Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve HTTP traffic. The tcpdump log confirmed the use of the HTTP protocol when contacting the server, and the malicious file was observed being transported to users' computers using HTTP at the Application layer. Additionally, the analysis shows the use of the IP protocol at the Internet layer for data transmission and the DNS protocol at the Application layer for resolving domain names, which also played a key role in the incident.

Section 2: Document the incident

- **Customer Reports:**
  - Customers contacted helpdesk after being prompted to download and run a file for new recipes.
  - Users reported their computers were operating slowly afterward.
  - Website owner found they were locked out of their admin account.
 	
- **Initial Investigation:**
  - Cybersecurity analyst used a sandbox to safely access the website.
  - Ran `tcpdump` to capture network traffic during interaction with the website.
  - Analyst was prompted to download and run a file claiming to offer free recipes.
  - After executing the file, the browser redirected to a fake website (greatrecipesforme.com).
 	
- **Traffic Analysis:**
  - `Tcpdump` logs showed the browser initially requested the IP address for yummyrecipesforme.com.
  - Connection established using HTTP protocol.

- After file execution, a sudden change in traffic was observed.
- Browser requested IP for greatrecipesforme.com, redirecting traffic to the fake site.

- **Source Code Analysis:**
- Senior cybersecurity professional examined website and file source code.
- Found that an attacker added malicious code prompting the download of a fake browser update.
- Evidence suggests the attacker used a brute force attack to gain admin access and change the password.
- Execution of the malicious file compromised users' computers.

Section 3: Recommend one remediation for brute force attacks
Remediation Recommendation: Implement **Multi-Factor Authentication (MFA)** to protect against brute force attacks. MFA adds an additional layer of security by requiring users to provide two or more verification factors (e.g., a password and a one-time code sent to a mobile device) before granting access. This significantly reduces the risk of unauthorized access, even if an attacker successfully guesses or cracks a password, as they would also need access to the second factor, which is typically more difficult to obtain.