Scenario Overview

As a cybersecurity analyst for a company that hosts the cooking website yummyrecipesforme.com, your role is to investigate a security incident affecting the website. Customers reported being prompted to download a file upon visiting the site, after which they were redirected to a different webpage. The investigation revealed that a former employee executed a brute force attack to gain access to the admin account, embedded a malicious JavaScript function in the website's source code, and changed the administrative password. Your task is to analyze the incident, document the network activity, and recommend security measures to prevent similar occurrences in the future.

Section 1: Identify the network protocols involved in the incident

The protocols involved in this incident are the Hypertext Transfer Protocol (HTTP) and the Domain Name System (DNS). HTTP was used to establish connections between users and the website, allowing for the transmission of web content. The DNS protocol played a crucial role in redirecting users to the malicious site, as it resolved the domain name for the fake website (greatrecipesforme.com) after the malware-infected script was executed. Additionally, since DNS queries rely on the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) for communication, TCP was also involved in establishing these connections.

Section 2: Document the Incident

According to customer reports, when they visited the website, they were prompted to download a file that supposedly contained free recipes. After executing the file, they noticed that their browser redirected to a different website, and their personal computers began running slower.

Upon investigation, it was determined that an attacker had gained unauthorized access to the website's administrative account via a brute force attack. Since the administrator credentials were still set to a default password, the attacker was able to repeatedly guess passwords until gaining access. Once inside, the attacker modified the website’s source code, embedding a malicious JavaScript function. This function prompted visitors to download a fake browser update containing malware. After execution, the malware triggered a DNS request to resolve the fake domain (greatrecipesforme.com), leading to redirection.

The cybersecurity team used a sandbox environment to analyze the issue and captured network traffic using tcpdump. The logs confirmed that the initial request was made to the legitimate website (yummyrecipesforme.com) via HTTP. A DNS request was then issued when the browser attempted to reach greatrecipesforme.com, resulting in a response with the IP address of the fake website. This sequence of events indicated that the attacker manipulated the DNS resolution process to redirect users after executing the malware.

Section 3: Recommend one or more remediations for brute force attacks

To prevent similar incidents in the future, it is critical to implement stronger access controls and security measures:

1. Enforce strict password policies – The attacker was able to gain access due to the use of a default password. Implementing policies that require strong, unique passwords across the organization would make brute force attacks significantly harder.

2. **Implement CAPTCHA or login rate limiting – Adding CAPTCHA or limiting the number of failed login attempts would slow down or deter brute force attacks.**
3. **Enable multi-factor authentication (MFA) – Requiring an additional verification step, such as a one-time passcode sent via email or an authenticator app, would prevent unauthorized access even if the password is compromised.**
4. **Monitor and log authentication attempts – Regularly reviewing authentication logs can help detect suspicious login attempts before they result in a breach.**
5. **Consider switching to HTTPS – While HTTPS would not have prevented this specific attack (since the attacker had direct access to internal services), implementing secure communication protocols is a best practice to protect against other forms of data interception and manipulation.**

By applying these security measures, the organization can significantly reduce the risk of future brute force attacks and unauthorized access to critical systems.