Security incident report

Section 1: Identify the network protocol involved in the incident
The web server is using HTTP, which is an unsecure protocol.

Section 2: Document the incident
TCPDUMP data shows that the original session to yummyrecipesforme.com is successful. Subsequently, the Client uses DNS once again to resolve greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks
The bad actor was able to use a brute force attack to determine the password for the yummyrecipesforme.com website. Using a complex password would help prevent this type of attack Requiring different passwords for the administrator would help with determining which user is responsible for accessing a website server. In this case it appears there was only one password being used for all administrators. Multi-factor authentication would also help prevent this type of attack. When the baker left the organization, it would be beneficial to remove all their access to vital company resources.