## **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
* Windows Attack Logs
* Apache Webserver Logs
* Apache Webserver Attack Logs

### **Part 1: Windows Server Attack**

Note: This is a public-facing windows server that VSI employees access.

#### **Question 1**

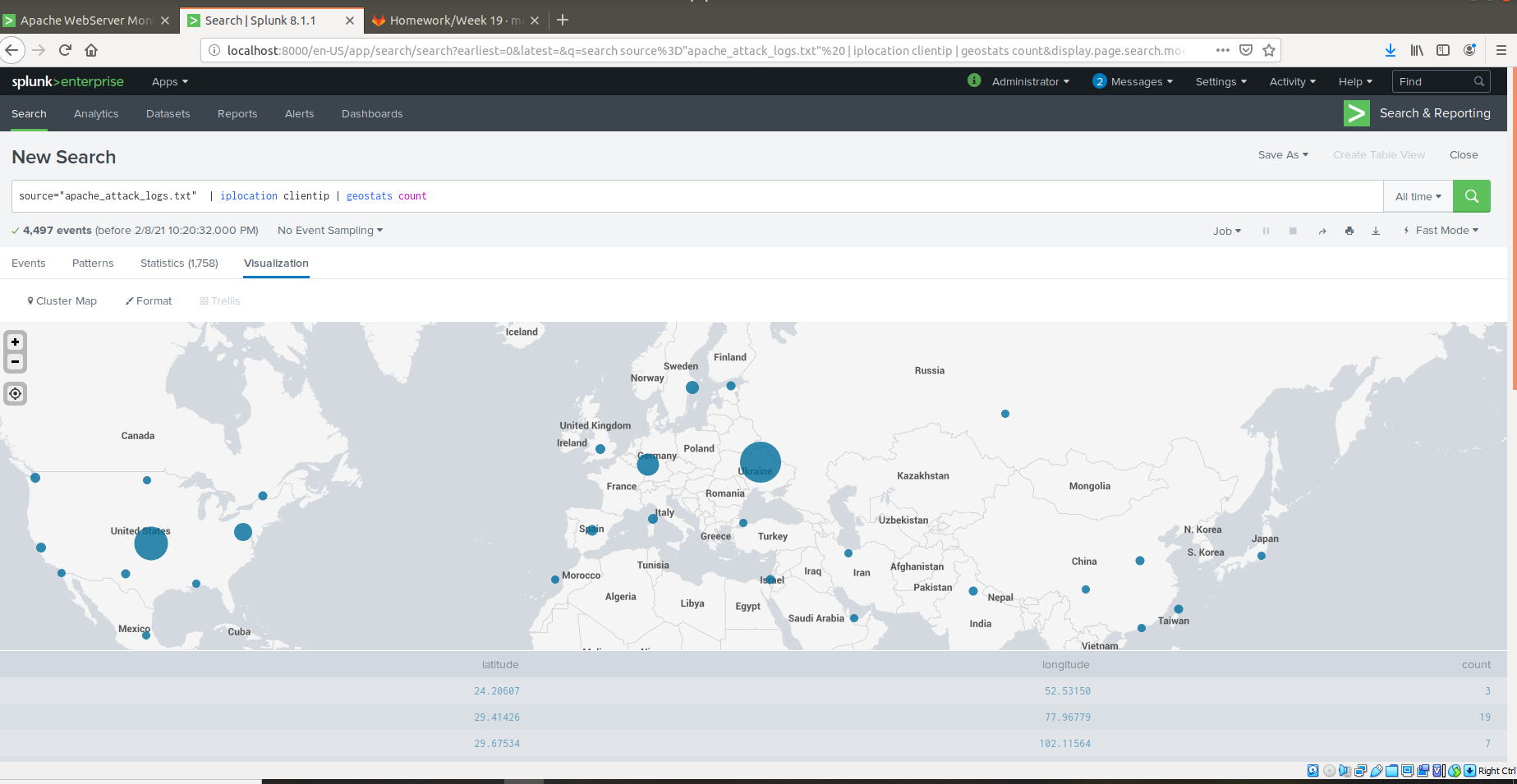
* Several users were impacted during the attack on March 25th.
* Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.
  + A company wide mitigation would be to require two factor authentication in order to log in or to reset a password.
  + An individual mitigation would be to have security questions in order to reset your password.

#### **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?
  + Only allow account access through the VSI vpn so that only employees can attempt to log in.

### **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.
  + Block all incoming HTTP traffic where the source IP comes from Ukraine.
* Provide a screen shot of the geographic map that justifies why you created this rule.
* 

#### **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?  
  + Block all POST requests above 5 per hour.
  + Block all uri of /VSI\_Account\_logon.php above 5 per hour.

### **Guidelines for your Submission:**

In a word document, provide the following:

* Answers for all questions.
* Screenshots where indicated

Submit your findings in BootCampSpot!

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.