Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfer protocol (HTTP). The issue was with accessing a web server therefore it most likely involves the HTTP protocol. Also while looking at the logs from tcpdump, we can see that http was used in contacting the web server. The malicious file is seen being transported to the user's computer using HTTP at the application layer.

Section 2: Document the incident
Several customers contacted the helpdesk stating that when they visited the website, they were prompted to download a file that redirected them to another website called "greatrecipesforme.com". Their computers started to operate slower than they were operating before after accessing the new website. The website owner also tried to access the admin account for the website but he was locked out of the account. After being notified of the incident, I tried navigating to the website while running a network sniffing tool called tcpdump to further understand what was happening. I also was doing this in a sandbox to avoid downloading any malware on my device. When I navigated to the website, I was prompted to download a file that would give me access to free recipes. After I downloaded it, I was redirected to a website called "greatrecipesforme". Looking at the logs, it is clear that when users type "yummyrecipes.com" they are going to the real sites as DNS resolves to the actual IP of the site. After HTTP gets the content of the site, there was a sudden change in the tcp logs and it was noticed that there was a new DNS request being sent from the client for a website titled "greatrecipesforme.com". The DNS resolution for this website is successful and the browser then establishes a connection over HTTP with the new website. After analyzing the source code, it was discovered that an attacker had added code to the website that prompted the users to download the malicious file. Also since the website owner stated that they had been locked out of their administrator account, I believe that the attacker may have used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
One security measure to remediate or prevent brute force attacks is the implementation of MFA (multi-factor authentication) as well as an account lockout policy. MFA requires authentication via a password and another method such as an OTP sent to the user's phone or email. also by confirming a one-time passcode (OTP) sent to either their email or phone. This disallows an attacker from accessing the system even if they guess the password. An account lockout policy also limits the amount of time an attacker can try to guess a password.