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 was an increase of about 453 high-warning events from 658(prior)
to 1,111 (attack logs).
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, the events with failed activities associated went up by almost two
times.
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes, I did.
```

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

```
The count was 35.
```

- When did it occur?

```
2020-03-25 08:00
```

- Would your alert be triggered for this activity?

```
Yes it would have been triggered.
```

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

```
No, I would not have changed my threshold of 12 and a baseline of 6.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes
```

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

```
23, 196, 77
```

- Who is the primary user logging in?

```
user_j
```

- When did it occur?

```
It occurred from 2020-03-25 10:00 to 2020-03-25 13:00
```

- Would your alert be triggered for this activity?

```
Yes the alert would have been triggered
```

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

```
No I would not change my threshold of 22 and baseline of 14.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No suspicious volume was detected. a baseline of 27 and a threshold of 36
were used.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, 3 signatures stand out as suspicious.
```

- What signatures stand out?

```
“An attempt was made to reset accounts password,” “A user account was locked
out,” and “An account was successfully logged on.”
```

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

```
For “An attempt was made to reset accounts password,”  it was 9-11am
For “A user account was locked out,” it was 1-3am
For “An account was successfully logged on.” it was 11am-1pm
```

- What is the peak count of the different signatures?

```
For “An attempt was made to reset accounts password,”  it was 1258
For “A user account was locked out,” it was 896
```

```
For “An account was successfully logged on.” it was 196.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, 3 users are showing to be unusually active.
```

- Which users stand out?

```
user_a, user_k, and user_k
```

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

```
user_a: 1:40 am to 2:50 am
user_k: 9:10 am to 11:00 am
user_j: 10:40 am to 12:20 pm
```

- What is the peak count of the different users?

```
user_a: 785
user_k: 397
user_j: 35
```

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

- Does anything stand out as suspicious?

```
Yes, the following signatures are:
“An attempt was made to reset accounts password,” “A user account was locked
out,” and “An account was successfully logged on.”
```

- 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?

```
Yes, the following users are suspicious: user_a, user_k, and user_k
```

- 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?

```
Disadvantages: You can not see the specific time in which the spikes happen.
Advantages: You can very accurately identify the exact number of events
associated with each user which makes it easier to be concise in a report.
```

user ⇕	count ⇕	percent ⇕
user_k	2118	35.608608
user_a	1878	31.573638
user_j	398	6.691325
user_l	145	2.437794
user_e	117	1.967048
user_m	112	1.882986
user_f	109	1.832549
user_b	109	1.832549
user_i	106	1.782112
user_n	105	1.765299
user_c	105	1.765299
user_g	98	1.647613
user_d	92	1.546738
user_h	87	1.462677
Domain_A\user_d	28	0.470746
Domain_A\user_g	27	0.453934
Domain_A\user_e	23	0.386685
Domain_A\user_m	19	0.319435
Domain_A\user_n	18	0.302623
Domain_A\user_f	17	0.285810

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 marked increase in POST methods and a huge decrease in GET methods.
```

- What is that method used for?

```
The HTTP Post method is used to send data to a server in order to create or update a resource. The HTTP GET methods are used to request data from a source. DDoS attacks commonly use both HTTP Post and Get methods.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
No, other than there were markedly less active but the domain hierarchy remained the same.
```

Report Analysis for HTTP Response Codes

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

```
Yes, 200 response codes went down by over 5000, 404 response codes went up by over 400, and 304 response codes went down by over 300.
```

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, using a baseline of 74 and a threshold of 122.
```

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

```
It occurred from 8pm to 9pm with a count of 939.
```

- Would your alert be triggered for this activity?

```
Yes, it would have been triggered.
```

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

```
No, I would not change my previously determined threshold.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, using a threshold of 6 and a baseline of 2.
```

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

```
7 and 1296
```

- When did it occur?

```
2020-03-25 13:00 and 2020-03-25 20:00
```

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

```
Yes I would raise the threshold to 7 to avoid the false positive on the
13:00 time period.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
The spike in Get methods at 6pm and the spike in Post methods at 8pm.
```

- Which method seems to be used in the attack?

```
The Post method seems to be used for the attack.
```

- At what times did the attack start and stop?

```
The attack started at 7:30 pm and ended at 8:30 pm.
```

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

```
1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes there are more events associated with Ukraine.
```

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

```
Both Kyviv and Kharkiv in Ukraine have a volume of activity.
```

- What is the count of that city?

```
Kyviv has a count of 438 and Kharkiv has a count of 432.
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
There was over a thousand count increase in /VSI_Account_logon.php and
drastic decrease in /VSI_Company_Homepage.html
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
The attacker could potentially be conducting a brute force attack such as
password spraying.
```