Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved is HTTP since this issue revolved around accessing the web server for the client's site. When examining the log file generated by tcpdump , it showed that the site was successfully accessed initially, however it was then re-directed after a 2-minute-long communication where a piece of malware was transferred to the users computer at the application layer.

Section 2: Document the incident
The incident was reported by multiple customers of yummyreceipesforme.com to the helpdesk sometime in the early afternoon. They reported that upon visiting the yummyreceipesforme.com website, they were prompted to download a file that purported to have new recipes before continuing. Since downloading the file, their computers have been operating slowly. The website owner tried logging into the web server but noticed they were unable to access their account. IT responded by setting up a sandbox and utilizing tcpdump to track the issue. During this process the log file revealed that upon initial request of the DNS to the client's website, the correct IP address is obtained. Once arriving at the site a 2-minute communication occurs (14:18 – 14:20) where the browser is requesting data. This could be a malware download . At 14:20, a sudden request from the browser to the DNS is triggered and a new site is requested . The browser is then re-directed to this new site and a new port number is being used by the local machine . The senior analyst then examined the source code for the websites and the downloaded file. They discovered that an attacker had manipulated the site to add code that prompted the user to download a file disguised as a browser

update. Since the website owner stated that they had been locked out of their admin account, the team now believes that the attacker used a brute force attack of some kind to gain access to the account and change the admin password.

Section 3: Recommend one remediation for brute force attacks
One option to remediate the issue is to update the admin password policies with possibilities ranging from stronger requirements to 2FA/MFAs . The team also recommends that previously used passwords be no longer allowed. It is also recommended that default passwords be changed upon the user receiving the password. Frequent password changes are also encourage d.