**Security Incident Report**

**Section 1**: Identify the network protocol involved in the incident

Based on the analysis of the provided tcpdump logs, the following network protocols were identified:

- DNS (Domain Name System): Used to resolve the IP addresses of the domains “yummyrecipesforme.com” and “greatrecipesforme.com”.

- HTTP (Hypertext Transfer Protocol): Used for the page requests and for downloading the malicious file.

**Section 2**: Incident Documentation

On the day of the incident, the website “yummyrecipesforme.com” was compromised by a former employee through a brute force attack, where the default password of the administrative panel was used to gain access. After obtaining the credentials, the attacker added JavaScript code to the website’s source, causing visitors to be redirected to a fake domain (“greatrecipesforme.com”) after downloading a malicious executable file. The malware was designed to slow down infected computers and potentially steal data.

**The logs show the following process:**

1. Upon accessing the site, the browser performed a DNS request to obtain the IP address of “yummyrecipesforme.com”.

2. After resolving the IP, an HTTP connection was established, and the browser downloaded the malicious file.

3. Subsequently, the executed malware redirected the browser to “greatrecipesforme.com” via another DNS resolution and HTTP connection.

4. The administrative panel was locked by the attacker by changing the password.

The incident was discovered through user complaints and confirmed by technical analysis of the website’s source code.

**Section 3**: Recommendation for Brute Force Attack Remediation

To prevent future brute force attacks, we recommend implementing two-factor authentication (2FA). This method adds an extra layer of security by requiring users to provide a second form of verification, such as a code generated by an app or sent via SMS. Even if an attacker obtains the password, they will not be able to access the system without the second factor, significantly reducing the risk of compromising the administrative panel.