OS Security Hardening

Section 1: Identify the network protocol involved in the incident

In this incident, the analysis logs show the connections between the user, the Google domain server, and the web servers with the recipes (paid and not paid). Throughout the tcpdump the common protocol used is IP to make connections between the user and the servers.

Section 2: Document the incident

This incident was first observed by yummyrecipesforme.com users. They then contacted the company's helpdesk complaining that the company website was prompting them to download a file and update their browsers. They then claimed that after running the file, the address of the website changed and their computers were running slowly. The owner of the website tried to log in to the admin panel but was locked out, so they contacted our cybersecurity team to investigate.
Our team decided to take precautions by loading up the website in a sandbox environment. We then ran tcpdump, a network protocol analyzer, on the URL for the website (yummyrecipesforme.com). We noticed that upon the loading of the webpage, the user is prompted to download a .exe file to update their browser. By accepting the download and running the executable, our browser redirected us to a different webpage (greatrecipesforme.com) which looks exactly like the original website, but with all the recipes available for free.
Below is a more detailed breakdown of what the logs showed:

- The browser requests a DNS resolution for the URL yummyrecipesforme.com
- The DNS replies with the correct IP address for the website.
- The browser initiates an HTTP request for the webpage.
- The browser initiates the download of the malware.
- The browser then requests another DNS resolution, now for the URL greatrecipesforme.com
- The DNS server responds with the new IP address.
- The browser initiates an HTTP request to the new IP address (wrong one).

Upon further investigation, one of the senior analysts confirmed that the website was compromised upon finding a suspicious javascript in the website's source code. This would run after the user makes an HTTP request and prompts users to download an executable file. The script was then analyzed and found to have redirected any user's browser from the original yummyrecipesforme.com to greatrecipesforme.com.

After learning that the owner of the website no longer had access to the admin features, our team concluded that the website was hacked by a brute force attack. It was found that the owner had not changed the admin password from the default, thus allowing the malicious actor to easily hack and inject the web server with a malicious script.

Section 3: Recommend one remediation for brute force attacks

Out of all the possible solutions to increase security in an attempt to prevent brute force attacks, I believe introducing two-factor authentication (2FA) is the best solution. Having a proper 2FA implemented can almost guarantee full security from brute force attacks as it adds another layer of protection to your account. A 2FA app that refreshes every few seconds ensures that the malicious actor not only has to correctly guess your password but also the 2FA code that is constantly changing. This would've helped the owner of yummyrecipesforyou as it would've required the malicious actor to provide a secure, frequently alternating code to gain access to the admin controls of the website.