Security incident report

Section 1: Identify the network protocol involved in the incident
According to the log file the protocol impacted is HyperText Transfer Protocol (HTTP).

Section 2: Document the incident
In the afternoon, the company's helpdesk received multiple customer emails reporting an incident on the website. Customers mentioned encountering a prompt on the website that requested them to download a file for browser updates. After downloading the file, they noticed a change in the website's address, and their personal computers started running more slowly. After this incident, the cybersecurity analysts were asked to investigate. In response to the incident, the team conducted website testing using tcpdump within a sandbox environment. Upon downloading and executing the prompted file, they were redirected to greatrecipesforme.com, a website designed to mimic the company's site. However, they discovered that the recipes their company sells were now freely available on the new website. This is the result of a brute force attack. The attacker gained access to the admin account by repeatedly attempting variously known default passwords. Once successful, they proceeded to modify the source code.

Section 3: Recommend one remediation for brute force attacks
To prevent future occurrences of this type of attack, it is essential to implement robust password policies. This can help by ensuring that strong and unique passwords