Security incident report

Section 1: Identify the network protocol involved in the incident
HTTP, a communication protocol that is not secure enough. When they loaded the webpage initiated an HTTP request, it was able to download a file containing malware.

Section 2: Document the incident
In a sandbox environment, I ran the network protocol analyzer tcpdump, then typed in the URL for the website, yummyrecipesforme.com. As soon as the website loaded, I was prompted to download an executable file to update my browser. I accepted the download and allowed the file to run, then noticed that my browser redirected me to a different URL, greatrecipesforme.com, which contains the malware. The logs show the following process: 1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server. 2. The DNS replies with the correct IP address. 3. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server. 4. The browser initiates the download of the malware. 5. The browser initiates a DNS request for greatrecipesforme.com. 6. The DNS server responds with the IP address for greatrecipesforme.com. 7. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks
A stronger password policy, with more complicated password requirements for the admin credentials : no default passwords allow, disable all the old passwords, establish multi factor authentication.