Security incident report

Section 1: Identify the network protocol involved in the incident
Using the TCP/IP model, the application layer was affected specifically the HTTP protocol. This was concluded from running the tcpdump log, where the changes were seen during the HTTP protocol.

Section 2: Document the incident
This attack was noticed when complaints from users stated that upon visiting the website, they were asked to download a file that was alleged to update the browser software. After downloading and running the program, were re-directed to another website, and their computers “began running more slowly”. The website owners tried logging into the admin panel but were unable, so they reached out to the hosting provider. The security analyst using a sandbox environment tried visiting the website and was asked to download a file that would supposedly update the browser. After running the file, they were redirected to a fake website “greatrecipesforme.com” which is identical to the original website “yummyrecipesforme.com”. On the fake website, the recipes from the original website were uploaded for free. Upon inspecting the source code, the security analyst found a JavaScript function code that was added which prompts users to download and run a file. This is a suspected brute force attack by a threat actor. A network analyzer log was run, and the tcpdump logs show that during the HTTP protocol, another DNS resolution request was made. This time the DNS servers IP address was changed and the destination URL was changed to “greatrecipesforme.com.http:” The timestamp from going to the website to re-directing to the fake website is (14:18:32.192571 - 14:20:32.192571) about 2 minutes.

Section 3: Recommend one remediation for brute force attacks
• Stronger password policies e.g. longer passwords, and passwords with unique characters and numbers (not just default passwords), especially for the admin panel. This reduces the chances of guessing the right password, making it hard to access and login to the admin panel. • Multi-factor authentication (MFA) and 2-factor authentication (2FA): this could include having other authentication like a one-time-password (OTP) being sent to an email or phone number, finger or facial recognition, etc.