Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in this incident is HTTP. DNS traffic was redirected to a new domain greatrecipesforme.com. Malicious files were being sent over HTTP to unsuspecting users.

Section 2: Document the incident
Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. The cybersecurity analyst created a sandbox environment to observe suspicious website behaviour. Tcpdump was run to analyse traffic while in the sandbox environment. After visiting the website, the analyst was prompted to download an executable file to update the browser. When the file was downloaded and run, the site was redirected to a new website, greatrecipesforme.com. The senior analyst checked the source code and confirmed that the website had been compromised. Javascript code had been injected which prompted the executable file download. Analysis of the file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com. The cybersecurity team reported that the web server was impacted by a brute force attack. The threat actor was able to guess a password easily because an 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
This attack was a result of weak passwords being used by the admin user for yummyrecipesforme.com. I would recommend that a stronger password policy be put in place and that a user will be locked out of their account after 3-5 failed password attempts. Implementing MFA will allow the original user to regain access to their account if a threat actor tries a brute force attack and locks the original user out. A stronger password policy is an effective way of deterring a brute force attack because a random string of characters is much harder to guess.