Defensive Security

Review Questions

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
Informational: There has been a decrease of 13% in informational severity,
declining from 93% to 80%.

High: Conversely, high severity cases have observed an increase of 13%,
rising from 7% to 20%.

These findings indicate the presence of suspicious changes in severity
within the analyzed data.
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Success Rate: The success rate has exhibited a marginal increase,
transitioning from 97% to 98%, thereby reflecting a modest 1% improvement.

Failure Rate: Conversely, the failure rate has witnessed a slight decrease,
moving from 3% to 2%, indicating a 1% reduction.

There have been no significant shifts or suspicious changes in failed
activities during the analyzed period.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, there was a suspicious volume of failed activity detected at 8:00 AM, Wednesday, March 25th, 2020.
```

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

```
During this hour, there were seventy (70) events counted.
```

- When did it occur?

```
This occurred at 8:00 AM, Wednesday, March 25th, 2020.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would be triggered as the threshold is set at twenty (20).
```

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

```
No, changing the threshold is unnecessary in this instance.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Suspicious volume of successful logins was detected from 10:00 AM to 12:00 PM on Wednesday, March 25th, 2020.
```

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

```
The activity count is 46 events at 10:00 AM, 392 events at 11:00AM, and 154 events at 12:00 PM. This led to a total of 592 events occurring during the three (3) hour window.
```

- Who is the primary user logging in?

```
The primary user logging in during this timeframe was “user_j”.
```

- When did it occur?

```
The suspicious activities occurred from 10:00 AM to 12:00 PM on Wednesday, March 25th 2020.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would be triggered as the threshold is set at forty-five (45).
```

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

```
Yes, I would want to increase the threshold, slightly, from forty-five (45) to sixty (60).
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
There were no signs of suspicious volumes of deleted accounts.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
There was suspicious activity with the signature “An account was locked out” from 12:00 a.m. to 3:00 a.m. on Wednesday, March 25th 2020 and with the signature “An attempt was made to reset an accounts password” from 8:00 a.m. to 11:00 a.m. on Wednesday, March 25th 2020.
```

- What signatures stand out?

```
The “A user account was locked out” and “An attempt was made to reset an accounts password” signatures stand out for suspicious activity.
```

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

```
A user account was locked out: Started at 12:00 a.m. on Wednesday, March 25th 2020 and stopped at 3:00 a.m. on Wednesday, March 25th 2020.

An attempt was made to reset an accounts password: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th 2020.
```

- What is the peak count of the different signatures?

```
A user account was locked out: Peak count during the attack was at 1,792.

An attempt was made to reset an accounts password: Peak count during the attack was at 2,516.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
There was suspicious activity from 12:00 AM to 3:00 AM and at 9:00 AM to 10 AM on Wednesday, March 25th 2020.
```

- Which users stand out?

```
“user_a” and “user_k” stand out for suspicious activity.
```

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

```
user_a: Started at 12:00 AM and stopped at 3:00 AM on Wednesday, March 25th 2020.

user_k: Started at 8:00 AM and stopped at 11:00 AM on Wednesday, March 25th 2020.
```

- What is the peak count of the different users?

```
user_a: Peak count was at 1,968.

user_k: Peak count was at 2,512.
```

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

- Does anything stand out as suspicious?

```
There was suspicious activity from 12:00 AM to 3:00 AM and at 9:00 AM to 10 AM on Wednesday, March 25th 2020.
```

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

```
Yes, the results match the findings within the signature time chart.
```

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

- Does anything stand out as suspicious?

```
There was suspicious activity from 12:00 AM to 3:00 AM and at 9:00 AM to 10 AM on Wednesday, March 25th 2020.
```

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

```
Yes, the results are synonymous to the findings within the user time chart.
```

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?

```
One notable advantage of utilizing the statistical chart is its ability to provide a succinct and readily accessible list of the top users flagged for suspicious activity. This condensed format facilitates quick identification and prioritization of potential security concerns.
```

However, it is important to acknowledge a corresponding disadvantage. The statistical chart primarily offers a cumulative perspective of the data, presenting an overview of trends and patterns over a specified period.

Alternative data representation methods may offer more granular and specific insights, enabling a deeper examination of individual events or shorter timeframes. Consequently, while the statistical chart excels in presenting an overarching view, it may not be as effective in revealing the fine-grained details that other data visualization approaches can provide.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes; there was a 29% decrease in GET activity, from 99% to 70%, and as well as a 29% increase in POST activity, from 1% to 29%.

- What is that method used for?

The POST method is an essential part of web development for sending data securely to the server and triggering actions that modify server-side resources or state. It is particularly useful when dealing with sensitive information or large data payloads.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No suspicious referrer domains were identified during the course of the attack or analysis.

Report Analysis for HTTP Response Codes

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

```
While numerous minor changes have been observed in response code patterns, the most noteworthy and suspicious change pertains to the 404-response code. It has exhibited a 11% increase, rising from 4% to 15%.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, there was a suspicious volume of activity detected.
```

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

```
There was a total count of 937 events during the 8:00 PM attack.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would be triggered as the threshold is set at 170.
```

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

```
Yes, I want to increase the threshold from 170 to 300 to help avoid any false positive alerts.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, a suspicious and potentially concerning escalation in POST method activities has been detected.
```

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

```
There was a total count of 1,296 during the attack.
```

- When did it occur?

```
The attack occurred at 8:00 PM, Wednesday, March 25th 2020.
```

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

```
No, changing the threshold is unnecessary in this instance.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, there were unusual spikes in HTTP method activity.
```

- Which method seems to be used in the attack?

```
Both the “GET” and “POST” methods seem to be used in this attack.
```

- At what times did the attack start and stop?

```
GET: Occurred on Wednesday, March 25th 2020. Starting at 5:00 PM and stopping
at 7:00 PM.

POST: Occurred on Wednesday, March 25th 2020. Starting at 7:00 PM and
stopping at 9:00 PM.
```

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

```
POST: The top method, with a peak count of 1,296.

GET: Peak count during the attack was 729.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, new clusters formed at a location that was not previously shown to have connected with VSI’s administrative webpage.
```

- Which new location (city, country) on the map has a high volume of activity?

```
By zooming in on the cluster map, shown in Dashboard 12, we can see that the new cluster(s) of high activity are from Kiev, Ukraine and Kharkiv, Ukraine.
```

- What is the count of that city?

```
Kiev displays a count of 454 connections to the webpage.

Kharkiv displays a count of 433 connections to the webpage.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Suspicious activity was observed with the URI "/files/logstash/logstash-1.3.2-monolithic.jar" between 6:00 PM and 7:00 PM on Wednesday, March 25th, 2020.

Another instance of suspicious activity was identified with the URI "/VSI_Account_logon.php" occurring from 8:00 PM to 9:00 PM on the same day, Wednesday, March 25th, 2020.
```

- What URI is hit the most?

```
The URI “/VSI_Account_logon.php” was hit the most with 1,296 events.
```

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

```
The access to "/files/logstash/logstash-1.3.2-monolithic.jar" suggests an attempt to access or download a specific file, which could potentially be a part of an attack involving the exploitation of vulnerabilities associated with the file or software it represents. This may include attempts to gain unauthorized access, install malicious software, or compromise the integrity of the file.
```

The access to "/VSI_Account_logon.php" is indicative of potential involvement in a credential-based attack or an attempt to gain unauthorized access to an application or system. Attackers might use this URI to launch phishing campaigns, attempt brute force login attacks, or exploit vulnerabilities in the login functionality to compromise user accounts or system security.