Security incident report

Section 1: Identify the network protocol involved in the incident
Both DNS and HTTP were involved in this incident.

Section 2: Document the incident
According to the logs, a valid DNS request was made for “yummyrecipesforme.com” from a source device. The source then made an HTTP connection request to the web server at 2:18pm. Following this HTTP request, at 2:20pm another DNS request was made for “greatrecipesforme.com”, which was then followed by an HTTP connection request to that web server. The cybersecurity team discovered that a password brute-force attack was performed on the admin account for the web server. This allowed a malicious actor to inject Javascript code onto the website that requested users to download a file that redirects them to greatrecipesforme.com. This is consistent with the network traffic described above.

Section 3: Recommend one remediation for brute force attacks
To remediate this incident, strong password policies for all server accounts should be enforced. For admin accounts, multi-factor authentication (MFA) should also be enforced. Additional monitoring of login attempts can also be implemented.