Security Incident Report

Section 1: Identify the Network Protocol Involved in the Incident

During the investigation, the tcpdump log revealed that three network protocols were involved:

- **DNS (Domain Name System)** – Used to translate the domain names (yummyrecipesforme.com and greatrecipesforme.com) into IP addresses.

- **TCP (Transmission Control Protocol)** – Established reliable connections between the client and servers.

- **HTTP (Hypertext Transfer Protocol)** – Used to request and receive web content from the websites.

Example from the log:

```
 14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, ... length 73: HTTP: GET / HTTP/1.1
```

> ^The use of **HTTP** instead of **HTTPS** means the traffic was **not encrypted**^ making the site more vulnerable to attack.

Section 2: Document the Incident

Incident Summary

On **14:18:36**, the website yummyrecipesforme.com was compromised after a former employee gained unauthorized access to the administrative panel by using a **brute force attack**. This was possible due to a **default password** being in place and no protections against multiple failed login attempts.

Once inside, the attacker:

1. **Injected malicious JavaScript** into the website's code.

2. This script prompted visitors to **download a file**, which seemed like a recipe update.

3. Upon execution, the file **redirected users** to greatrecipesforme.com, a malicious site distributing malware.

4. The attacker then **changed the admin password**, locking out the site's legitimate owner.

Discovery and Investigation Timeline

- **14:18:32** – DNS query for `yummyrecipesforme.com` was sent and resolved to an IP.
- **14:18:36** – HTTP request initiated; connection established.
- **Immediately after** – Users prompted to download an executable file.
- **Users reported issues** – Browser redirection and performance slowdowns were reported to the help desk.
- **Investigation actions taken**:
  - Admin login failed — confirmed unauthorized access.
  - Sandbox testing performed to safely observe behavior.
  - **Tcpdump is used** to capture and analyze network traffic.
  - Redirect to `greatrecipesforme.com` was observed in real time.
  - Senior analyst confirmed **malicious JavaScript** in the website source code.

Impact Assessment

- **Integrity Compromised**: Website code was altered without permission.
- **Confidentiality at Risk**: Users downloaded malicious software that could steal personal data.
- **Availability Affected**: Users could not access the original website content.
- **Reputation Damaged**: Multiple customer complaints; risk of lost trust.

Root Cause

The attacker successfully guessed the admin password using brute force due to **lack of account protections** and **use of a default password**.

Section 3: Recommendation for Preventing Brute Force Attacks

Recommended Action:

Implement Multi-Factor Authentication for all administrative logins.

Why MFA is Effective

Even if an attacker successfully guesses a password, **MFA requires a second verification step**, such as:

- A code from an authenticator app
- A fingerprint scan
- A one-time text message code

Without access to this second factor, an attacker cannot log in — stopping brute force attempts from succeeding.

> **Next Step**: Enable MFA on all admin accounts within the hosting control panel and make it mandatory for all future logins.