Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident

The protocol involved in the incident is the **Hypertext Transfer Protocol (HTTP)**. Since the issue involved accessing the web server for `yummyrecipesforme.com`, we know that requests to web servers for web pages use HTTP traffic. This is further supported by the tcpdump log file, which shows HTTP protocol activity when contacting the server. The malicious file prompting visitors to download it was also transported to users' computers via the HTTP protocol at the application layer

Section 2: Document the incident

Several customers contacted the helpdesk for `yummyrecipesforme.com` reporting that they were prompted to download and run a file claiming to provide access to free recipes. After running the file, their personal computers began operating more slowly. The customers also noticed that their browsers were redirected to a different website, `greatrecipesforme.com`.

The website owner attempted to log into the admin panel but was locked out of their account. They contacted the hosting provider, and the cybersecurity team was tasked with investigating the issue.

Investigation Details:

- A sandbox environment was used to safely observe the behavior of the compromised website without impacting the company's internal network.
- Using the network protocol analyzer `tcpdump`, analysts captured traffic while interacting with the website. They observed an initial HTTP request for the legitimate website, `yummyrecipesforme.com`. Upon visiting the website, the analyst was prompted to download a file. After executing the downloaded file, the browser redirected to the fake website `greatrecipesforme.com`.
- The tcpdump log showed that the browser first requested the IP address for `yummyrecipesforme.com`. Once the HTTP connection was established, the analyst downloaded the malicious file. The logs also revealed that the browser later requested the IP address for `greatrecipesforme.com`, confirming the redirection to the fake website.

Findings:

- A senior analyst examined the source code of `yummyrecipesforme.com` and found embedded JavaScript that prompted users to download the malicious file. The file executed a script that redirected browsers to `greatrecipesforme.com`.
- The team confirmed that the attacker gained unauthorized access to the admin account by exploiting the default admin password through a brute force attack. The attacker then changed the admin password to lock out the legitimate owner and injected the malicious code into the website.

Impact:

- End users who downloaded and ran the malicious file experienced compromised systems.
- The website's reputation was negatively affected, and customers' trust was compromised.

Section 3: Recommend one or more remediations for brute force attacks

To mitigate the risk of future brute force attacks, implementing **two-factor authentication (2FA)** is highly effective. This requires users to authenticate using both a password and a secondary verification method, such as a one-time passcode (OTP) sent to their email or mobile device.

Why 2FA is Effective:
Even if a malicious actor guesses or obtains the password, they cannot bypass the additional authentication layer without access to the user's secondary device or email. This significantly reduces the likelihood of unauthorized access, even in scenarios involving weak or reused passwords.

Additionally, combining 2FA with practices such as monitoring login attempts and enforcing strong, unique passwords would further enhance security.