**Unit 19 Homework: Protecting VSI from Future Attacks**

Part 1: Windows Server Attack

Question 1

There are several actions we should take after this attack.

To start, it is highly likely that the accounts for user m, user k, and user a are compromised in some fashion. User m was the source user for 2,021 of the attempts at resetting an account’s password, where the majority of these occurred over a 2 hour period, starting at 9 AM. Meanwhile, user k was the user of 2,021 attempts of a password reset. Furthermore, earlier on, user k was the source user of more than 1,600 account lockouts over the course of 2 hours, starting at 1 AM, and user a was the user for a similar number of those. This indicates suspicious activity with these three accounts. I would recommend for the time being we change the passwords and lock these accounts while we investigate further. (Though it’s possible that user a’s account was just a victim, rather than being hijacked.)

Other things we could do include setting up alerts for a large number of password reset attempts (i.e., 30+ in one hour) or large numbers of account lockouts (30+ in one hour as well). Another we might consider is creating an alert, or even preventing further action when a single account makes more than 50 password change or lockouts in 1 hour.

Question 2

We need to prevent the flood of bad logins locking out all our accounts. One thing we may want to do is, when we detect that one machine or user has caused multiple account lockouts, we prevent that machine from taking any more actions that could lead to account lockouts. Another thing we may do is change our login names to be a bit more complex than user\_a, user \_c. This would make it harder for them to guess the names of the accounts, making it harder to lock them out.

Part 2: Apache Webserver Attack

Question 1

An large amount of suspicious activity was coming from Ukraine. Specifically, it was coming from the cities of Kiev and Kharkiv. I would recommend that we implement a firewall rule blocking all http traffic from IP addresses within these two cities. Below are pictures of the geographical maps of http requests around the time of the attacks. The number of connections from Ukraine is well above the baseline.

Graphical user interface

Description automatically generated with medium confidence

Map

Description automatically generated

Question 2

Another rule we might consider doing is blocking one particular user agent. It appears that the user agent for all the POST requests in the attack at 8 p.m. on the login screen was the same. The same user agent wasn’t used for any other connection. Thus, if we firewall against useragent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)", that might help prevent that type of attack once again.

Around 6:05 PM, many GET requests were made for "/files/logstash/logstash-1.3.2-monolithic.jar HTTP/1.1." It seems likely that the attackers wanted access to this logstash file for one reason or another. We might want to set up a fire wall rule where only a whitelist of pre-selected users can access this file, to help prevent whatever the attacker was aiming to accomplish.