Security incident report

Section 1: Identify the network protocol involved in the incident

HTTP and DNS.

Section 2: Document the incident

The admin password for the website yummyrecipes.com was weak and ended up being compromised by a Brute force attack. The logs from tcpdump (see attachment) show that the cybercriminal took advantage of this, installing a malware that redirected from the original site to the newly created greatrecipesforme.com, which distributed the recipes owned by the original site for free.

Section 3: Recommend one remediation for brute force attacks

-Increase security by switching to an HTTPS domain or implement stricter password policies or multi-factor authentication (MFA)