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 signatures raised from 6.906% to 20.222%
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
No, changes in the total amount of failed activities were minimal
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
At 8am there was a suspicious jump in failed activity
```

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

```
35
```

- When did it occur?

```
8am March 25th 2020
```

- Would your alert be triggered for this activity?

```
Yes
```

- 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 1am to 3am and 9am to 11am
```

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

```
1am to 2am 965
2am to 3am 1005
9am to 10am 1293
10am to 11am 784
```

- Who is the primary user logging in?

```
user_k at 36.1%
user_a at 31.933%
user_j at 6.611%

user_k is the primary user logging in at 9am to 11am
user_a is the primary user logging in at 1am to 3am
```

- When did it occur?

```
At 1am to 3am and 9am to 11am
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
Yes, increase the threshold
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
A high amount of user accounts were locked out between 1am and 3am
```

- What signatures stand out?

```
-A user account was locked out
Which ties in with
-An attempt was made to reset accounts password
-Special privileges assigned to new logon
```

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

```
A user account was locked out -> 12am 1pm
An attempt was made to reset accounts password -> 12am 1pm
Special privileges assigned to new logon -> 12am 1pm
```

- What is the peak count of the different signatures?

```
A user account was locked out -> 896 at 2am
An attempt was made to reset accounts password -> 1258 at 9am
Special privileges assigned to new logon -> 17 at 6am and 8am
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, the hourly windows activity exhibits a potentially suspicious pattern.
Typically, failures range between 2 and 9, peaking at 9. However, we
consider counts exceeding 15 as overly suspicious and outside the expected
range, warranting further investigation.
```

- Which users stand out?

```
user_k and user_a
```

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

```
Both user_a and user_k have events starting from 12am  and ending at 2pm
But user_a has maximum activity from 1am to 3am
And user_k has maximum activity from 9am to 11am
```

- What is the peak count of the different users?

```
user_a has 984 events at 2am
user_k has 1256 events at 9am
```

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

- Does anything stand out as suspicious?

```
The amount of high severity signatures increased during the attack and the
amount of the usual signatures decreased from 10-20 to 0-5
```

- 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?

```
The amount of usual logins reduced heavily and even dropped to 0 between 2am
to 2:30am and 9:30am to 12am
```

- 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?

```
It is very easy to see the level of activity and the users with most
activity
But is is difficult to parse more specific details especially from user with
lower activity
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
The most suspicious change detected was the spike in POST request activity,
going from 1.06% of all method requests in the normal logs, up to 29.44%
during the attack logs.
```

```
Also suspicious is the significant decrease in GET requests, going from a massive 98.51% of all requests during normal activity, down to 70.2% during the attack log timeframe.
```

- What is that method used for?

```
The POST request method is used to request a web server to accept data being sent to it, which often changes/updates the server. For example, a POST request could include one’s credentials for logging in.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Upon initial examination, the referrer domains, especially the top two results, do not appear suspicious. However, a more in-depth investigation is necessary to identify any potential anomalies or suspicious activity.
```

Report Analysis for HTTP Response Codes

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

```
Yes, the most suspicious being the spike in status code 404 (page/file not found) going from 2.13% of all codes up to 15.09% during the attack. Also, there were less drastic but still very noticeable changes in the other 3 top response codes:
Code 200 from 91.26% down to 83.29%;
Code 304 from 4.45% down to 0.8%;
Code 301 from 1.64% down to 0.64%
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Upon investigation, we identified a concerning surge in international activity. Closer examination revealed that the suspicious hourly patterns are emanating from Ukraine, specifically from two cities: Kyiv (Solom’yans’kyi District) and Kharkiv (Shevchenkivs’kyi District).
```

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

```
864 at 8 PM on March 25, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, the significant spike in international activity (emanating from
Ukraine) breached our threshold of 160 and triggered an alert.
```

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

```
For the moment, we would not change the threshold that was selected. It did
its job effectively, as it was triggered by the suspicious increase in
activity from within Ukraine, while at the same time not producing any false
positives. With greater sample sizes and timeframes, it may come to the
point where the threshold should be fine tuned, however, for now it will be
kept as is.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, on March 25, 2020 at 8:00 PM, there was a massive spike in POST
requests detected
```

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

```
Count at 8:00 PM = 1296
```

- When did it occur?

```
March 25, 2020, at 8:00 PM
```

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

No, we would not change the threshold. The alert threshold worked as intended, by notifying the security team of unusual activity. Also significant is that all the “normal” activity values fell well below the threshold level, thus reducing the chances of false positives.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

The drastic increase in GET requests at 6 PM on March 25, 2020, along with the subsequent drastic increase in POST requests at 8 PM of the same day stand out as very suspicious. To illustrate, the high count of GET and POST requests during the normal activity log stands at 135 and 7, respectively, compared to 729 and 1296, respectively, during the attack hours. That is a massive disparity.

- Which method seems to be used in the attack?

Both GET and POST request methods seem to be used in the attack.
Beginning with the spike in GET requests, this could illustrate some sort of Denial of Service attack. It is likely that it also represents reconnaissance probing activity, with the goal of gathering information to be used in the exploitation phase. This could also include exfiltrating data, such as credentials, potentially from a URI with abnormally high request counts (/files/logstash/logstash-1.3.2-monolithic.jar).
The subsequent spike in POST request activity could be part of a further attempt to degrade the availability of VSI’s server, which might explain the drastically reduced hourly activity from other typically high usage countries (i.e. France, Germany, China, Netherlands, etc). It also likely illustrates some sort of brute force or credential stuffing attack, where information gained in the probing (GET request) stage is used to gain access to user account(s).

- At what times did the attack start and stop?

It seems that the attacks started at 6 PM on March 25, 2020, and subsided by 9 PM on the same date.

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

```
1296 is the peak count of POST requests, taking place at 8:00 pm.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
The most suspicious observation is that a country, Ukraine, has about 10 times the level of activity in the attack logs vs normal logs (877 vs 89). This occurred in an overall sample size of events that is about half the number of total events when compared to the logs of normal activity.

What is less suspicious, but should be noted, is that some of the countries with the highest count of activity saw their usage drastically decreased. This is notably the case with European nations, excluding Ukraine. Some examples include:
France going from 859 down to 190
Germany going from 567 down to 161
India going from 430 down to 49
China going from 376 down to 64
Netherlands going from 235 down to 63
Russia going from 210 down to 31

This might be explained by a Denial of Service attack, which could limit activity from certain regions.
```

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

```
Kyiv (Solom’yans’kyi District), Ukraine
Kharkiv (Shevchenkivs’kyi District), Ukraine
```

- What is the count of that city?

```
Kyiv - 438
Kharkiv - 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
The number of unique URIs is drastically lower in the attack logs compared to the normal logs (613 vs 1498). Less resources being accessed could signify a Denial of Service attack, as this could be indicative of less users being able to access VSI web resources.

Upon closer examination, there are some peculiarities that could be indicative of the method of attack used. In the normal logs, the two URIs with the highest counts are: 1) /VSI_Company_Homepage.html; 2) /contactus.html. This makes sense and is to be expected of what constitutes normal activity.
On the other hand, in the attack logs, the two URIs with the highest counts are: 1) /VSI_Account_logon.php; 2) /files/logstash/logstash-1.3.2-monolithic.jar.
What is very interesting is the timing of the high counts for these two URIs:
The logstash-1.3.2-monolithic.jar file sounds like it may hold some information, such as credentials. The high count for access to this URI happens at 6:00 pm on March 25, 2020, which coincides with the unusually high number of GET requests at the exact same time. Furthermore, the unusually high count on the Account_logon page is at 8:00 pm on the same day, which also coincides with the unusually high number of POST requests at the exact same time.
```

- What URI is hit the most?

```
/VSI_Account_logon.php - Count: 1323
```

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

```
The fact that the VSI logon page is seeing activity many times higher than usual potentially indicates a Brute Force attack, or credential stuffing. The unusually high amount of POST requests at the same time supports this theory, since a Brute Force attack would be sending information (i.e. numerous credentials attempting to log in) at a much greater rate compared to normal conditions.
Some other possibilities include performing an SQL injection with the purpose of revealing any login vulnerabilities, or a cross-site scripting attacks (xss) that insert scripts into a URI with the high POST request count representing payloads that target any exploits that have been
```

uncovered. Furthermore, the high number of login requests in a short period of time could also lead to a Denial of Service for other users.