**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](/the-university-of-western-australia/waus-virt-cyber-pt-05-2021-u-lol/-/blob/master/Unit%2019%20-%20SIEMs%202/Homework/resources/windows_server_logs.csv)
* [Windows Attack Logs](/the-university-of-western-australia/waus-virt-cyber-pt-05-2021-u-lol/-/blob/master/Unit%2019%20-%20SIEMs%202/Homework/resources/windows_server_attack_logs.csv)
* [Apache Webserver Logs](/the-university-of-western-australia/waus-virt-cyber-pt-05-2021-u-lol/-/blob/master/Unit%2019%20-%20SIEMs%202/Homework/resources/apache_logs.txt)
* [Apache Webserver Attack Logs](/the-university-of-western-australia/waus-virt-cyber-pt-05-2021-u-lol/-/blob/master/Unit%2019%20-%20SIEMs%202/Homework/resources/apache_attack_logs.txt)

**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.

User\_a :

User had their account locked after a large amount of log in attempts. Suspected brute force could be mitigated with a lockout time period for more than 5 log in attempts and an email sent to the user.

User\_k

User had an excessive amount of password reset attempts. Mitigation would be to limit the amount the reset attempts that can be requested in a day. Also emailing the user to alert them to the reset attempts.

To protect users accounts VSI could implement a lock out period of increasing time with failed login and password reset attempts and email the user that their account has been locked. Implementing 3 factor authentication would help mitigate this issue also setting up and alert for these attempts so VSI can block IP address is also something they can look at.

**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?

One mitigation would be to block JobeCorb entirely, you can also set up an alert for a high number failed user login. Educating the employees in best user practices is highly recommended as humans tend to be the weakest link when it come to security.

**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.

The attacks look to be coming from within Europe. You can block all traffic from Europe due the attack alternatively, you can block all users from outside the USA. As the company is based in the USA most users should not be accessing accounts from outside the country.

Graphical user interface, application, map

Description automatically generated

**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. Most of the attacks are coming from Mozilla 4.0 and 5.0 which are old versions of Firefox. We can block all traffic from that version of Mozilla.
2. All attacks come from HTTP/1.0 or 1.1. We should only accept traffic from the newer versions HTTP/2.0 and above.

**Guidelines for your Submission:**

In a word document, provide the following:

* Answers for all questions.
* Screenshots where indicated

Submit your findings in BootCampSpot!