Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in the incident include: ● **DNS (Domain Name System)**: Used to resolve the domain names (yummyrecipesforme.com and greatrecipesforme.com) to their respective IP addresses. ● **HTTP (Hypertext Transfer Protocol)**: Used to request web pages and download the malicious file. ● **TCP (Transmission Control Protocol)**: Ensures reliable communication between the client and the compromised web server.

Section 2: Document the incident
The attacker gained access to `yummyrecipesforme.com` through a **brute force attack**, exploiting the weak default password of the admin account. They modified the **website source code** by embedding **JavaScript malware**, which prompted users to download a file. When users visited `yummyrecipesforme.com`, the **browser sent a DNS request** to resolve the domain's IP address. The **HTTP request to the server** initiated the webpage load, and a malicious file was prompted for download. Once users executed the file, their browser was **redirected to a fake website** (`greatrecipesforme.com`), which contained further malware. Users reported slow PC performance after running the file, indicating potential malware infection.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks, the company should implement **Multi-Factor Authentication (MFA)** for admin logins. MFA would require a second form of authentication (e.g., a one-time password or authentication app), making it significantly harder for attackers to gain access even if they guess the correct password.