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.

  To mitigate the threat of brute force attacks like what was seen in the logs; stricter access protocols need to be put in place. For instance mandatory password changes throughout the year in combination with lock out protocols could reduce the attempts let alone the successful attempts to access the system illegally. Suggesting a lock out after 3-5 attempts seems sufficient for this access rule and it's an easy implementation that can be used across the board for the server and all employees.

Question 2

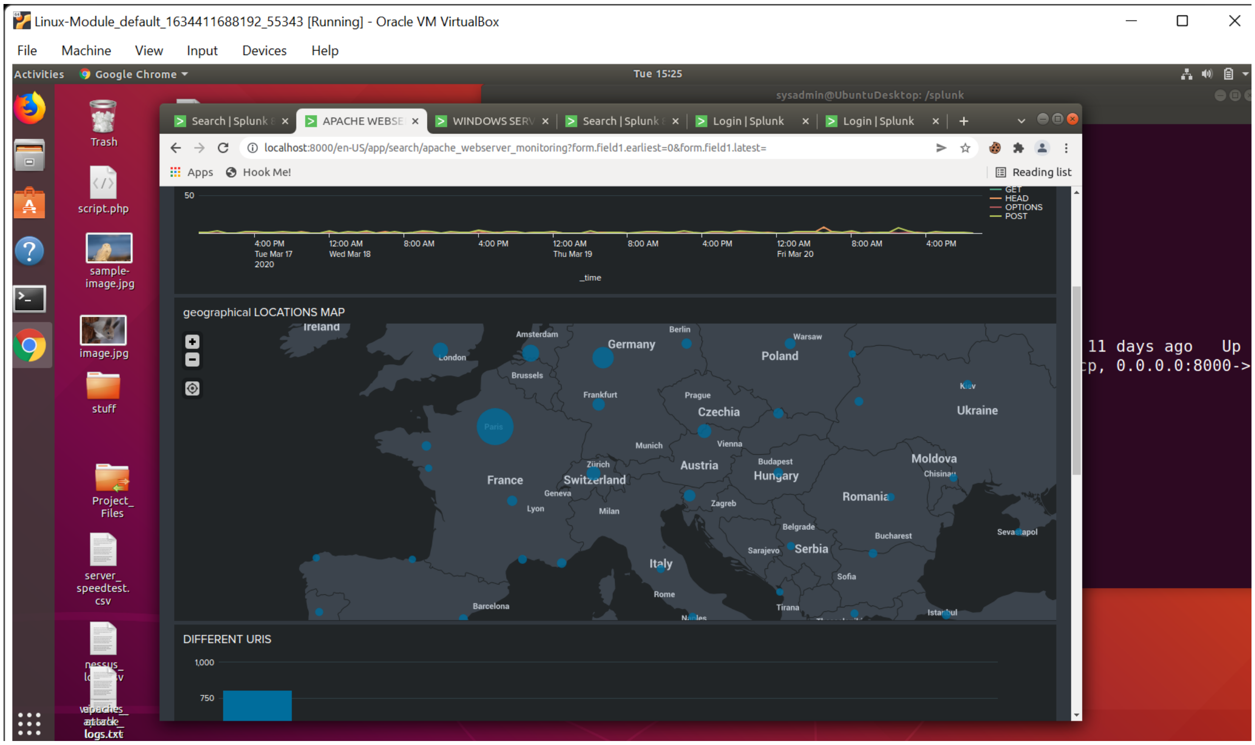
- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

  In order to avoid unnecessary lock outs from this type of brute force attack to deny service to employees; there are additional steps that can be taken. 2 specific additions that can help are: 2 or 3 factor authentication can help prevent these by needing authentication from multiple sources of a specific employees. Lastly , the use of Captchas can reduce these being used in an automated form as script or programs may not have a way around the captchas.

Part 2: Apache Webserver Attack:

Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement. Based on the geographical map of the incoming traffic that affected the server, it appeared the traffic originated from Paris, France. Implementing a rule restricting traffic from Paris or even France all together can prevent being attacked from the same source. This could be a leveled rule that once a certain amount of traffic has been received it will block all further traffic for the day; that way it doesn't restrict all but at least will restrict the extreme amounts.
- 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.


Linux-Module_default_1634411688192_55343 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Google Chrome Tue 15:25
sysadmin@UbuntuDesktop: /splunk
Search | Splunk
APACHE WEBSE
WINDOWS SERV
Search | Splunk
Login | Splunk
Login | Splunk
localhost:8000/en-US/app/search/apache_webserver_monitoring?form.field1.earliest=0&form.field1.latest=
Apps Hook Me! Reading list
Trash
script.php
sample-image.jpg
image.jpg
stuff
Project_Files
server_speedtest.csv
GET
HEAD
OPTIONS
POST
_time
geographical LOCATIONS MAP
Ireland
Germany
Poland
Czechia
Ukraine
France
Switzerland
Austria
Hungary
Moldova
Romania
Italy
Serbia
DIFFERENT URIS
1,000
750
11 days ago Up
0.0.0.0:8000->

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.

Additional rules can help mitigate the risk of these happening again. During the time of the attack the amount of post attacks and the number of error codes were significantly increased. This correlates to POST request and to the error code 404. Generating the following 2 rules could help reduce these brute force or lock out attacks:

1. Create an average and threshold for post requests per hour to reduce or control the traffic coming to the server; once it exceeds the threshold it can create an alert to inform a team member. Additionally doing the same with the error codes; creating a threshold so that it notifies a team member or restricts access once it passes a certain number of error codes can help rudeness frequency or success of brute force attacks.

Guidelines for your Submission:

In a word document, provide the following:

- Answers for all questions.
- Screenshots where indicated