Security incident report

Section 1: Protocols observed in the tcpdump logs

1. **DNS (Port 53):** Used to resolve domain names like `yummyrecipesforme.com` and `greatrecipesforme.com` to their IP addresses.

- Example from log:

```
your.machine.52444 > dns.google.domain: A? yummyrecipesforme.com
dns.google.domain > your.machine.52444: A 203.0.113.22
```

2. **HTTP (Port 80):** Used to request and load web pages (including downloading the malicious file). The traffic shows full HTTP communication (GET requests).

- Example from log:

```
your.machine.36086 > yummyrecipesforme.com.http: GET / HTTP/1.1
your.machine.56378 > greatrecipesforme.com.http: GET / HTTP/1.1
```

Summary: The protocols identified in this attack were **DNS** and **HTTP**, both operating at the **Application Layer** of the TCP/IP model. HTTP was used to fetch the malicious content, and DNS was used to redirect the user from a legitimate to a malicious domain.

Section 2: Incident Summary

The website `yummyrecipesforme.com` was compromised through a brute force attack. The attacker, a former employee, successfully accessed the admin panel by repeatedly attempting default passwords. Once access was gained, the attacker embedded malicious JavaScript in the site's source code, which prompted users to download a fake browser update in `.exe` format.

After executing the file, users were redirected to `greatrecipesforme.com`, a clone of the original site, which was hosting malware.

Using `tcpdump`, it was observed that the following occurred:

- A **DNS request** was made to resolve `yummyrecipesforme.com`.
- An **HTTP GET request** loaded the website.
- A prompt appeared for users to download and run a file.
- Upon execution, another **DNS request** was made for `greatrecipesforme.com`.
- The browser then made an **HTTP GET request** to the fake site.

The attacker also changed the admin credentials, locking the owner out of the site. The issue was reported by users who noticed redirection and system performance issues after running the file. The source code confirmed the embedded JavaScript and redirection.

Evidence Source: tcpdump traffic logs and helpdesk reports from affected users.

Section 3: Recommend one remediation for brute force attacks
Enforce Two-Factor Authentication (2FA) To prevent future brute force attacks, the company should enforce **two-factor authentication (2FA)** for all administrator accounts. Even if an attacker is able to guess a password, they would still require a second form of authentication (e.g., OTP, security token) to access the system. This significantly reduces the likelihood of successful unauthorized access. **Why it's effective:** 2FA adds a second layer of protection and prevents unauthorized logins, even when weak or default passwords are present. It is especially important for high-privilege accounts such as admin or root users.