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.
    - VSI should require all employees to use strong passwords with two-factor authorization.
    - Restrict access to authentication URLs
    - Limit login attempts to 10 per user and then lock them out if they exceed that.
    - You could also use CAPTCHAs
    - Employees should make sure to use passwords that are not easy to guess

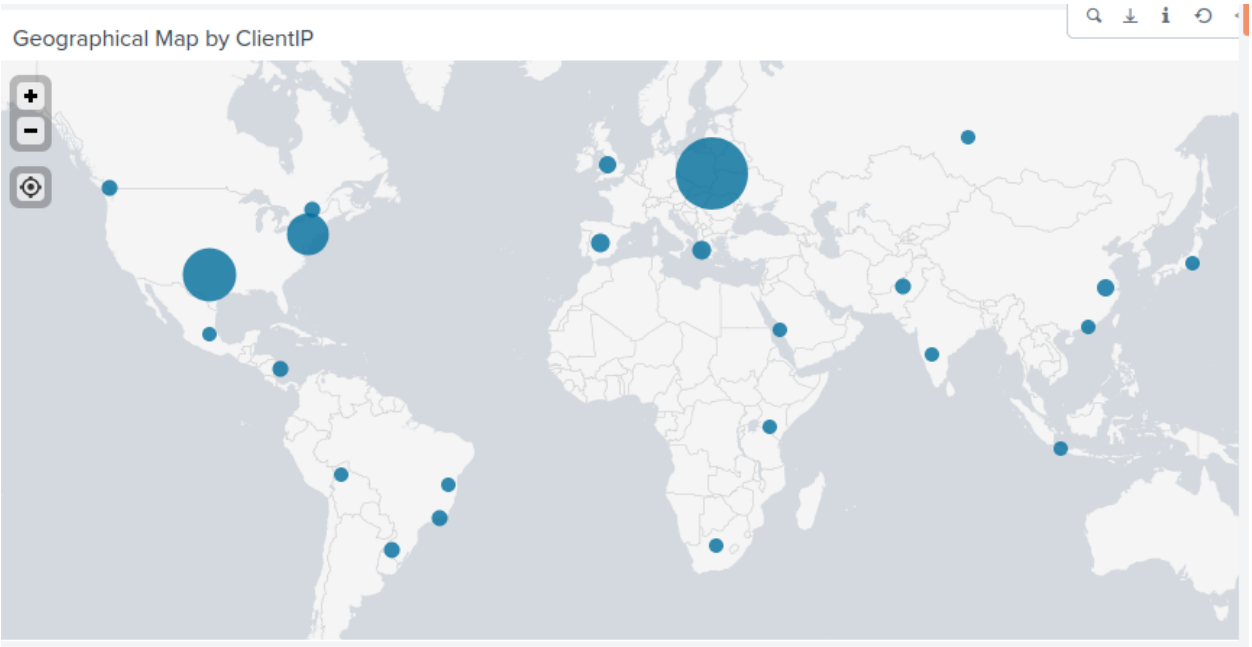
Question 2

- 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?
    - A mitigation could be to lock out any user that has exceeded the failed logins and block that user out if their IP is not a VSI IP address.

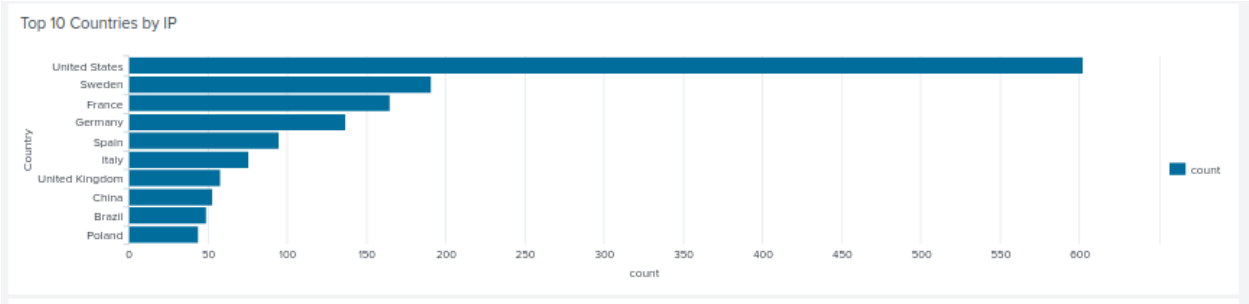
Part 2: Apache Webserver Attack:

Question 1

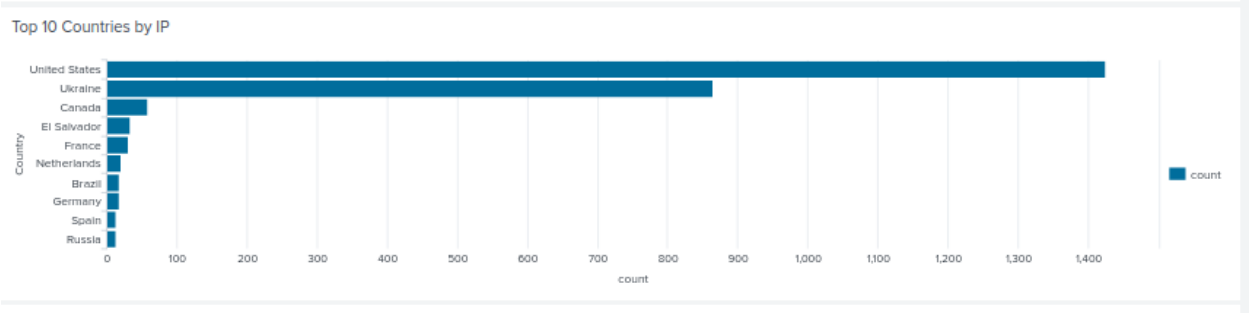
- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
    - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic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



IPs before the attack:



IPs during the attack



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.
- Block any IP address that has 3 or more POST requests to the URI of /VSI_Account_logon.php
- Block any IP address that has 3 or more POST requests using the user agent of Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)

Guidelines for your Submission:

In a word document, provide the following:

- Answers for all questions.
- Screenshots where indicated

Submit your findings in BootCampSpot!