Cybersecurity

Project 3 Review Questions

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
Percentages jumped from 6% to 20% high severity
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Did not show significant differences between before and during the attack
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Suspicious activity detected at 8am, Mar 25
```

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

```
35
```

- When did it occur?

```
8am, Mar 25
```

- 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?

```
Suspicious activity detected at 11am and 12pm on Mar 25
```

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

```
11am: 196 count
12pm: 77 count
```

- Who is the primary user logging in?

```
User j
```

- When did it occur?

```
11am and 12pm, Mar 25
```

- 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 Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No signs of suspicious activity detected
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
12am-3am account lockouts, 8am-11am password reset attempts
```

- What signatures stand out?

```
“A user account was locked out” and “An attempt was made to reset an
accounts password”
```

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

```
Account lockout: 12am-3am
Password reset attempt: 8am-11am
```

- What is the peak count of the different signatures?

```
Account lockout: 896
Password reset attempt: 1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
User I was the number one user at a count of a little over 1000, user K was the number one user during the attack, at a count of over 2000. Followed by user A, at just under 2000, compared to their normal activity of about 800
```

- Which users stand out?

```
Users K and A
```

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

```
K:9am-10am
A: 1am-2am
```

- What is the peak count of the different users?

```
K:over 2000, password reset attempts
A: slightly less than 2000, locked out accounts
```

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

- Does anything stand out as suspicious?

```
Prior to the attack, the top signature was “Special privileges assigned to new login” at about 1000 count, while “An attempt was made to reset an accounts password” had a count of over 2000 during the attack
```

- 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?

```
User A locked out an account 805 times at 1 am, and 896 times at 2 am.

User K attempted to reset an account's password 1258 times at 9am, and 761 times at 10 am.
```

- 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 allows for visual representation, compiling the data into easy to read formats. It becomes very easy to see discrepancies in data. The data is compiled though, other avenues could show more specific data.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Increase in POST requests by 29%
```

- What is that method used for?

```
Used to update, or submit data to a webserver
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No signs of suspicious activity detected
```

Report Analysis for HTTP Response Codes

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

```
404 response code returns increased from 2% to 15%
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Suspicious activity detected at 8pm, Mar 25, out of Ukraine
```

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

```
1369 count at 8pm out of Ukraine
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

Alert Analysis for HTTP POST Activity

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

```
Suspicious amount of POST activity detected
```

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

```
1296 at 8pm
```

- When did it occur?

```
8pm, Mar 25
```

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

```
No
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There were 2592 post requests at 20:00, and 1458 get requests at 18:00
during the attack
```

- Which method seems to be used in the attack?

```
GET and POST
```

- At what times did the attack start and stop?

```
GET: 5pm-7pm, Mar 25
POST: 7pm-8pm, Mar 25
```

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

```
GET: 1296
POST: 729
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Suspicious activity detected out of Ukraine
```

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

```
Kiev and Kharkiv, Ukraine
```

- What is the count of that city?

```
Kiev: 872
Kharkiv: 432
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
During the attack, the main URI was VSI_Account_logon.php with more than
2500 count, while VIS_Company_homepage.html at slightly over 800 prior to
the attack
```

- What URI is hit the most?

```
VSI_Account_logon.php at 1415 event count
```

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

```
The attacker is likely attempting to brute force the VSI user logon page
```