**Week 19 Homework**

**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.

Chart

Description automatically generated with medium confidence

Graphical user interface, application

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated with low confidence

Graphical user interface, text, application, email

Description automatically generated

Based on the search information, it appears that user\_a caused 1,686 account lockout signatures between 1 AM – 3 AM.

Graphical user interface, text

Description automatically generated

Based on the search information, it appears that user\_k caused 2,021 account reset attempt signatures between 9 AM – 11 AM.

* 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.

It seems that these mitigations should be applied:

* General Mitigations for both problems.
  + Setting up alerts for both events/signatures. For certain users, such as admins or those with infrastructure access, having a lower threshold would be ideal.
  + If the attack signatures are coming from only a few user accounts, doing a security scan on their computer(s) could be beneficial.
* Problem: “A user account was locked out”
  + Since this is Windows based, creating an **Account lockout threshold** policy with a reasonable threshold. Microsoft recommends the threshold to be 10 attempts.  
    Source: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold>
  + Add **Account lockout duration** threshold. Microsoft advices 15 minutes.  
    Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration
* Problem: “An attempt was made to reset an accounts password”
  + Have a self-service password reset that includes security questions. This would make it harder for attackers to spam account resets since the barrier to do so would be higher.
  + Require Multi-Factor Authentication (Duo or Microsoft Authenticator, depends on the password reset location for users) to login and to change account settings. This is something we do at my work.

**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?

Mitigations:

* Require the use of Multi-Factor Authentication.
* Require the user going through a VPN to increase security.
* Have conditional access, if possible.
* Only allow login attempts based on IP or Range.
* Making sure group policies and access are limited to only what the user(s) needs.
* Setting up alerts based on EventIDs.
* Have 24/7 Log Monitoring

**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."
  + **Answer:** Block all incoming HTTP traffic where the source IP comes from Kiev and Kharkiv, Ukraine.
  + **Answer:** Block all incoming HTTP traffic where the source IP is not in regions where the company operates.
* Provide a screen shot of the geographic map that justifies why you created this rule.

Map

Description automatically generated

Timeline

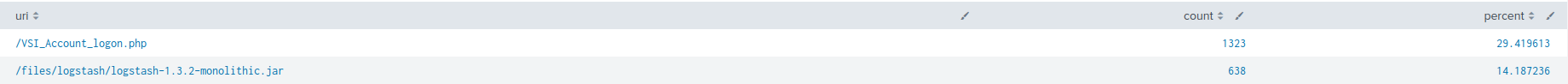
Description automatically generated

**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.

Chart

Description automatically generated with medium confidence



A picture containing bar chart

Description automatically generated

Looking at March 25, 2020, there was a spike in POST method usage between 7 PM – 9 PM with the top UFI being /VSI\_Account\_logon.php. With this information it seems that JobeCorp will try to use another brute force attack.

Rule Mitigations:

1. Assign unique login URLs to users.
2. Block IP addresses that have multiple failed login attempts.