Security incident report

Section 1: Identify the network protocol involved in the incident
Since we found, “yummyrecipesforme.com.http:” in the tcpdump logs we can point to the network protocol involved being HTTP.

Section 2: Document the incident
Some customers report that they had to download a file from the website and that when executed the URL was changed for the website. It has slowed down users' computers. The owner of the website is locked out. We used a sandbox environment to test it on our end and received the issue the customers are facing, logs showed a change of website destination when executed. We believe the website admin was hacked by a brute force attack, and the password was changed giving the attacker control of the source of the website and updating it to add their malware. This malware when downloaded and executed redirects the url to their own malicious website which could further cause damage to users.

Section 3: Recommend one remediation for brute force attacks
One of the security measures known to protect from a bruteforce attack was that the attacker used a default password. We should always set secure passwords as they are harder to bruteforce because of time complexity. The second measure is to always setup 2FA authentication meaning even if the attacker was to gain access to your password, they would need a secure code or device that only you have to get past the second set of barriers.