Security incident report

Section 1: Identify the network protocol involved in the incident
DNS (Domain Name System) was used to discover the IP addresses of the websites, first for "yummyrecipesforme.com" and then for the malicious site "greatrecipesforme.com". **TCP (Transmission Control Protocol)** was used to create a stable network connection between the user and the web server. The proof is in the logs with the [S] and [S.] flags, which initiate the connection. **HTTP (Hypertext Transfer Protocol)** was used to request and load the web page content. It was through HTTP that the compromised site delivered the malicious script to the user.

Section 2: Document the incident
1. The user connected to the website "yummyrecipesforme.com". The logs show the initial DNS query and HTTP connection. 2. Upon loading the site, a script injected by the attacker requested a file download. 3. The script forced the browser to make a new DNS query, this time for "greatrecipesforme.com". This is the key evidence of the redirection. 4. The user's browser connected to the new IP address, completing the attack and exposing the machine to malware. 5. The incident was possible because the attacker gained access to the admin panel through a brute-force attack, exploiting a default password that was never changed.

Section 3: Recommend one remediation for brute force attacks
The main recommendation is to implement a robust access control policy. This includes strong password policies, requiring passwords of at least 12 characters, including uppercase letters, lowercase letters, numbers, and symbols. Prohibit default or weak passwords. Implement automatic account lockout after a low number of failed login attempts (e.g., 5 attempts) to neutralize automated brute-force attacks. Enable Multi-Factor Authentication (MFA) for all administrative accounts.