Unit 19 Homework: Protecting VSI from Future Attacks

Scenario

In the previous class, you set up your SOC and monitored attacks from JobeCorp. Now, you will need to design mitigation strategies to protect VSI from future attacks.

You are tasked with using your findings from the Master of SOC activity to answer questions about mitigation strategies.

System Requirements

You will be using the Splunk app located in the Ubuntu VM.

Logs

Use the same log files you used during the Master of SOC activity:

- Windows Logs
- Windows Attack Logs
- Apache Webserver Logs
- Apache Webserver Attack Logs

Part 1: Windows Server Attack

Note: This is a public-facing windows server that VSI employees access.

Question 1

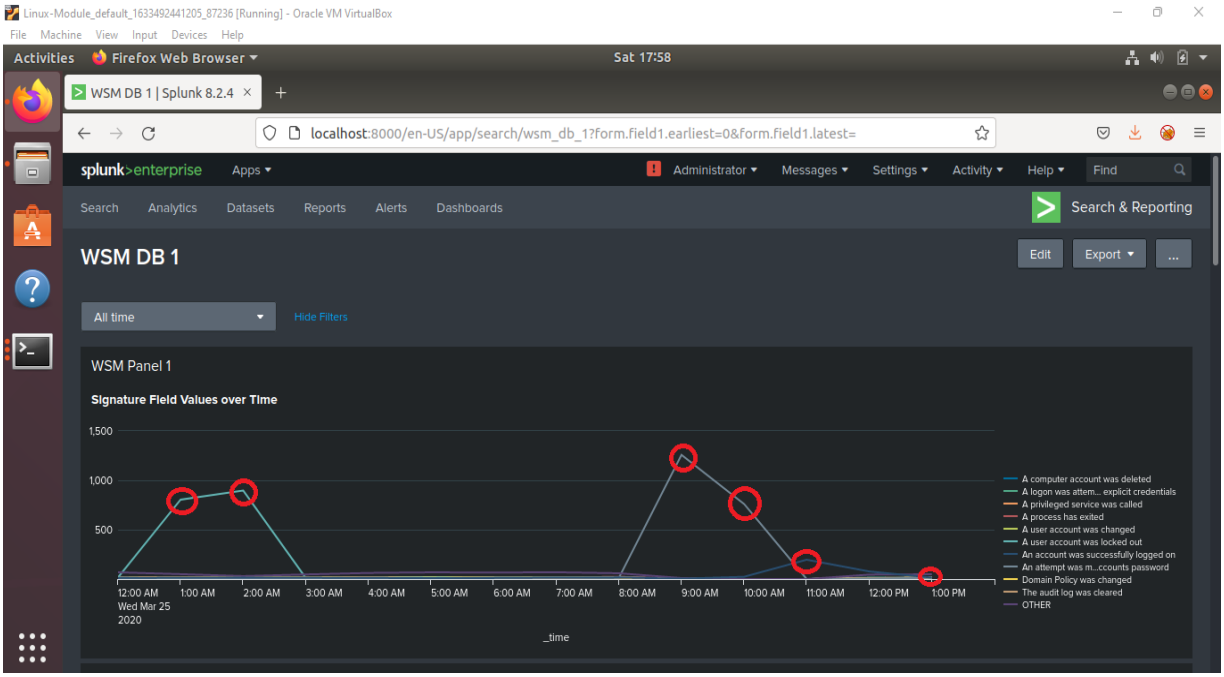
- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

Answer/Solution:

Below are the observations from the attack signatures on the 25th March:

- User account was locked out: Started around 1 a.m. and ended at 3 a.m. on March 25th. The peak count was 896.
- An attempt was made to reset a user's password: Started around 9 a.m. and ended at 11 a.m. on March 25th. The peak count was 1,258.
- The account was successfully logged on: Started around 11 a.m. and ended at 1 p.m. on March 25th. The peak count was 196.

The below screenshot shows the peak activity for the above 3:



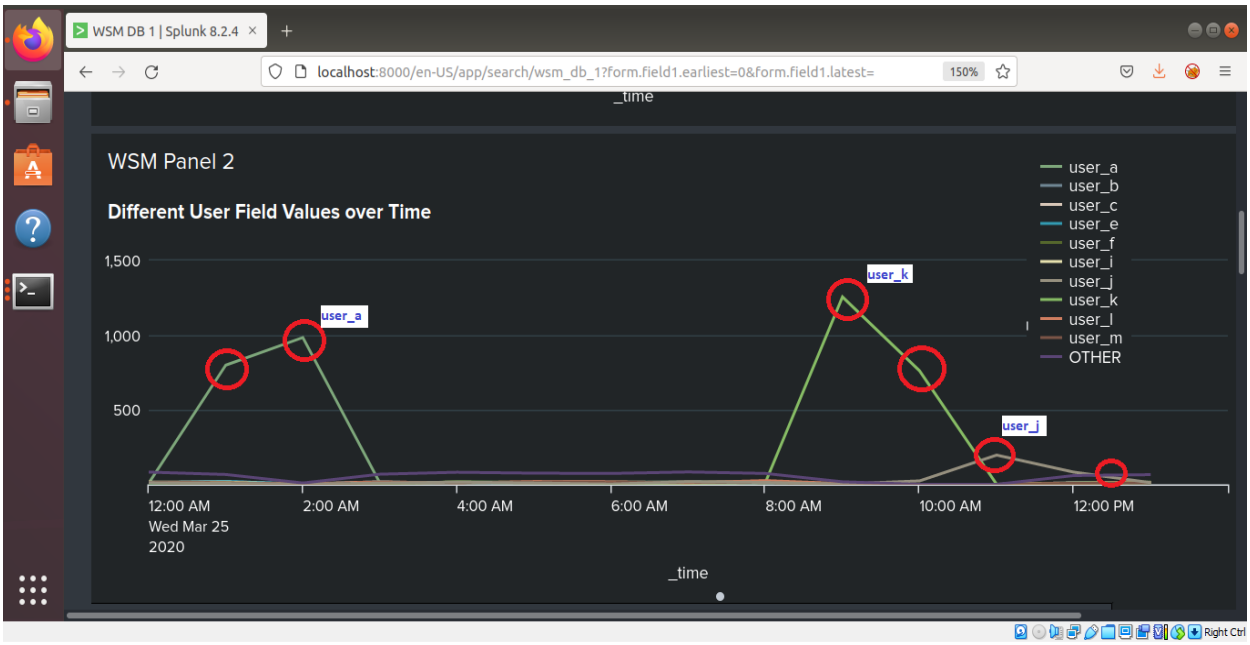
Global Level Mitigation:

- Implement multi-factor authentication for the systems, which would make it difficult for a threat actor to easily get access into the systems.
- The duration between multiple attempts to reset passwords should be made longer to avoid too many trials at one time.
- A group policy could be set up company-wide that would automatically unlock users accounts after a specific amount of time.
- If three or more "Bad Logins" were detected originating from a single IP address (that is not a VSI IP address), that IP address should be blacklisted and prevented from accessing the user account login in the future.

Individual Level Mitigation:

The below screenshot shows suspicious activity for 3 users-user_a, user_k and user_j:

- **User A: Started around 1 a.m. and ended at 3 a.m. on March 25th. Peak count was 985.**
- **User K: Started around 9 a.m. and ended at 11 AM on March 25th. Peak count was 1,256.**
- **User J: Started around 11 a.m. and ended at 1 p.m. on March 25th. Peak count was 196.**



-

• **For user_a:** *The user account was locked out.* This indicates that the attacker is trying to brute force their way to the user's password to access the account. **Mitigation**:user_a should change their password immediately to something completely different and ensure that the complexity is high.
• **For user_k:** *An attempt was made to reset an account password.*

There were several attempts to reset the password for this user, but the logs do not show any evidence that the attacker was successful in logging into the user's account or being able to successfully reset the password for user_k.

Mitigation: An user-specific alert should be set up with lower configured values and the account should be monitored closely to analyze if password changes happen again for this user.

- **For user_j:** *The account was successfully logged on.*

For this user, the log shows that the attacker was able to successfully obtain the user's password.

Mitigation: The user needs to manually change the password. Another step could be similar to what was used for user_k-create a user-specific alerts to watch the users activity more closely.

All other users had accounts either created or changed.

Question 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

Answer/Solution:

Mitigation: If three or more "Bad Logins" were detected originating from a single IP address (that is not a VSI IP address), that IP address should be blacklisted and prevented from accessing the user account login in the future.

As soon as VSI finds out about this attack, employees should be notified immediately to be more vigilant and careful about who they accept information from.

Part 2: Apache Webserver Attack:

Question 1:

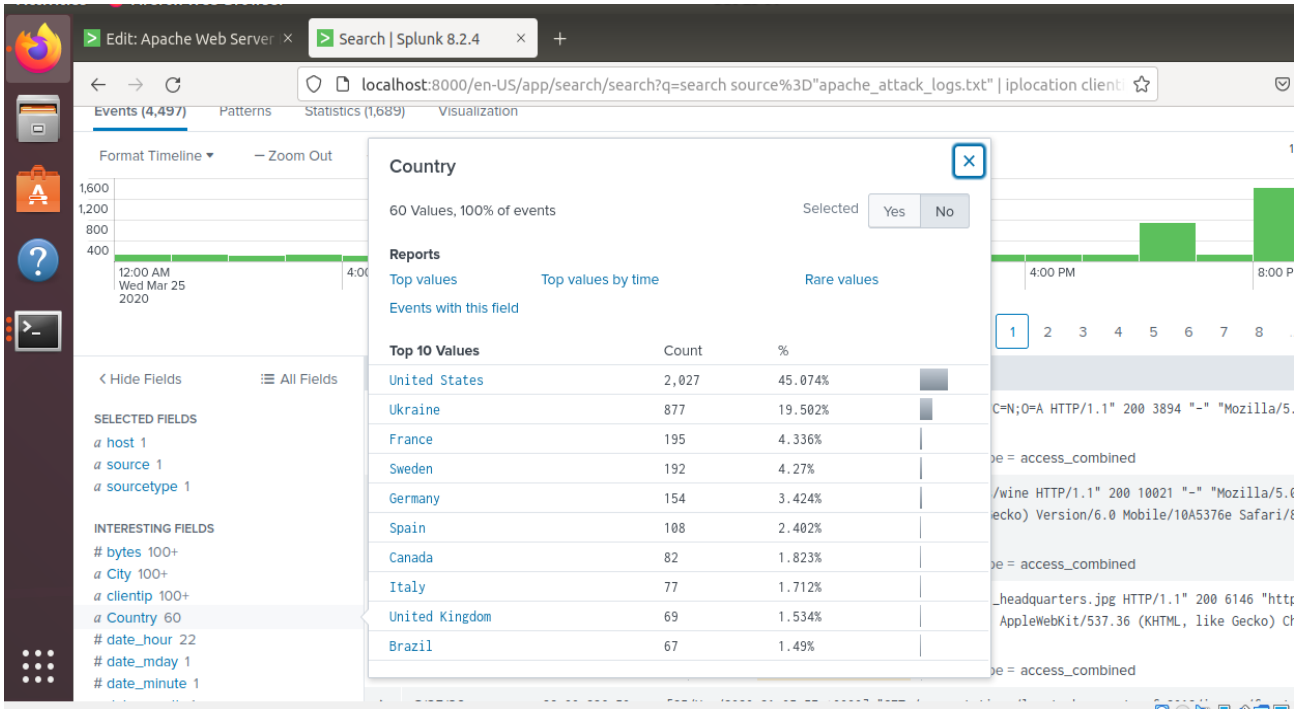
- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
    - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic map that justifies why you created this rule.

Answer/Solution:

Based on the search on the GEO Map, VSI's Apache Webserver was attacked on March 25, 2020 between the hours of 6:00 PM and 9:00 PM. The incoming attacks were mostly coming from Ukraine, therefore we should set up a firewall rule to block HTTP traffic from Ukraine.

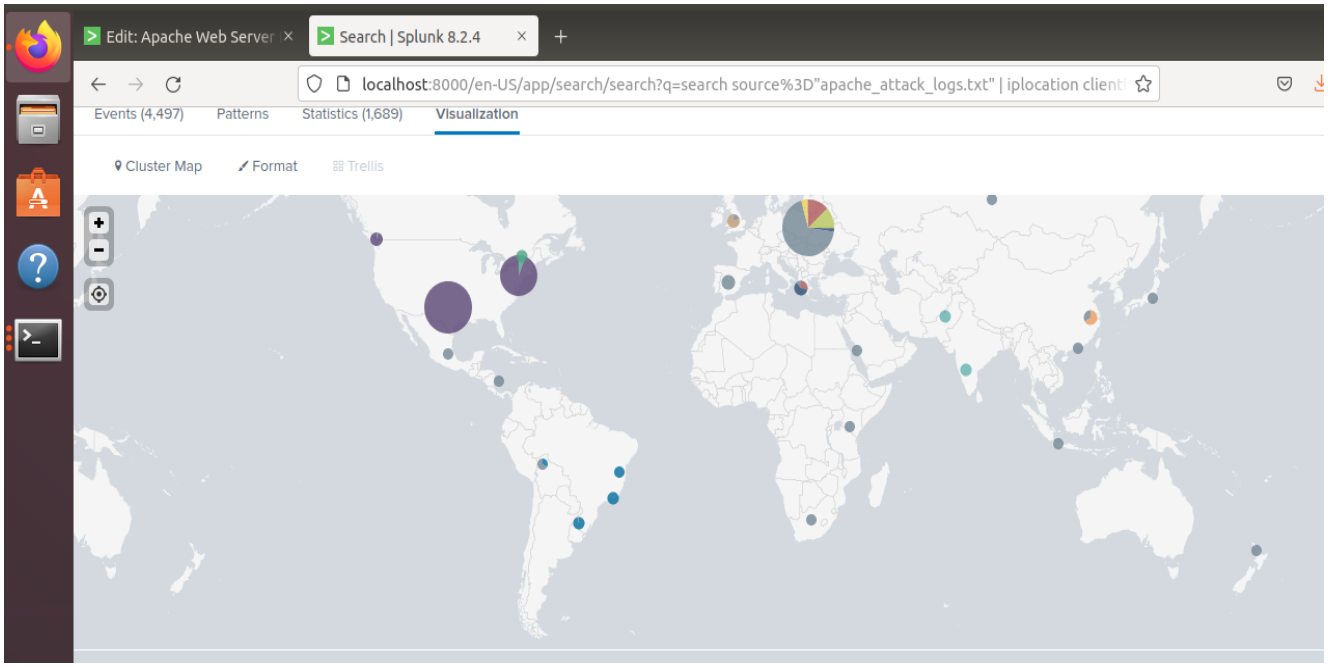
Firewall Rule Description - "Block all incoming HTTP traffic where the source IP comes from Ukraine"

Below is a screenshot of the attack origination based on country :



The below screenshot shows Ukraine's incoming HTTP Traffic, which can be got from the below search in SPLUNK:

source="apache_attack_logs.txt" | iplocation clientip | geostats count by Country



Question 2

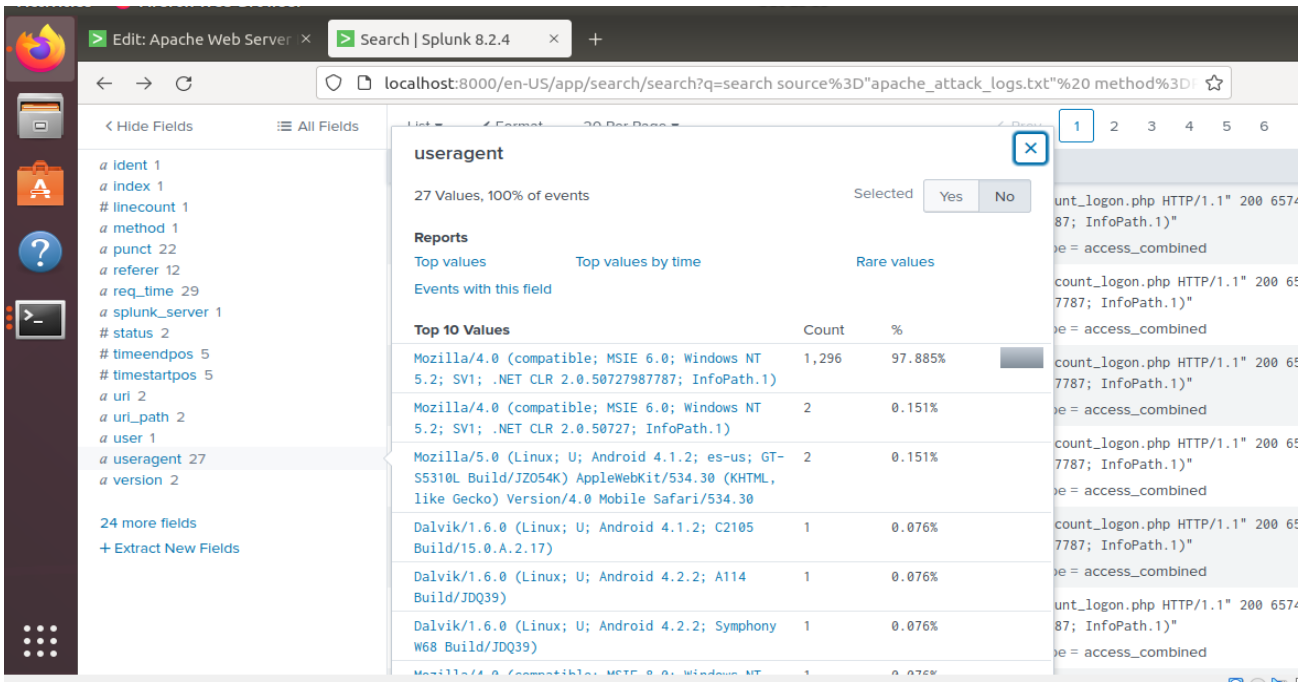
- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.
- What other rules can you create to protect VSI from attacks against your webserver?
    - Conceive of two more rules in "plain english".
    - Hint: Look for other fields that indicate the attacker.

Answer/Solution:

RULE 1: "Block all incoming HTTP traffic where the useragent is "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)."

Looking at the below screenshot, the search: source="apache_attack_logs.txt" method=POST

The user agent is which has the maximum attack percent is : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1



RULE 2:"Block all incoming HTTP traffic which generates three or more consecutive POST requests to the login page ("/VSI_Account_logon.php")."
Below is a screenshot of the uri_path that takes the maximum hits, hence a rule should be configured for how this php page is accessed. This would prevent any brute-force attacks on the login page, regardless of source IP.