Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol identified during the investigation was HTTP, which was used to deliver the altered webpage, the malicious executable, and the redirection to the fraudulent domain

Section 2: Document the incident
A former employee gained access to the administrative portal through a brute-force attack made possible by the default admin password. After logging in, the attacker changed the password, modified the website's source code, and added malicious JavaScript prompting users to download an executable. When executed, the file redirected visitors from the legitimate website to a fake domain hosting malware

Section 3: Recommend one remediation for brute force attacks
Implementing multi-factor authentication (MFA) is recommended, as it prevents attackers from accessing the administrative portal even if they manage to guess or obtain the password