Brute Force Attack: Security Incident Report

Section 1: Identify the network protocol involved in the incident

This attack occurred at the application layer, exploiting HTTP and DNS protocols to push malicious updates to users' browsers and redirect them to a counterfeit version of yummyrecipesforme.com.

Section 2: Document the incident

A dissatisfied user of yummyrecipesforme.com carried out a brute force attack on the website's administrative account. Once they successfully guessed the correct password, the attacker gained access to the admin panel and modified the website's source code. They embedded a malicious JavaScript function that prompted site visitors to download and execute a file.

Following the download, users were redirected to a fake version of the site with the domain name greatrecipesforme.com. The attacker then made all of a seller's paid recipes available for free on this fake site. Additionally, users reported experiencing slower computer performance after running the downloaded file.

The cybersecurity analyst reproduced the customer's experience in a sandbox environment and confirmed the following sequence of events when visiting yummyrecipesforme.com:

1. The browser sends a DNS query to resolve the domain name for yummyrecipesforme.com.
2. The DNS server replies with the correct IP address.
3. The browser makes an HTTP request to load the webpage.
4. The browser initiates the download of malware.
5. The browser sends another DNS query for greatrecipesforme.com.
6. The DNS server provides the IP address for the fake site.
7. The browser initiates an HTTP request to this new IP address, leading to the spoofed website.

Section 3: Recommend one remediation for brute force attacks

It was found that the admin account still had the default password, which significantly increased the vulnerability to the brute force attack. To prevent future incidents, it is critical to enforce strong password policies across the organization. Key steps include:

1. Implementing measures to block excessive failed login attempts, such as temporarily blocking IP addresses after too many unsuccessful tries.
2. Strengthening password complexity requirements by mandating a minimum length and the use of a combination of letters, numbers, and special characters.
3. Enforcing regular password updates.
4. Requiring Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) for sensitive accounts.

A specific recommendation is to implement IP blocking for repeated failed login attempts. Brute force attacks rely on systematically guessing passwords until the correct one is found, often using a list of common passwords. The admin account lacked mechanisms to detect or limit repeated failed attempts, allowing the attacker to continue trying different passwords without restriction.