Security incident report

Section 1: Identify the network protocol involved in the incident
HTTP: to load the website content and download the malicious executable file. (DNS was used to resolve domain names but it was not the main exploit)

Section 2: Document the incident
Users contacted helpdesk stating that upon entering the website, they were prompted to download and run a file that contained access to new recipes, after which they claim to have their computers slow down and website address changed. The website owner tried to login but was not able due to a password change to their account. The cybersecurity analyst started investigating the matter by first using a sandbox and opening the website, then running tcpdump. After downloading the recipes file from the prompt, they were redirected to a fake website The analyst observed the tcpdump logs and found the normal dns request and response of the actual website after which they recalled downloading and running the recipes files, which explains the sudden change in network traffic as the browser requests a new IP address for greatrecipesforme.com and traffic is rerouted there. The senior analyst confirms that the website was compromised, then they check the source code for the website and find out that it was altered and had some javascript code injected inside which prompted the users to download an executable file disguised as a browser update. The file was analyzed and was found that it contained a script that redirects the users to the fake website. The team believes it was a brute force attack done by a disgruntled hacker who was able to guess the password easily as it was still set to the default password. Users' computers were also compromised in the attack

Section 3: Recommend one remediation for brute force attacks
• Enforce stronger and non-default password policies • Enforce account lockouts after a limited number of failed login attempts. • Prevent the reuse of old passwords • Require frequent updates to passwords • Implementing MFA