Brute Force Attack: Security incident report

Section 1: Identify the network protocol involved in the incident
This is an application layer attack that exploits HTTP and DNS requests to download malicious updates to the user's browser and redirect them to a fake version of yummyrecipesforme.com.

Section 2: Document the incident
A disgruntled user of yummyrecipesforme.com executed a brute force attack on the administrative account of the web server. After successfully obtaining the password, the attacker accessed the admin panel and altered the website's source code. They added a JavaScript function that prompted visitors to download and run a file when they visited the site. After downloading the file, users were redirected to a spoofed version of the website at greatrecipesforme.com. The attacker also uploaded all of a seller's paid recipes for free on this site. Additionally, users reported that their computers began running more slowly after executing the downloaded file. The cybersecurity analyst simulated the customer's actions in a sandbox (Virtual Machine) and confirmed the following sequence of events when visiting yummyrecipesforme.com:

1. The browser requests a DNS resolution for the yummyrecipesforme.com URL.
2. The DNS server responds with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser prompts the download of the malware.
5. The browser requests a DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

Section 3: Recommend one remediation for brute force attacks

It was later discovered that the admin account password was still set to the default. To protect against future brute force attacks, it is essential to implement secure password policies for this account and the organization. Recommended password policies include:

- Blocking specific IPs after a certain number of failed password attempts.
- Updating password requirements to ensure a certain length and inclusion of various character types (not just letters).
- Requiring periodic password changes.
- Implementing 2-Factor or Multi-Factor Authentication (2FA or MFA).

Focusing on blocking large amounts of failed password attempts is crucial. A brute force attack guesses account credentials by trying many passwords from a commonly used list. The admin account lacked measures to detect and block excessive failed password attempts, allowing the attacker to try as many guesses as needed to succeed.