**HW 19: SIEMS PART 2**

**Part 1: Windows Server Attack**

Note: This is a public-facing windows server that VSI employee 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 mitigations for the Company:**

1. ***Password Length:***

The first step towards Brute Force Attack prevention should be longer password length. Enforce users to create a password of certain length (8 – 16 characters).

1. ***Password Complexity:***

Another important thing is to create a complex password. It is not recommended to create passwords like ‘ilovemycountry’ or ‘password123456’; instead, the password should consist of UPPERCASE and lowercase alphabets and should also have numbers and special characters. Complexity of the password delays the cracking process.

1. ***Limit Login Attempts/IP lockout:***

Simple yet powerful action is to limit the login attempts. For example, if there is a certain number of failed login attempts; it should block that IP for a certain period to stop further attempts being made.

1. ***Delaying the response time.***

The more time between permitted password attempts, the more slowly the brute force attack will proceed, and the more time is available for sysadmins to discover an attack is underway.

1. ***Using Captcha:***

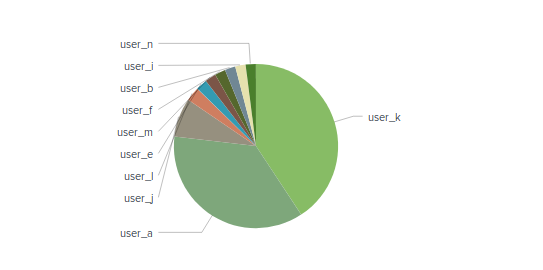
Captchas are now commonly used in websites. They prevent bots from executing automated scripts mainly used in Brute Force attack.

1. ***Brute force site scanners.***

The idea behind these tools is to go through site logs looking for signs that a brute force exploit has recently been attempted.

**Mitigations specific to each user:**

The pie chart depicts the top user after the windows attack:

The users that have suspicious activity are users A, K, and J.

**The mitigation strategies to be considered specific to users are:**

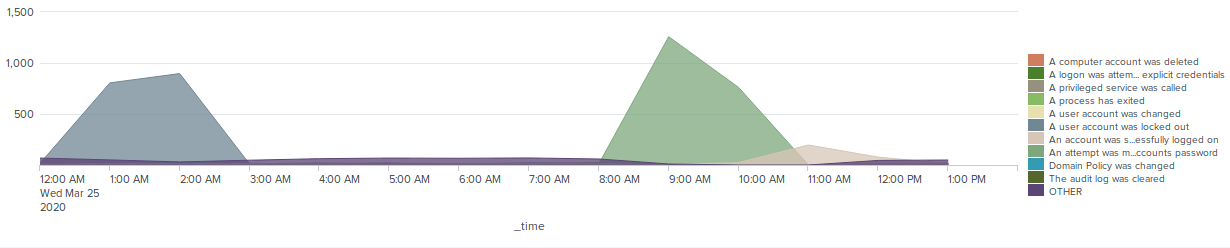
1. Enforce password length and complexity policy
2. Enforce change passwords regularly.
3. Security questions after account lockout.

**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 for this could include monitoring access controls so accounts do not have the ability to send "Bad Logins" to every user.

Use of CAPACHA.



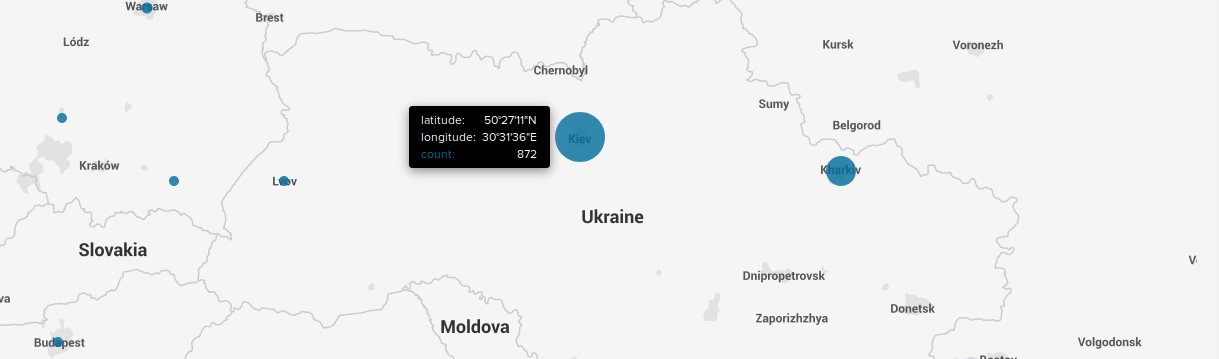
**Part 2: Apache Webserver Attack:**

**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 the city of Kiev, Ukraine”

"Block all incoming HTTP traffic where the source IP comes from the city of Kharkiv, Ukraine”



#### Dashboard analysis for cluster amp showed there is suspicious activity in Ukraine. When zoomed in, we can see the cities in Ukraine are:

* + - Kiev: Count of 872
    - Kharkiv: Count of 432

**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.

Whitelist all IPs within the company network and check fields for location.

Blacklist all IP s coming from that location.