or making requests that change the state of the server, such as creating or modifying resources. However, in the context of an attack, POST requests are often used by

attackers to inject malicious payloads, exploit server vulnerabilities, or attempt unauthorized actions like file uploads or SQL injections.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Yes, there were suspicious changes detected in the referrer domains between the normal and attack logs.
In the attack logs (apache_attack_logs.txt), there is a noticeable drop in the number of requests from known and reputable referrer domains like Google compared to the normal logs (apache_logs.txt). Additionally, certain referrer domains such as logstash.net, tuxradar.com, and kufli.blogspot.com appear in the attack logs but are not prominently seen in the normal logs.
The high count from semicomplete.com remains consistent across both normal and attack logs but with reduced counts during the attack. This domain's behavior is suspicious given its high volume compared to other referrers.

Report Analysis for HTTP Response Codes

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

Yes, there were noticeable changes in the HTTP response codes between the normal (apache_logs.txt) and attack logs (apache_attack_logs.txt).
In the attack logs, there is a significant increase in 4xx (client error) and 5xx (server error) response codes, particularly the 404 (Not Found) and 500 (Internal Server Error) codes.
The presence of 500 errors is particularly concerning as it indicates issues with the server's ability to process requests, which could be due to the server being overloaded, experiencing crashes, or being exploited.
Additionally, the increase in 404 errors suggests attempts to access resources that are not present, potentially indicating scanning or probing activity by attackers looking for vulnerable endpoints.

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes, there was a suspicious spike in international activity detected in the attack logs (apache_attack_logs.txt). The count of events increased dramatically during a specific time frame compared to the regular pattern seen in the normal logs (apache_logs.txt).

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

The spike occurred at 8:00 PM on March 25, 2020, with a total of 1,415 events logged during this hour. This is significantly higher than the usual baseline activity observed in the normal logs.

- Would your alert be triggered for this activity?

Yes, the alert would likely be triggered due to the unusual volume of activity, and going above the set threshold.

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

No, as my alert will work perfectly in this scenario.

Alert Analysis for HTTP POST Activity

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

Yes, there was a significant increase in the volume of HTTP POST activity in the attack logs (apache_attack_logs.txt). This is markedly different from the regular pattern seen in the normal logs (apache_logs.txt).

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

The attack logs show a massive spike with 1,324 POST events occurring during a specific time frame, compared to the usual 106 events seen in the normal logs.

- When did it occur?

The suspicious spike in POST requests occurred on March 25, 2020, specifically around 8:00 PM. This sudden increase indicates potentially malicious activities such as an attempt to exploit vulnerabilities through POST requests.

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

```
Nope, as my alert would work perfectly in this scenario.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, several aspects stand out as suspicious:Abnormal Increase in POST Requests: There is a significant spike in POST requests in the attack logs (apache_attack_logs.txt) compared to the normal logs. POST requests jumped from around 106 events in normal activity to over 1,324 during the attack, suggesting a potential exploitation attempt.High Volume of 404 and 500 Error Codes: The attack logs show an unusual increase in 404 (Not Found) and 500 (Internal Server Error) response codes, indicating possible scanning activity for non-existent resources and server instability during the attack.Suspicious Referrer Domains: The appearance of less common referrer domains such as logstash.net and tuxradar.com during the attack period, which were not prominent in the normal logs, suggests that traffic might be generated from unconventional or potentially malicious sources.

- Which method seems to be used in the attack?

POST Method: The POST method appears to be heavily utilized, with a peak count of 1,296 events occurring at 8:00 PM on March 25, 2020. This volume is abnormally high compared to typical usage, suggesting that POST requests were likely used as part of the attack, possibly for data exfiltration or command injection attempts.
GET Method: The GET method also showed suspiciously high usage with a peak of 729 events at 6:00 PM on March 25, 2020. This could indicate scanning or other malicious activity exploiting URLs.

- At what times did the attack start and stop?

The attack seems to start around 2:00 AM on March 25, 2020, as indicated by the initial spike in POST requests. It peaks at 8:00 PM and then subsides, suggesting a duration of approximately 18 hours.

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

The peak count was for the POST method with 1,296 requests at 8:00 PM on March 25, 2020.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

The cluster maps display high concentrations of activity in the United States, specifically around major cities, suggesting potential command and control or malicious servers in those locations. Additionally, the map highlights clusters in unexpected regions with high volume, indicating potential new attack origins.

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

The new suspicious location on the map with high activity is notably in Ukraine, specifically showing high counts in a cluster around the capital or other major cities.

- What is the count of that city?

Ukraine has a count of 1369 events during the attack

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

The frequent access to administrative pages (/admin.php, /administrator/, /administrator/index.php) and account login pages (/VSI_Account_logon.php) suggests a targeted attack on sensitive or administrative endpoints. These are typical targets for unauthorized access attempts, which can be highly suspicious.

- What URI is hit the most?

The URI /VSI_Company_Homepage.html has the highest count in the attack logs with 1,323 hits. This specific page appears to be the main target, followed closely by the account login page /VSI_Account_logon.php.

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

Based on the accessed URIs, the attacker seems to be attempting unauthorized access, particularly trying to breach login and administrative sections.