Week 19 Homework

SIEM Homework II

Billy Smith

## 

## 

[**### Part 1: Windows Server Attack**](#_wvgzbqenzim3) **3**

[Question 1](#_yzp9m3gg0gol) 3

[Question 2](#_6q9d5celpgh0) 3

[**### Part 2: Apache Webserver Attack:**](#_31pkel5feqtu) **4**

[Question 1](#_mwm8awnsafee) 4

[Question 2](#_4sjquko0o1fu) 5

[Citations:](#_c6lwrgy5ngyl) 5

## 

## ### Part 1: Windows Server Attack

### Question 1

- Several users were impacted during the attack on March 25th.

* Based on the attack signatures, what mitigation would you recommend to protect each user account?

**As this looks to be a PHP SQL Injection attack, it is recommended to validate the input to ensure the data that is being sent is what is expected. You can also use prepared statements and bind the parameters in a statement.**

**As far as the individual users, it is recommended to employ the least restrictions needed for each user that logs in, create a separate account for each user that needs to login, and you can also create Views for the database for each user that gives them access to only the part of the database that they need access to.** (SQL Injection Prevention Cheat Sheet) \*

[**https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

### 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?

**To mitigate against the “Bad Logins” I would set firewall rules to deny access from any IP address that causes multiple bad login attempts across multiple usernames. I would also set up the IDP/IDS system to alert on such attempts for them to follow up and determine where the attack is coming from.**

## 

## 

## 

## 

## 

## ### Part 2: Apache Webserver Attack:

### Question 1

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

**The networking team should block all HTTP traffic where the source IP is coming from Kiev, Ukraine**





### 

### 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.

**The first rule that I would set up will block any IP address that attempts the login attack in so many iterations within a specific time frame. Like 5 attempts across multiple accounts in 1 minute.**

**The second rule I could create is for the IDS to look for a specific string, if noticed in other attempts, send an alert, and blacklist any IP address that meets that criteria until it can be determined that the IP address is valid.**

### Citations:

*SQL Injection Prevention - OWASP Cheat Sheet Series*. (2021). OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/cheatsheets/SQL\_Injection\_Prevention\_Cheat\_Sheet.html