Security incident report

Section 1: Identify the network protocol involved in the incident
HTTP

Section 2: Document the incident
Several customers contacted Yummyreceipyforme.com to complain about the download prompt and their machines being slow. The website owner could not log into the admin account to see what's going on. Cyber security analysts used a sandbox to run a test to see what was going on with the website after loading yummyreceipiesforme.com they observed a prompt to download an executable after downloading the executable a redirection happened to greatrecepiesforme.com With TCPdump we can observe that initially, the website is working properly but after the webpage of yummyreceipiesforme.com loads an executable is being downloaded using javascript to prompt the user to initiate. After the download, a redirection happens to greatreceipiesforme.com, After analyzing the source code a conclusion has been made the website has been compromised and javascript code has been added for the download and the redirection. The team believes a brute force attack has been conducted to compromise the password due to no known knowledge about the password being updated

Section 3: Recommend one remediation for brute force attacks
Password policies MFA IPS and IDS