



Cybersecurity

Project 3 Review Questions

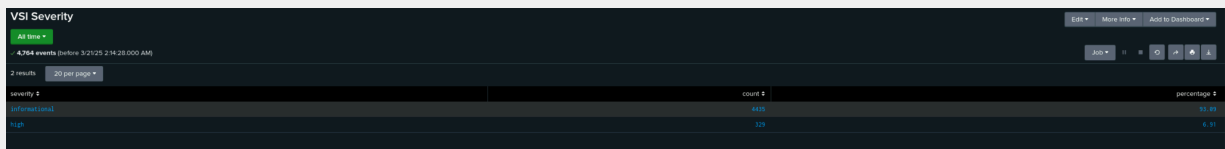
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, early in the morning on March 24th 2020 from 12am to 11am experienced a higher severity than usual, totaling around 6.91% of the total logs from that time period, being a total high severity number of 329.



severity	count	percentage
Informational	4425	97.02
High	329	6.91

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Not anything too alarming for a day to day standpoint. Successes account to 97.02% with a total of 4622 successful statuses, while 2.98% of requests were met with a fail status.

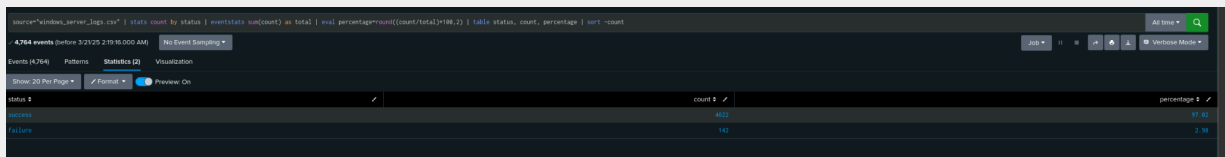


status	count	percentage
Success	4622	97.02
Failure	140	2.98

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Originally after observing the first set of logs it seemed business as usual, nothing out of the ordinary. However, when using the same alert for the attack_logs portion, it shows an obvious spike of failed activity without a doubt.



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

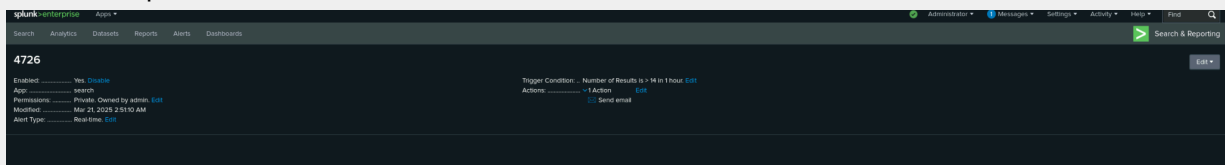
91 events in total, 35 events in 1 single hour being the notable spike.

- When did it occur?

March 25th 2020 is the date, from the hours 12am to 2pm. The spike occurred at 8am.

- Would your alert be triggered for this activity?

Yes, the alert I chose would have worked perfectly. It is in my opinion a little low, and in hindsight would have still worked, but should still be higher despite the success. I chose the alert number of 9, and the only spike of 35 would have been alerted, but to eliminate false positives I would bump it to around 15.



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

Yes, as stated in the previous answer, it should have been bumped up to at least 15, despite the success.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Like the previous alert we analyzed, when looking at the base logs it was a normal snapshot of daily server activity; But when inputting the attack logs it shows clear as day that the servers underwent a cyberattack.

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

Like the previous analysis', the date is March 25th 2020, with the snapshot taking place between 12am to 2pm. The total event counts 432, with the spike of 196 events taking place at 11am.

- Who is the primary user logging in?

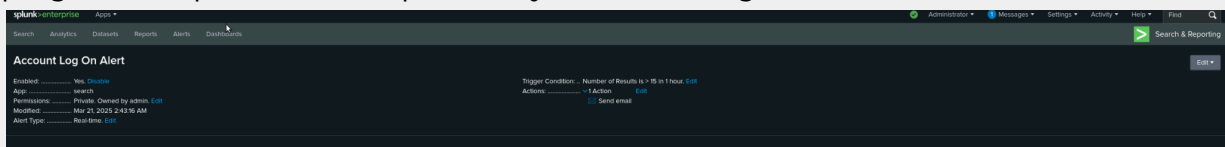
DOMAIN-A\SYSTEM and user_k were the highest counts of logins during this time.

- When did it occur?

Largest spike occurred at 11am on March 25th 2020.

- Would your alert be triggered for this activity?

Yes, but like before should have been set higher, as it would have been pinged multiple times despite only 1 hour being the bulk of the attack.



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

The alert threshold I set was a total of 15 events. This was too low, as my alert would have been pinged a total of 3 times, only 1 of those needed to be accounted for, and that being a total of 196, crushing the 15 count alert. If I were to set it again, a more appropriate number would be around 50, to truly show an attack and not simply a larger number of normal traffic.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Not necessarily in either of the logs provided. In the standard logs the highest spike was 22 which was high but not out of the ordinary, where in the attack logs the highest hourly event count was 17 deleted accounts.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Comparing on my dashboard I prepared of both the standard and the attack logs, like the previous statements the attack logs stand out as suspicious. The signatures of 'An attempt was made to reset the accounts password' with 2,128 signatures, and 'A user account was logged out' with a total of 1,811 events.

- What signatures stand out?

An attempt was made to reset the accounts password and A user account was logged out.

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

For changing the passwords it occurred between 9 to 11am on March 25th 2020 and for the users logged out it spiked between 1am and 3am the same day.

- What is the peak count of the different signatures?

Peak count of 'A user account was logged out' was 1,811 events and 'An attempt was made to reset the accounts password' was 2,128 events.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

With my dashboard I curated for the project, like before, the attack part of my dashboard stands out significantly in contrast to the unattached logs.



- Which users stand out?

User_K with 35.6% of activity and User_A with 31.5% of activity.

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

User_K attack started at 9am on Wednesday the 25th of March 2020 with a total of 1,256 events, followed by the 10am spike of 761 events the next hour, then stopping by 11am. For User_A it was the same day, at 1am the events spiked at a total of 799, followed by the next hour of 984 events at 2am, then stopping by 3am.

- What is the peak count of the different users?

User_K with a total of 2,017 events and User_A with 1783 events.

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

- Does anything stand out as suspicious?

Besides the already discussed inconsistencies between the standard and attack logs, everything lined up as expected.

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

Yes, as reported before with proper alerts and dashboards you can make educated assumptions.

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?

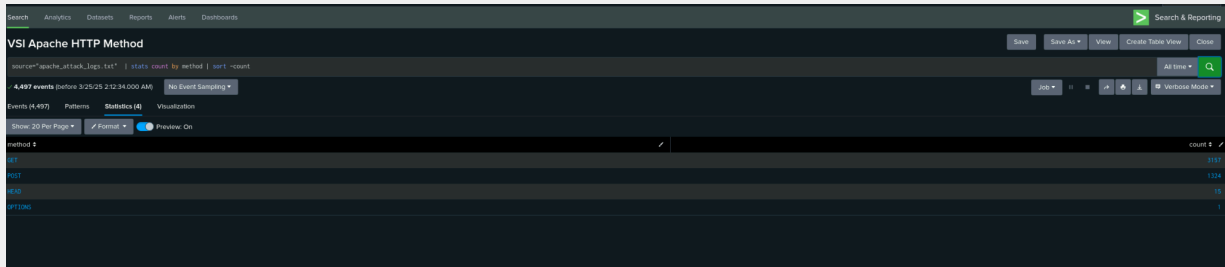
One of the advantages is that it is a simplified way to see outliers in a set of data if the creator of said stats chart put it together properly. A disadvantage is the lack of being able to properly account for time while using a bar graph, the only thing comparable with time is line chart, which doesn't work with all sets of statistical data.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, with the standard subset of Apache logs, there were a total of 9,851 GET requests and 106 Post Requests; Compared to the 3,157 GET requests and 1,324 POST requests after the Apache attacks.



- What is that method used for?

The GET requests are used to request data from the Apache server, and the POST requests are used to send data to the server or create/update a resource on that server.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No, in terms of the referrer domains from both sets of logs, nothing stuck out as suspicious.

Report Analysis for HTTP Response Codes

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

Slightly, 200 response went from 9,126 counts, when attacked dropped to 3,746, which means the request went through 'OK'. 404 response codes went from 213 on the unattached logs, whereas they jumped to 679, which means there was a 3x increase in 'Page not Found' response.

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

100% indicator of an attack comparing the 2 logs. While there are between the ranges of 20-50 an hour of non-US IP connections, the attack logs occurred a major shift.

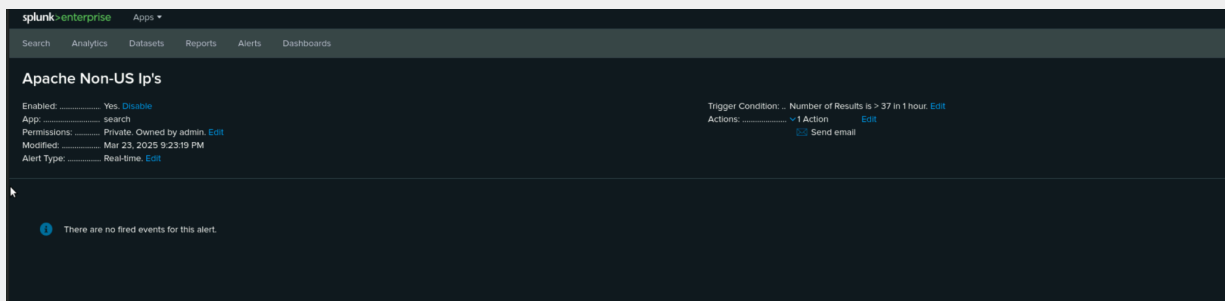


- If so, what was the count of the hour(s) it occurred in?

At exactly 8pm there was a massive uptick of 432 non-US IP's connected.

- Would your alert be triggered for this activity?

Yes, albeit like a few of my other alerts it was too conservative. It would have an alert at 37, but so would many many things, and lead to a great deal of false positives.



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

Yes, I would change it to an easy 150 to truly encapsulate an attack.

Alert Analysis for HTTP POST Activity

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

Most definitely, after the attack occurred there was a colossal uptick in POST requests, 1,324 to be exact.

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

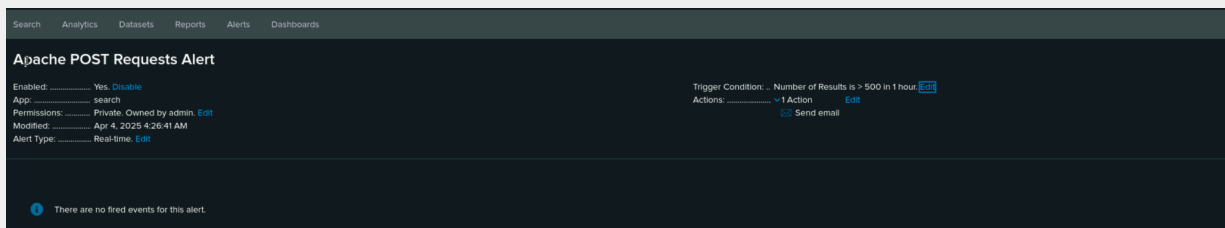
The peak was from 8pm to 9pm with a total of 1,296 POST requests.

- When did it occur?

The attack on this seems to have occurred on March 25th 2020 at 8pm.

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

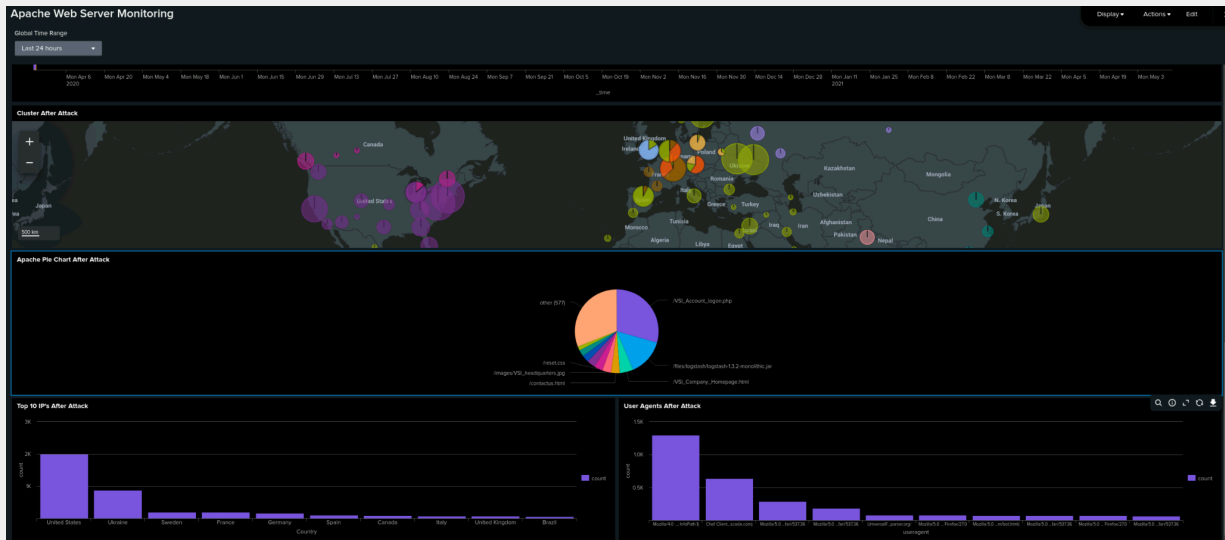
This one was perfectly fine, my alert was an even 500, triggering a proper alert on this with no chance of a false positive.



Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

As previously stated, these GET and POST requests show an attack occurred without a reasonable doubt.



- Which method seems to be used in the attack?

It seems to be the GET | POST Methods

- At what times did the attack start and stop?

For the GET requests they peaked between the hours of 5:00pm to 7:00pm. The Post Requests had a peak uptick from the following hours, 7:00-9:00pm.

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

For the GET requests it peaked at 3,157, and for the POST it peaked at 1,324.

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Most definitely shows aspects of attacks. On a daily basis, the top 3 countries represented being overwhelmingly being #1 United States, #2 being France, followed by a small #3 of Germany. Post attack it shows that the United States is still #1 with 2,000 of the total IP's, followed very closely with Ukraine at #2 with a total of 877 of the total IP's. To put it

in perspective, in the base daily amount the United States was 3,860 followed by a measly 859 IP's comparatively.

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

This is Ukraine as mentioned beforehand. Specifically the city of Kiev.

- What is the count of that city?

For just Kiev it is a total of 440 IP's. Kharkiv is also a large factor, being 432 IP's.

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, on a standard day the most connected to URI was the Company homepage, "VSI_Company_Homepage.html", where after the attack occurred, that changed to the account logon page "VSI_Account_logon.php" followed by a file pull on a .jar file.

- What URI is hit the most?

The URI hit the most after the attack was the logon page, "VSI_Account_logon.php". It was accessed 1,323 times, making it 29.4% of all traffic. This is followed closely by, "/files/logstash/logstash-1.3.2-monolithic.jar" URI with it being accessed 638 times, making it 14.2% of traffic.

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

It seems as if the attack was meant to brute force the website and hoping VSI would have improper password policies, being able to be accessed. Following the successful login, they seemed to have downloaded a swash of important company data.

