Security incident report

Section 1: Network protocol involved in the incident
The protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). After running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, and capture protocol and traffic activity, the DNS and HTTP traffic log file provided enough evidence to conclude that the malicious file in the website's code transported the user's computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website owner stating that when they visited the website, they were asked to download a file that asked them to update their browsers. Their personal computers have been running slowly since they downloaded and executed the file. The owner of the website tried to login into the website and found out they were locked out of their account. The cybersecurity analyst used a virtual machine to test the website to protect the company's network. Then, the cybersecurity analyst used tcpdump to capture traffic packets between the machine and the website, when the analyst accessed the website they were asked to update their browser, they agreed and downloaded the file, after downloading the file the analyst was redirected to a fake website (greatrecipesforme.com) that looked identical to the original website (yummyrecipesforme.com). The analyst inspected the tcpdump logs and noticed that the browser initially requested the IP address for yummyrecipesforme.com, once the connection was established over HTTP and after downloading the file, a sudden change in network traffic happened: the browser requested a new IP address resolution for greatrecipesforme.com website. The browser was then redirected to the new IP address for the greatrecipesforme.com website. The senior cybersecurity professional analyzed the source code for both websites, and discovered that an attacker had manipulated the original website by inserting a code that asked users to download a malicious file disguised as an update.

The cybersecurity team believes that the attackers used a brute force attack to access the administrator account and change the password because the owner said that they had been locked out of their administrator account and there was no protection against brute force attacks.

Section 3: Recommend one remediation for brute force attacks
One security measure the team plans to implement to protect against brute force attack is multi-factor authentication (MFA). This plan includes multiple requirements for users to validate their identities by confirming one-time password (OTP) sent to their email or phone numbers as well as an authentication code through an authenticator app such as Google Authenticator. Once the user confirms their identity through their credentials and MFA, they will gain access to their account. The probability of a threat actor gaining access to the account by brute force attack is greatly reduced because the account requires multiple steps of verification.