Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved is HTTP. Running tcpdump and loading yummyrecipesforme.com, the log informed us that there was a lot of traffic at port 80.

Section 2: Document the incident
Customers emailed the website owner in response to the need to download a file, redirecting you to a different website that slows down processing speeds. The website owner tried to log onto the admin panel, but is unable to. A security analyst was prompted to investigate this issue. A sandbox environment was loaded up and tcp dumping was used to capture network and traffic packets. The logs show that an IP was requested and upon loading up the website, yummyrecipesforme.com, a file was needed to be downloaded. Upon downloading, the log showed that the website requested a new IP to a different website called yummyrecipesforme.com, rerouting to it. A senior analyst confirms that the website was compromised and upon further inspection, they notice a javascript code has been added to prompt website visitors to download an executable file. The cybersecurity team reports that this issue was caused by a brute force attack as there were no controls in place to protect the website from this problem.

Section 3: Recommend one remediation for brute force attacks

Implementing password policies and 2FA would be remediations for brute force attacks. This would make it harder to guess the password and if the password was cracked, 2FA would validate unknown logins by asking for one time passwords.