**Security Incident Report.**

**Hypertext Transfer Protocol (HTTP).**

**Section 1: Identify the network protocol involved in the incident**  
The protocol involved in the incident is the Hypertext Transfer Protocol (HTTP), as the issue was related to accessing the web server for yummyrecipesforme.com. Additionally, when we ran tcpdump and accessed the website, the corresponding tcpdump log file showed the use of the HTTP protocol when contacting the file. It was observed that the malicious file was transferred to users' computers using the HTTP protocol at the application layer.

**Section 2: Document the incident**  
Several customers contacted the website's technical support service, reporting that when they accessed the website, they were prompted to download and run a file that claimed to provide access to new recipes. Since then, their personal computers have been running slowly. The website owner attempted to log into the web server but noticed that their account was locked.

A sandbox environment was used to open the website without affecting the company's network, and tcpdump was run to capture network traffic packets produced when interacting with the website. The file claiming to give access to free recipes was downloaded. After this, the browser redirected to a fake website (greatrecipesforme.com).

The tcpdump log was inspected, showing that the browser initially requested the IP address for yummyrecipesforme.com. However, once the file was downloaded and executed, the logs showed a sudden change in network traffic, requesting a new IP address for the URL greatrecipesforme.com. Then, the network traffic was redirected to the new IP address for greatrecipesforme.com.

The senior cybersecurity professional analyzed the source code of the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add code that prompted users to download a malicious file disguised as a browser update. Since the website owner stated that their administrator account access had been blocked, the team believes the attacker used a brute-force attack to gain access to the account and change the administrator password.

**Section 3: Recommend a solution for brute-force attacks**  
One security measure the team plans to implement to protect against brute-force attacks is to prevent the use of old passwords. Since the vulnerability that caused this attack was the attacker’s ability to use a default password to log in, it is important to prevent old, default passwords from being used when resetting a password. Another supporting measure is to require longer passwords. Passwords of 15 characters or more provide stronger protection against brute-force attacks. A useful additional solution is to implement two-factor authentication (2FA), as it requires authentication through a password and the confirmation of a one-time passcode (OTP) sent to the user’s email or phone.