Security incident report

Section 1: Identify the network protocol involved in the incident
Communication protocols are involved in this incident: - Hypertext Transfer Protocol - Domain name system

Section 2: Document the incident
Someone took over the administration's account using brute force attack and put malware inside the website. The source computer using port 52444 sent a DNS resolution request to the DNS server dns.google.domain which it replied back to the source computer with the IP address 203.0.113.22 of the destination URL. Then the source computer sends a connection request to the destination website yummyrecipesforme.com.http from port 36086, which the destination website replies back with acknowledging the request. The log entry HTTP: GET / HTTP/1.1 shows that the browser requested data from the website. This could be the request for downloading the malicious file. And this time, the source computer sends a DNS resolution request to the DNS server to connect with the fake website called greatrecipesforme.com. The DNS server replied with the IP address 192.0.2.17 of the malicious website. Then the source computer sends a connection request to the malicious website from port 36086, which the malicious website replies back with acknowledging the request. And again, the browser requested data from the website using HTTP: GET / HTTP/1.1.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks from happening again, a strong password and a frequent password change policies needs to be established.