Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in this incident is the Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic.

Section 2: Document the incident
We became aware of a potential security risk when multiple customers emailed yummyrecipesforme's helpdesk. Customers complained that the company's website had prompted them to download a file to access free recipes. They claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. To address the incident, I created a sandbox environment to observe the suspicious website behavior. I ran the network protocol analyzer tcpdump, and then proceeded to type in the URL for the website. The reported customer claims are validated as I am then prompted to download an executable file to update my browser. Upon allowing the file to run, I am redirected to a different URL: greatrecipesforme.com. Which houses the malware slowing personal computers implicated in this now definitive security breach.

Section 3: Recommend one remediation for brute force attacks
One remediation for this brute force attack would be monitoring login attempts. Whoever seized control of the website, did so by repeatedly guessing the password likely through pre-existing knowledge of potential passwords. By monitoring the attempts, not only can we limit how many attempts are allowed before access is locked, but also we can see where access is attempting to be gained from.