Security incident report

Section 1: Identify the network protocol involved in the incident
DNS (Domain Name System): Used to resolve the domain names `yummyrecipesforme.com` and `greatrecipesforme.com` into their respective IP addresses. **HTTP (Hypertext Transfer Protocol):** Used to send web page requests and also to initiate the download of the hosted malware. Both protocols are commonly used by attackers in phishing campaigns and malware delivery.

Section 2: Document the incident
A former employee executed a brute force attack to gain administrative access to the `yummyrecipesforme.com` website. The admin password was set to a weak default, making it easy to guess. Once access was obtained, the attacker injected a malicious JavaScript script into the site's source code. This script prompted visitors to download a file under the pretense of updating their browsers. Upon execution, the file redirected the users' browsers to a fake site, `greatrecipesforme.com`, which hosted malware. Users began reporting that the site asked them to download a suspicious file and that their computers became slower after doing so. DNS and HTTP traffic captured via `tcpdump` confirmed the redirection and the malicious behavior.

Section 3: Recommend one remediation for brute force attacks
Implement **account lockout policies** after several failed login attempts. For example, lock the account temporarily after 5 incorrect password attempts. Additionally, disable default credentials and enforce **multi-factor authentication (MFA)** for administrative access.