Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved with this incident is a HTTP. This is because visitors of the website are requesting to visit it on the web, which involves HTTP traffic. When I ran the tcpdump I could see that my machine was trying to access the website using the basic HTTP protocol. When my machine tried to access the website, it was given an acknowledgement for access [S.]

Section 2: Document the incident
Customers of the website, yummyrecipesforme.com , talked to the help desk support because they were prompted to download new recipes. After downloading the new recipes, the customers stated that their computers started to run slower. The website owner tried to log into their website but they were locked out. The cybersecurity analysts used a sandbox environment so that the website wouldn't harm their network. Then they ran a tcpdump to see what the network traffic said when interacting with the website. The analysts were prompted to download some free recipes, when they clicked on it, they were redirected to the new fake website, greatrecipesforme.com . The analysts looked over the tcpdump log and found that the browser initially requested the ip address for the correct website. However, once the connection request was made, they were redirected to the fake website over the HTTP protocol. The cyber security analysts discovered that the malicious actor wrote some java code that prompted the visitor to download the free recipes, and once done it would infect their computer. The website owner stated that they were locked out of their account, which means that the malicious actor brute forced their way into it and changed the login information.

Section 3: Recommend one remediation for brute force attacks
One security measure to prevent brute force attacks is a new password policy for the company. A good suggestion for passwords is to have it be 8 characters or more in length, a capital letter, and a symbol. This situation only happened because the malicious attacker was able to access the administrators account by a brute force attack. Another recommendation that I would say, is for the company to start using 2FA, two factor authentication.