Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol impacted during this incident was the Hypertext transfer protocol (HTTP). After running tcpdump, I established the DNS and HTTP log file gave enough evidence to come to that conclusion. The malicious file was transported into the users' computer using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers reported that they were prompted to download and run a file when they visited a website. After downloading and running the file, their computers started to run slowly. The website owner tried to log into the web server, but they were locked out of their account. A cybersecurity analyst tested the website in a sandbox environment. When the analyst visited the website, they were prompted to download and run a file. After downloading and running the file, the analyst was redirected to a fake website. The cybersecurity analyst inspected the tcpdump log and saw that the browser initially requested the IP address for the original website. However, after the analyst downloaded and ran the file, the browser requested a new IP address for the fake website. The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. They found that an attacker had manipulated the website to add code that prompted users to download a malicious file disguised as a browser update. The analyst believes that the attacker used a brute force attack to access the website owner's administrator 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
To protect against brute force attacks, the team plans to implement two-factor authentication (2FA). With 2FA, users will need to provide two pieces of information to log in: their login credentials and a one-time password (OTP) sent to their email or phone. This additional layer of security makes it much more difficult for attackers to gain access to accounts, even if they have the user's password.