**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](about:blank)
* [Windows Attack Logs](about:blank)
* [Apache Webserver Logs](about:blank)
* [Apache Webserver Attack Logs](about:blank)

**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.

*ANS: The attackers took advantage of the user name format “user\_alpha”. They were able to name walk and hammer the system, delete and recreate accounts, and cause accounts to be locked out. One system/admin user account name seemed to be named after a domain “ACME-002”. VSI will have to have unique login names so that invalid attempts can be ignored (for the most part). This will double that amount of work for bad actors by adding both user and password that needs to be cracked and help to prevent the login failed count from causing a denial of service. When a username is correct and the matching password is found the logged in user needs to be logged into a DMZ where the source ip address and number of attempts can be analyzed and selectively passed into the domain, or challenged to prove it has not come from a bot or other malicious source. Multiple filters can then scrutinize the login session activity and guard against unwanted access.*

* + *Reset Active Directory on domains* 
    - *Reconfigure for unique usernames and strong passwords on all accounts*
    - *Remove unused accounts*
    - *Develop new User Login Policy*
  + *Change addresses for Active Servers and Domain*
    - *Place a mote (DMZ) between the Domain and the public facing servers*
    - *Use IDS/IPS systems to catch and analyze traffic and to enforce rules on multiple login attempt sessions*
    - *Develop additional login requirements that force users to “prove who” and “prove not bot” to get logged in when multiple attempts are detected (with non-tolerant thresholds at first – to measure). Note: this should all happen in the DMZ prior to opening the domain to users.*
    - *DMZ server needs to be tuned, hardened, and defensive. Should only have minimal software - no extra’s, no public ports, not known ip, no nada… “non-pingable” (is that a word? Nonpingable..i like)- take referrals from IDS/IPS – should stream to logs - to SIEMS – to Reports – to Alerts/Alarms – to actions*
    - *Snort rules to lock out known offending ip address traffic from March 25th attack. IDS/IPS rules for the same.*
  + *Training*
    - *Sysadmins new public facing servers – to DMZ – to Domain security rules and procedures*
    - *Sysops Siems – necessary reports, alerts/alarms, actions*
    - *Users – new login campaign, rules, and procedures (create unique usernames and strong passwords rules and enforcement)*
    - *User – Cyber Consciousness (is that a thing – cyber consciousness… I really like)*
  + *VSI is in a pinch ….. twist*

**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?
  + *ANS: Snort rules to lock out known offending ip address traffic from March 25th attack. IDS/IPS rules for the same.*

**Part 2: Apache Webserver Attack:**

**Question 1**

* Based on the geographic map, recommend a firewall rule that the networking team *should implement.*

*ANS:We found the March 25th high number of events to be:*

*Query: source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined"| iplocation clientip | top Country*

*source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined" | iplocation clientip | search lat>=22.50000 lat<45.00000 lon>=-135.00000 lon<-90.00000 City="San Antonio"*

*== 637 events – ip 208.91.156.11*

*source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined" | iplocation clientip | search lat>=22.50000 lat<45.00000 lon>=-90.00000 lon<-45.00000 City=Springfield*

*== 433 events – ip 194.146.132.138*

*source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined" | iplocation clientip | search lat>=45.00000 lat<67.50000 lon>=0.00000 lon<45.00000 City=Stockholm*

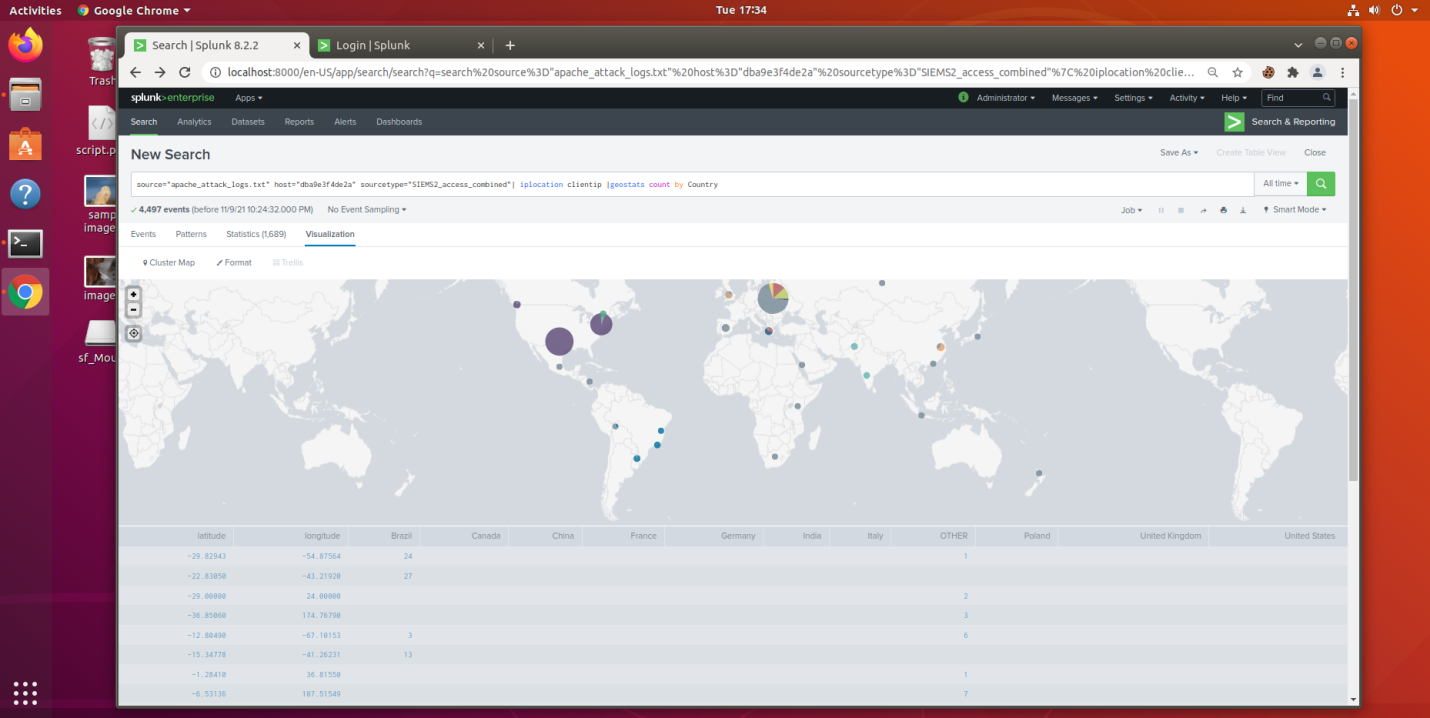
*== 183 events – ip 130.237.218.86*

*source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined" | iplocation clientip | search lat>=45.00000 lat<67.50000 lon>=0.00000 lon<45.00000 City=Kharkiv*

*== 433 events – ip 79.171.127.34*

*We suggest that a firewall rule be set to prevent access to the above sited ip addresses.*

* *Provide a "plain english" description of the rule.* 
  + *ANS: Block all incoming HTTP traffic where the source IP comes from the city San Antonio Texas, Springfield Massachusetts, Stockholm Sweden, and Kharkiv Ukraine*
* Provide a screenshot of the geographic map that justifies why you created this rule.



**Question 2**

* VSI has insider information that JobeCorp will launch the same web server 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?
  + Create a report that will measure and report brute force attacks
  + Hint: Look for other fields that indicate the attacker.

*Query: source="apache\_attack\_logs.txt" host="dba9e3f4de2a" sourcetype="SIEMS2\_access\_combined" status=200 OR status=404 AND uri\_path="/VSI\_Account\_logon.php" OR uri\_path="/VSI\_Company\_Homepage.html"*

