Security incident report

Section 1: Identify the network protocol involved in the incident
The primary network protocol involved in the incident based on tcpdump logs is HTTP over port 80. Secondarily DNS over port 53.

Section 2: Document the incident
An attacker has used a simple brute force attack to gain access to the web host admin panel for the website. Primarily caused by insufficient password controls. The attacker then added code to the site's source code triggering visitors to download and run a file. Then visitors were then redirected to a new domain greatrecipesforme.com. The incident was discovered when customers emailed the help desk complaining about a file download when loading the site, redirection to a new site and their computer now running slower.

Section 3: Recommend one remediation for brute force attacks
Immediately change default passwords and implement stronger password controls. Also recommend rate limiting login attempts to restrict attempts per IP address. Then implement 2FA/MFA.