**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](/University-of-Minnesota-Boot-Camp/uofm-stp-cyber-pt-03-2021-u-c/-/blob/master/19-SIEMs-2/Homework/resources/windows_server_logs.csv)
* [Windows Attack Logs](/University-of-Minnesota-Boot-Camp/uofm-stp-cyber-pt-03-2021-u-c/-/blob/master/19-SIEMs-2/Homework/resources/windows_server_attack_logs.csv)
* [Apache Webserver Logs](/University-of-Minnesota-Boot-Camp/uofm-stp-cyber-pt-03-2021-u-c/-/blob/master/19-SIEMs-2/Homework/resources/apache_logs.txt)
* [Apache Webserver Attack Logs](/University-of-Minnesota-Boot-Camp/uofm-stp-cyber-pt-03-2021-u-c/-/blob/master/19-SIEMs-2/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.

**Global mitigation:**

-All passwords will have to change every 3 months

-passwords must have specifications (characters, upper case letters, numbers, etc.

-Alerts will be sent to SOC team once thresholds are met

**Individual users Mitigation:**

-Account will lock out after 12 attempts

-User can only log onto account 15 times within an hour

**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?

**I would recommend a set amount of accounts to have failed log ins in a certain amount of time until the ICMP or whichever application used will divert to a fail safe lock down to protect the company and the network.**

**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 traffic where the source IP is from Germany because we don’t provide services for that country at this time.**

Graphical user interface, application

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. **Require password change after lock out**
2. **If a certain amount of accounts are locked on close down system to find breach / attack**

**Guidelines for your Submission:**

In a word document, provide the following:

* Answers for all questions.
* Screenshots where indicated

Submit your findings in BootCampSpot!