# Applying OS Hardening Techniques Activity Summary

This activity was provided by the Google Cybersecurity Certificate. In this activity, a disgruntled baker has decided to publish the best-selling recipes of the website yummyrecipesforme.com for free. The baker executed a brute force attack to gain access to the web host. After they obtained the login credentials, they were able to change the website’s source code and embed a JavaScript function that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller’s recipes are now available for free. Several hours after the attack, multiple customers emailed yummyrecipesforme’s helpdesk. They complained that the company’s website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed, and their personal computers began running more slowly.

To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors’ browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

**Your job is to document the incident in detail**, including identifying the network protocols used to establish the connection between the user and the website.  You should also recommend a security action to take to prevent brute force attacks in the future. The Incident report and DNS/ICMP traffic log can both be found within this folder.