Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involved several network protocols. DNS (Domain Name System) was used to resolve the website URLs to IP addresses, including `yummyrecipesforme.com` to `203.0.113.22` and the malicious redirect `greatrecipesforme.com` to `192.0.2.17`. TCP (Transmission Control Protocol) was used to establish reliable connections between the client and web servers, including the standard three-way handshake (SYN, SYN-ACK, ACK). HTTP (Hypertext Transfer Protocol) was used to request and retrieve the website content, including both the legitimate webpage and the malicious executable file that was downloaded from the attacker's site.

Section 2: Document the incident
The website `yummyrecipesforme.com` was compromised by a former employee who performed a brute force attack using default administrative credentials. After gaining access to the admin panel, the attacker modified the website's source code to include JavaScript that prompted visitors to download an executable file. When executed, the malware redirected users to a malicious website, `greatrecipesforme.com`, causing their computers to slow down and potentially become further compromised. Customers reported the issue to the helpdesk, and the website owner was unable to log in due to the attacker changing the administrative password. Network analysis confirmed DNS and HTTP requests to both the legitimate and malicious websites, revealing the path of infection and highlighting the root cause: weak default credentials, lack of brute force protection, and unauthorized modification of the site's source code.

Section 3: Recommend one remediation for brute force attacks

To prevent similar brute force attacks in the future, the organization should implement an account lockout policy that automatically locks administrative accounts after a set number of failed login attempts, such as three to five. This should be combined with strong password requirements and multi-factor authentication (MFA) to ensure that even if passwords are guessed, unauthorized access is prevented. Additionally, monitoring failed login attempts and sending alerts to administrators can help detect and mitigate attacks before they result in compromise.