Security incident report

Section 1: Identify the network protocol involved in the incident
The affected protocol is the HTTP protocol. Using tcpdump, we analyzed the log files, which identified an issue with HTTP and DNS. Since the error lies within the HTTP protocol, the malicious file was moved through the application layer.

Section 2: Document the incident
Customers reported that the website yummyrecipesforme.com was prompting them to download an update to their browser. They also noted that their computer had been operating slowly since the incident. The website owner was also unable to log back into the website. *The cybersecurity analyst checked the tcpdump log and noted that the browser requested the IP address for the intended website, yummyrecipesforme.com. After the connection to the website was established over the HTTP protocol, the analyst ran the executable file that was prompted by the website. This caused a change in network traffic and a resolution to a different IP address for a website called greatrecipesforme.com.* *On the new website, all the recipes were now free of charge. At 2:18 pm, the senior cybersecurity analyst tested the malicious website in a safe sandbox environment. After opening yummyrecipesforme.com and downloading the suspicious software, the senior cybersecurity analyst has confirmed that the attacker spoofed the website using malware. It is suspected that the attacker brute forced a default password and gained access to the website and inserted malware that created the nearly identical spoofed website. The malware also caused the end users' computers to slow down.*

Section 3: Recommend one remediation for brute force attacks

To prevent further brute force attacks, the bakery should not use default passwords for admin access to the website. They should also update their passwords more frequently to even further prevent guessing. Also, having the administrators use MFA would prevent anyone from accessing the website maliciously, even if they did guess that password.