Security incident report

Section 1: Identify the network protocol involved in the incident

The primary network protocol involved in the incident was **HTTP (HyperText Transfer Protocol)**, which operates at the **Application layer** of the TCP/IP model. Additionally, **DNS (Domain Name System)** was also used during the initial domain resolution phase.

Section 2: Document the incident

A cybersecurity incident was identified involving the company website, *yummyrecipesforme.com*. The issue was initially reported by customers who received unexpected prompts to download a file while visiting the website. After executing the file, users noticed their web browsers were redirected to a different domain, *greatrecipesforme.com*, and reported performance issues with their personal devices.

Upon investigating the issue using tcpdump in a sandboxed environment, the following sequence of events was observed:

1. The browser made a **DNS request** to resolve *yummyrecipesforme.com*.
2. A **DNS response** returned the IP address 203.0.113.22.
3. The browser initiated an **HTTP GET request** to that IP, requesting the main webpage.
4. The website responded with a page containing a **JavaScript function** prompting users to download and run an executable file.
5. Upon execution, the script issued a second **DNS request** for *greatrecipesforme.com*, which resolved to 192.0.2.17.
6. The browser then issued an **HTTP GET request** to the new domain,

where malicious content was hosted.

Further analysis confirmed the website had been compromised due to a **brute force attack**. The attacker, a former employee, gained unauthorized access by guessing a weak, default administrative password. After gaining access, they injected malicious JavaScript into the site's source code and changed the admin password, locking out legitimate administrators.

This information was corroborated through tcpdump packet captures and source code review by a senior analyst.

Section 3: Recommend one remediation for brute force attacks

To prevent future brute force attacks, it is recommended to **implement two-factor authentication (2FA)** for all administrative accounts.

2FA adds an extra layer of security by requiring users to provide a second verification method such as a time based one-time password (TOTP) or hardware token in addition to their standard password. This ensures that even if a password is compromised, unauthorized access is still prevented without the second factor.