Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol identified in the packet captures during the investigation corresponds to the HTTP protocol, which operates at the application layer (Layer 4) of the TCP/IP model. The incident involves the interaction between the client's web browser and the web servers for the "yummyrecipesforme.com" and "greatrecipesforme.com" websites. Specifically, the logs show HTTP requests and responses for the downloading of files and website content.

Section 2: Document the incident

A security incident was observed in the context of the "yummyrecipesforme.com" website, which sells recipes and cookbooks. The incident involved unauthorized access and malicious alterations to the website's content. The following details outline the incident:

- Location of Incident: "yummyrecipesforme.com" website.
- Attack Vector: A disgruntled baker executed a brute force attack to gain access to the website's web host. The attacker repeatedly entered known default passwords for the administrative account until the correct password was successfully guessed.
- Impact: After gaining access to the admin panel, the attacker embedded a malicious JavaScript function in the website's source code. This JavaScript function prompted visitors to download and run an executable file when they visited the website. Running the downloaded file resulted in a browser redirection to a fraudulent website, "greatrecipesforme.com," where the company's recipes were made available for free.
- Discovery of Incident: Multiple customers reported the incident to the "yummyrecipesforme" helpdesk. They encountered a prompt to download an executable file, which purportedly aimed to update their browsers. Upon running the downloaded file, their browsers redirected

them to "greatrecipesforme.com," and their computers experienced performance degradation.

- Source of Incident: The website was compromised due to the use of default administrative credentials and the absence of security controls to prevent a brute force attack.
- Evidence: The investigation involved the analysis of network traffic using tcpdump, which captured DNS resolution requests, HTTP requests, and responses related to the incident. Additionally, a review of the website's source code revealed the malicious JavaScript code that prompted downloads and browser redirection.
- Incident Report Source: The incident report is based on network traffic logs, source code analysis, and customer complaints.

Section 3: Recommend one remediation for brute force attacks

One effective measure to prevent brute force attacks is to implement account lockout policies. Account lockout policies temporarily or permanently lock a user's account after a specified number of unsuccessful login attempts. Here's why this measure is effective:

1. Deters Brute Force Attacks: By limiting the number of login attempts, attackers are discouraged from repeatedly trying different passwords, as they risk locking themselves out of the account.
2. Enhances Security: Account lockout policies enhance the security of user accounts by mitigating the risk of unauthorized access.
3. Reduces Manual Monitoring: This security measure reduces the need for manual monitoring of login attempts, as it automatically responds to excessive failed login attempts.
4. Customizable Settings: Organizations can tailor lockout policies to their specific needs, allowing flexibility in configuring lockout thresholds and lockout duration.
5. Complements Other Security Measures: Account lockout policies can work in conjunction with other security measures, such as strong password requirements and multi-factor authentication (MFA), to create a layered defense against brute force attacks.

It is important to strike a balance when configuring account lockout policies to avoid accidental lockouts. Properly configured policies will effectively thwart brute force attempts while ensuring legitimate users are not inconvenienced. Additionally, education and awareness among users regarding these policies can further enhance their effectiveness.