Sasha Shahidi

Unit 19 Homework: Protecting VSI from Future Attacks

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.

  There are several mitigations that I would recommend VSI to take in order to ensure that each user account is protected. One mitigation would be to block unknown IP addresses so that only known and local IP addresses can have access, making it more likely that it is a VSI employee trying to gain access. Another mitigation is to lock out user accounts after a small number of failed log-in attempts, and send an alert to the SOC, in order to deny access and investigate the potential attack. Another mitigation would be to limit the number of password reset attempts that could be made in an hour, and send an alert to the SOC when the threshold is met, in order to further investigate the source of the increased attempts. However, resetting passwords for employees should still be encouraged because it is a best practice. Another mitigation would be to send an alert to the SOC for investigation if a threshold is met for successful log-ins, as it could mean a potential attack underway if the number exceeds normality for VSI.

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 strategy that I would recommend would be to teach users to always consider the source of sensitive information they receive and to confer with the SOC if they have suspicions about certain credentials before inputting them and getting locked out. Another mitigation would be to have some sort of consistency in creating login credentials so that users can ignore bad logins that are not consistent with the style that VSI has implemented. There should however be inherent differences between user credentials for increased security.

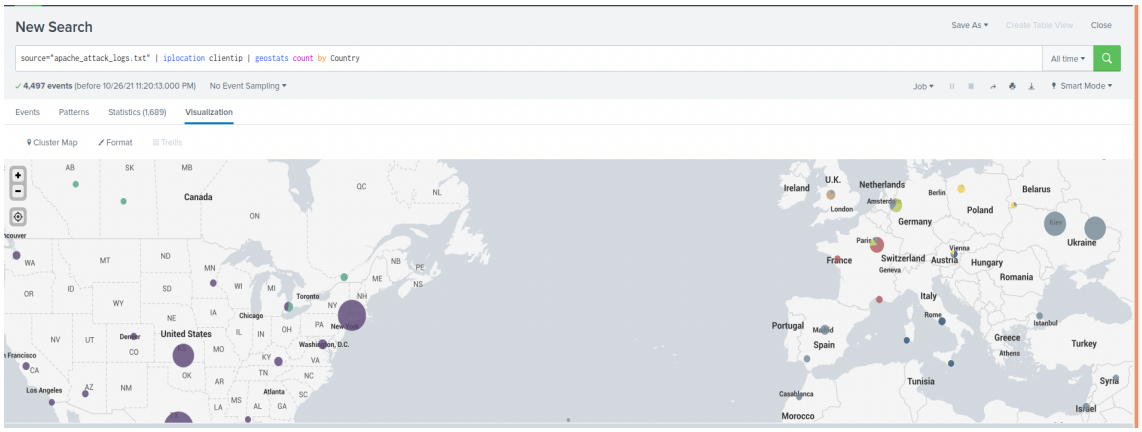
Part 2: Apache Webserver Attack:

Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.

  source=”apache_attack_logs.txt” | iplocation clientip | top limit=20 Country
- 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."

    Use the Apache Attack Logs file to pull the location of client IP addresses and sort them by the top 20 countries with the most counts
- 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 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.

    1. Use the Apache Attack Logs file to pull the count of potential attacks that occur within the same date and hour
    2. Use the Apache Attack Logs file to pull the different file types and the count of each to investigate potential attacks