Security incident report

Section 1: Identify the network protocol involved in the incident
After analyzing the tcpdump, analyzing the traffic, and accessing the yummyrecipesforme.com website; It was determined that the Hypertext transfer protocol was impacted.

Section 2: Document the incident
Customers had complained that when they had visited the website, they were prompted to download and run a file that asked them to update their browsers. It would also redirect them to another website. The customers also mentioned that their computers have been operating slower ever since. The website owner is also locked out of the web server. Our team created a sandbox environment to observe the suspicious website behavior. After running tcpdump, then visiting yummyrecipesforme.com; Once the website loads, we were prompted to download a executable filte to update our browser. We accepted the download and allowed the file to run. Then the browser automatically redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site, but with all the recipes leaked for free. We also checked the source code and found that a javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com. The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Section 3: Recommend one remediation for brute force attacks
One crucial remediation to prevent future brute force attacks would be to implement stronger controls for accessing the network. A good implementation would be 2FA. This 2FA plan would include an additional requirement for users to validate their identity when accessing the network. Once the user confirms two different forms of identification methods, they will gain access to the system. Brute force attacks will be almost impossible to work with additional authorization.