Security incident report:

OS hardening techniques

Section 1: Identify the network protocol involved in the incident

The protocol involved in the incident is HTTP.

Section 2: Document the incident

Multiple customers contacted yummyrecipesforme's helpdesk complaining that the company's website had prompted them to download a file to access free recipes. The customers claimed that after running the file, the address of the website changed and their personal computers began running more slowly. The website owner tried to log in to the admin panel but is unable to.

I used a sandbox environment to open the website. Then, I ran tcpdump to capture the network traffic packets produced by interacting with the website. I was prompted to download a file and the browser redirected me to a fake website.

I inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Then, I downloaded and executed the file. The logs showed that the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the fake website.

Since the website owner said that they weren't able to access the admin panel, it is possible that the attacker used a brute force attack to access the account and change the admin password.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks, it is necessary to implement password policies, disallow old or default passwords from being used and enable two-factor authentication.