Security incident report

Section 1: Identify the network protocol involved in the incident

Based on the analyzed scenario, the network protocols identified in the incident are:

- **DNS (Domain Name System):** Used by the browser to resolve the domain names (`yummyrecipesforme.com` and `greatrecipesforme.com`) into IP addresses.
- **HTTP (Hypertext Transfer Protocol):** Used to load the website content, send page requests, and perform the download of the malicious file.
- **TCP (Transmission Control Protocol):** The transport protocol used by `tcpdump` to capture the packets, ensuring the connection between the client and the server.

Section 2: Document the incident

Incident Title: Website Compromise via Brute Force and Malware Redirection. **Investigation Date:** January 23, 2026. **Lead Analyst:** Cybersecurity Analyst (Level 1).

1. Event Description: The website `yummyrecipesforme.com` was breached by a former employee following a successful brute force attack on the administrative account, which was still using a default password. The attacker modified the source code by inserting a malicious JavaScript snippet.

2. Symptoms and Impact:

- Customers reported computer slowdowns and suspicious download prompts.

- The website owner lost administrative access (password changed by the hacker).
- Users were silently redirected to the malicious domain `greatrecipesforme.com`.

3. Technical Analysis (Network Flow): Investigation in a sandbox environment using `tcpdump` revealed:

- **Name Resolution:** The system used **DNS** to resolve IP addresses for both domains (legitimate and malicious).
- **Data Transfer:** The **HTTP** protocol was used to load the website and transfer the infected executable file.
- **Malware Execution:** The downloaded file executed a redirection script that changed the user's browser destination.

Section 3: Recommend one remediation for brute force attacks

Implement Multi-Factor Authentication (MFA).

By requiring a second form of verification (such as a code sent via SMS, an authenticator app, or biometrics), MFA ensures that even if an attacker successfully guesses the correct password through brute force, they still will not be able to access the administrative account without the physical second factor.