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
```

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes
```

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

```
The attack occurred at 1pm-5pm
```

- When did it occur?

```
Thursday, Feb 20
```

- 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?

```
Yes
```

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

```
94 at 2AM, 70 at 9AM, 54 at 10AM
```

- Who is the primary user logging in?

```
user_K
```

- When did it occur?

```
9AM
```

- 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?

Yes

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes

- What signatures stand out?

```
“A computer account was deleted”
“The audit log was cleared”
“System security access was granted to an account”
“An account was successfully logged on”
"An attempt was made to reset an accounts password"
“A user account was created”
“A user account was changed”
“System security access was removed from an account”
“An account was successfully logged on”
“Special privileges assigned to new logon”
“A user account was deleted”
“Domain policy was changed”
“A process has exited”
“A user account was locked out”
“A privileged service was called”
“A process has exited”
“Password policy modified”
“A logon was attempted using explicit credentials”
“A user account was created”
```

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

```
“A computer account was deleted” 9-10 am
“The audit log was cleared” 9-10 am
“System security access was granted to an account” 9-10 am
“An account was successfully logged on” 1-2 am
"An attempt was made to reset an accounts password" 9-10 am
“A user account was created” 9-10 am
“A user account was changed” 9-10 am
“System security access was removed from an account” 9-10 am
“An account was successfully logged on” 9-10 am
“Special privileges assigned to new logon” 1-2 am
“A user account was deleted” 9-10 am
“Domain policy was changed” 9-10 am
“A process has exited” 9-10 am
“A user account was locked out” 1-2 am
“A privileged service was called” 1-2 am
“A process has exited” 1-2 am
“Password policy modified” 1-2 am
“A logon was attempted using explicit credentials” 1-2 am
“A user account was created” 1-2 am
```

- What is the peak count of the different signatures?

```
“A computer account was deleted” 59
“The audit log was cleared” 127
“System security access was granted to an account” 160
“An account was successfully logged on” 91
"An attempt was made to reset an accounts password" 64
“A user account was created” 127
“A user account was changed” 68
“System security access was removed from an account” 75
“An account was successfully logged on” 67
“Special privileges assigned to new logon” 71
“A user account was deleted” 72
“Domain policy was changed” 67
“A process has exited” 59
“A user account was locked out” 86
“A privileged service was called” 114
“A process has exited” 84
“Password policy modified” 75
“A logon was attempted using explicit credentials” 86
“A user account was created” 53
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes
```

- Which users stand out?

```
user_a, user_k
```

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

```
user_a: 1-2 am
user_k: 9-10 am
```

- What is the peak count of the different users?

```
user_a: 984
user_k: 1256
```

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

- Does anything stand out as suspicious?

```
Yes
```

- 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
```

- 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?

Advantages-with the right search query, you can find vulnerabilities. Disadvantages-it is easier to use the search bar to find the information if you are unfamiliar with dashboard setup.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, at 8AM there was an overwhelming amount of POST requests being made.

- What is that method used for?

The method is used to transfer data into a server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Yes, the referrer domain changed from http://semicomplete.com to http://www.semicomplete.com, with an overwhelming count of both being used.

Report Analysis for HTTP Response Codes

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

Yes, at 9PM there was an influx of successful HTTP responses in response to post request.

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes.
```

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

```
6pm and 8pm
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
Yes, I would give it more space because some false positives would have gone off.
```

Alert Analysis for HTTP POST Activity

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

```
Yes
```

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

```
1,296 POST requests were made.
```

- When did it occur?

```
8PM
```

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

Yes, I would make it higher to avoid false positives.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, at 6pm and 8pm there is a spike in web activity.

- Which method seems to be used in the attack?

POST

- At what times did the attack start and stop?

The attack started at 8:05PM and ended at 9:05PM

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

1,296

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

New York and Washington have an influx of traffic

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

Washington, D.C

- What is the count of that city?

668

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
There is a high amount of hits for the login page and for a subdirectory of
the web server.
```

- What URI is hit the most?

```
/VSI_Account_logon.php
```

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

```
Brute forcing the log in page.
```