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. The original Windows server logs showed only 6.91% of events marked as high severity, while 93.09% were informational. However, after switching to the attack log source, the percentage of high-severity events increased sharply to 20.22% — a nearly threefold spike.

This dramatic rise in high-severity events is a clear indicator of elevated threat activity. It suggests that the system experienced a concentrated wave of potentially malicious behavior during the attack period.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes. In the original logs, there were 284 failed login attempts compared to 9,244 successful logins — indicating a relatively low fail rate. However, in the attack logs, failed attempts dropped to 93, while successful logins slightly increased to 5,856.

```
This suggests a shift in attack technique: rather than brute-force attempts, the attacker may already have valid credentials or escalated access — evidenced by the higher ratio of successful logins during the attack period.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, a spike in failed login attempts was detected, indicating potentially unauthorized access attempts.
```

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

```
35 failed login events were recorded.
```

- When did it occur?

```
On March 25, 2020, at 03:00 AM.
```

- Would your alert be triggered for this activity?

```
Yes, under real-time or continuous logging conditions, this alert would be triggered correctly
```

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

```
Yes — I would consider temporarily lowering the threshold or adjusting the alert logic to ensure it reliably triggers during similar spikes.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes. There are multiple time blocks where the count exceeds 10, peaking at **15 events** in several hours.

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

15 events at 20:00 and 08:00
14 events at 21:00 and 22:00
11-12 in other hours

- Who is the primary user logging in?

user_n had the highest count: **18 events (12.86%)**

- When did it occur?

March 24, 2020 at 19:00
March 25, 2020 at 08:00

- Would your alert be triggered for this activity?

Yes. With the threshold adjusted to **count ≥ 10**, your alert would successfully **trigger during at least 9 time intervals**.

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

Yes. **Lowering the threshold to 10** significantly improved detection accuracy in this lab environment, which contains fewer overall events.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes. Multiple time bins had a high count of user deletions.
The counts exceeded the threshold of 5 in several hourly spans:

2020-03-24 19:00 - 14 deletions
2020-03-24 23:00 - 14 deletions
2020-03-25 00:00 - 17 deletions

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Unusual spike in account lockouts on 2020-03-25 at 04:00 with **1,258** events.

Another **smaller surge** at 03:00 and 06:00 with **16** and **196** lockouts, respectively.

These likely indicate brute-force attempts or policy misconfigurations causing widespread lockouts.

- What signatures stand out?

A user account was locked out – abnormally high counts (over 1,000 in one hour).

An attempt was made to reset an account's password – spikes (e.g., 23 at 06:00, 15 at 08:00).

The audit log was cleared – seen multiple times, which can indicate **anti-forensic activity**.

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

Signature	Start Time	End Time
Account lockouts	03/24 19:00	03/25 08:00
High lockout peak	03/25 04:00	03/25 06:00

Password reset attempts	03/25 04:00	03/25 08:00
Audit log cleared	03/24 19:00	03/25 08:00
Computer/user account changes/deletions	Periodically active	Ongoing throughout

- What is the peak count of the different signatures?

Signature	Peak Count	Time
A user account was locked out	1,258	03/25 04:00
Attempt to reset an account's password	23	03/25 06:00
Audit log was cleared	16	03/24–03/25
Computer account deleted	19	03/24 19:00

Dashboard Analysis for Users

- Does anything stand out as suspicious?

user_a spikes to **799 logons** at 2020-03-24 20:00 and then again to **984 logons** at 21:00.

user_k hits a **staggering 1,256 events** at 2020-03-25 04:00.

- Which users stand out?

user_a: 799 + 984 = **1,783 logons** in two hours.

user_k: 1,256 events in one hour.

user_j: Appears with 196 events at 2020-03-25 06:00, another high-volume anomaly.

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

User	First Spike	Last Activity
user_a	2020-03-24 20:00	2020-03-25 08:00
user_k	2020-03-25 03:00	2020-03-25 04:00
user_j	2020-03-25 04:00	2020-03-25 07:00

- What is the peak count of the different users?

User	Peak Count
user_a	984
user_k	1,256
user_j	196

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

- Does anything stand out as suspicious?

“A user account was locked out” shows an abnormally high volume — peaking at **896 events** in a single hour.

“An account was successfully logged on” and **“A user account was changed”** also show unusually high and clustered spikes.

The **pie chart** likely reflects a disproportionate share of total events attributed to just a few signatures — confirming that a small number of behaviors are driving most of the suspicious activity.

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

Yes, the bar and pie chart results **complement and confirm** the patterns observed in the time chart:

The **time chart pinpointed the hours of intense activity** per signature.

The **bar and pie charts visualize the overall weight of each signature**, revealing that the same few (account lockouts, logons, changes) dominate the event landscape.

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

- Does anything stand out as suspicious?

user_a had an explosive spike in activity — **799 events at 8 PM and 984 events at 9 PM** — which is drastically higher than all other users and time periods.

user_k also triggered **1,256 events at 4 AM** and **761 events at 5 AM**, indicating scripted or automated behavior, possibly from malware or brute-force automation.

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

The time chart gave us **hour-by-hour spikes** in activity, which are clearly shown to be dominated by **user_a** and **user_k**.

The bar and pie charts highlight that **those two users are responsible for the majority of total activity**, far outpacing the rest.

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:

- **Clear numerical breakdown**: The statistical chart delivers *exact* event counts per user, making it easy to quantify suspicious activity without interpreting visuals.
- **Efficient comparison**: You can quickly identify which users have the most activity and stack-rank them without scrolling through timelines or hovering over charts.
- **Lightweight on resources**: Compared to visualizations, statistical tables are faster to load and less demanding on the system — ideal for large datasets.

Disadvantages:

- **Lacks temporal context**: Unlike time charts, this panel doesn't show *when* the activity occurred — only *how much*. You lose the sense of spikes or patterns over time.
- **Not visually intuitive**: At a glance, it's harder to notice anomalies or trends compared to bar/pie/time-based charts.
- **More manual effort**: Requires more scrolling and mental math to spot outliers, especially when user activity is close in count.

Apache Web Server Log Questions

Report Analysis for Methods

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

The **POST** method shows an unusually high volume with **1,324** requests. While **GET** requests are expected and high (3,157), the spike in **POST** usage often signals potential data submission or exploitation attempts, especially in an attack log context.

- What is that method used for?

```
POST is used to send data to a server (e.g., login credentials, form submissions, file uploads).
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
High Volume from Semicomplete Domains:

http://www.semicomplete.com (764 hits)
http://semicomplete.com (572 hits)
 These domains account for over 29% of total activity (1336 out of 4497 events), which is unusually high and suggests they may have been exploited or spoofed in the attack traffic.
```

Report Analysis for HTTP Response Codes

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

```
404 (Not Found) — 679 occurrences

A high number of 404s suggests potential directory or file enumeration attempts — attackers probing for known vulnerable scripts or admin portals.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
There was a clear spike in international web traffic during a specific time window
```

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

```
2020-03-24 19:00 — 120 events
2020-03-24 20:00 — 108 events
```

```
2020-03-25 04:00 – 107 events
2020-03-25 15:00 – 937 events
```

- Would your alert be triggered for this activity?

```
Yes. All of the above time blocks surpassed the 100-event threshold and
would have triggered the alert.
```

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

```
While the 100-event threshold effectively catches spikes, the 937-event
burst at 15:00 is orders of magnitude higher, suggesting it may be worth
increasing the threshold to 200+ if you want to isolate only extreme
anomalies and reduce noise.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, there was an extremely suspicious spike in POST requests.
```

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

```
The peak count occurred at 2020-03-25 15:00 with 1415 POST requests, which
is far beyond typical volume.
```

- When did it occur?

```
This spike occurred on March 25th, 2020 between 15:00 and 16:00.
```

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

```
Yes. The previous threshold was set at 20, which is too low for general
traffic and may cause false positives. A revised threshold around 200 would
better distinguish truly abnormal activity without excessive alerting.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes – there is an anomalous spike in HTTP POST requests, while other methods
(GET, HEAD, OPTIONS) remain flat and consistent. This is highly indicative
of a targeted attack.
```

- Which method seems to be used in the attack?

```
The POST method was used, likely attempting to exploit form submissions or
upload mechanisms.
```

- At what times did the attack start and stop?

```
The spike began around 2020-03-25 13:00, peaked at 15:00, and stopped
shortly after 16:00.
```

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

```
The POST method peaked at approximately 1415 requests in a single hour
(15:00-16:00).
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes. A large concentration of traffic appears in Ukraine, which is
inconsistent with normal access patterns and could signify a coordinated
attack or unauthorized probing.
```

- 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 is prominently displayed with a notably large
volume of traffic.
```

- What is the count of that city?

```
439
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes – the URI /VSI_Account_logon.php was accessed far more than any other, with over 1,200 requests, which is a strong indicator of brute-force login attempts or credential stuffing.
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
Given the URI includes logon.php, it likely points to a login page. The high volume of traffic suggests that the attacker may be:

- Performing brute-force attacks to guess user credentials.
- Launching a credential stuffing campaign using leaked usernames and passwords.
- Attempting to exploit known vulnerabilities in the login logic (e.g., SQL injection, authentication bypass).
```