Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is TCP and HTTPS.

Section 2: Document the incident
The yummyrecipesforme.com website was attacked by malicious attackers. The attacker gained control of administrative control by using brute force attack to gain access and then changed the password to prevent access by admin. The attacker then installed a piece of code into the website such that a file containing malware is installed into the system and redirected to a fake malicious website called greatrecipesforme.com. When a HTTPS connection is established after the TCP Three way handshake, a DNS request for greatrecipesforme is submitted automatically and redirected to the malicious website.

Section 3: Recommend one remediation for brute force attacks
Some remediations are : 1. Multifactor authentication 2. Captcha and reCaptcha 3. Stronger passwords