Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is HTTP. (Hypertext Transfer Protocol). From the onset of the incident, we were informed the issue had to do with accessing the web server for “yummyrecipesforme.com”. Upon running and analyzing tcpdump, the log file showed http usage including a GET request for the malicious file.

Section 2: Document the incident
Customers contacted the company’s helpdesk and reported that they were being prompted to download a file when visiting the website. The customers also mentioned that ever since the download of this file, they were experiencing decreased performance on their computer. Upon initial investigation, the website owner attempted to log into the web server and discovered that they were locked out of their account. The security analyst investigated this further by accessing the company website in a sandbox environment and capturing the network traffic using tcpdump. The analyst was prompted to download a file which caused their browser to redirect to the spoofed website “greatrecipesforme.com”. Upon analyzing the tcpdump log, a sudden change in traffic occurred after the malicious file was downloaded. The browser began to request a new IP address which resolved to “greatrecipesforme.com” a malicious website. A senior analyst completed a more in-depth analysis of the company website and discovered that the attacker added code to the source code which prompted users to download the malicious file. The cybersecurity team believes that the attacker used a brute force attack to gain access to the company website and manipulate the source code.

Section 3: Recommend one remediation for brute force attacks
Since the attacker was able to gain access by using a default admin password, the team plans to implement the following security measures for passwords. ● Disallow previous passwords ● 2FA (Two-Factor Authentication) ● OTP ● Require frequent password updates.