SIEM II

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 Web Server Logs
- Apache Web Server 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.

  I would implement an account lockout that will be triggered if a set amount of logins fails had been met. I would create a login fails threshhold number based on the normal vs unusual number of events.

  Two factor authentication. Strong password requirements which include length, numbers, and caracters. Change password on a regular basis. If the account is on lockeout, then

there should be a wait period for resetting the account, and will require authentication via the user email account.

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?

Block anyone that is trying to use the same password for multiple users at the same time, and will not lock an account when the exact password entered multiple times, but will have to re-authenticate the user via email or any other means of 2 factor authentication.

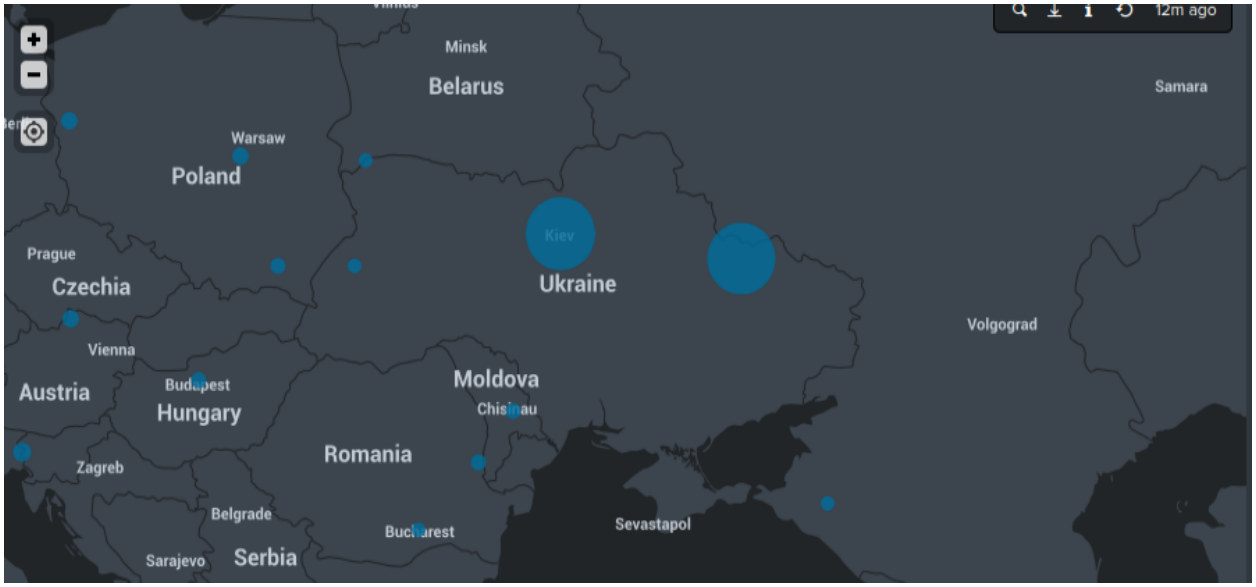
Part 2: Apache Webserver Attack:

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."

Block all incoming HTTP traffic where the source IP comes from Ukraine.

- Provide a screenshot of the geographic map that justifies why you created this rule.



Question 2

- VSI has insider information that JobeCorp will launch the same web server 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.

Send an alert email for HTTP POST from outside the United States that goes over 100 events in an hour

Send an alert email for HTTP GET for /files/logstash/logstash-1.3.2-monolithic.jar for events that exceed 100 in an hour

Guidelines for your Submission:

In a word document, provide the following:

- Answers for all questions.
- Screenshots where indicated

Submit your findings in BootCampSpot!