Security incident report

Section 1: Identify the network protocol involved in the incident

HTTP is used in this incident. It involves a problem in accessing the web server and the tcpdump log shows there are usage of http protocol.

Section 2: Document the incident

Multiple customers emailed yummyrecipesformes'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 into the admin panel but was unable to. The cybersecurity team took action by looking into the tcpdump logs to investigate the situation. They were prompted to download a file and it redirected to a fake website.

Initially, the DNS request replied with the correct IP address. Then in the logs, around 2:18PM, it shows that there is a lot of traffic on port 80. Around 2:25PM, the DNS server routes the traffic to a new IP address and its associated URL. The traffic changes to a route between the source computer and the spoofed website. The port number changed again when redirected to a new website. It changed from port number 52444 to 56378. This incident most likely happened in the application layer of the TCP/IP model which involves HTTP protocols.

Section 3: Recommend one remediation for brute force attacks

It is mentioned that the admin password was a default password. In order to fix this problem and fix the ongoing future problems, the organization can use password policies to standardize good password. They could make the password more complex, increase the frequency of updating passwords, check whether the password can be reused or not, and put limits to how many times a user can attempt to log in before their account is suspended.