Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol that's involved in the incident are: ● HTTP Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP a traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Customers emailed the help desk informing that after entering yummyrecipesforme.com, they were prompted to download a file to update their browsers. After running the file, the address of the website changed and their computer began to run slower. To investigate the incident, I created a sandbox to observe the issues. Protocol analyzer tcpdump was run as we entered yummyrecipesforme.com. Upon entering the website, I was prompted to download a file to update my browser. I ran the file then it redirected me to a different URL, greatrecipesforme.com. It was a different URL but designed to look like the original site. Recipes were free instead of for sale. The senior analyst confirmed that the website was compromised. The analyst had checked the source code for the website and found that javascript code had been added to prompt visitors to download the update file. A script that redirects visitors to greatrecipesforme.com instead of yummyrecipesforme.com. The attacker had gained access through the administrative account, granting them the right to lock everyone out.

Section 3: Recommend one remediation for brute force attacks
I recommend to implement: ● MFA Implementing this will help the web host from being accessed by an unauthorized user. MFA will protect the admin account by having them verify their identity before being able to log in, by a one-time password (OTP) by email or phone.