Security incident report : Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is **HTTP (Hypertext Transfer Protocol)**. The issue occurred while trying to access the company's website, *yummyrecipesforme.com*, which means that the web requests were made through HTTP. When I ran **tcpdump** during the test, the logs confirmed that the communication with the server was happening over HTTP. The malicious file that infected users' devices was also transferred through this protocol at the **application layer**.

Section 2: Document the incident

Some customers reported that when they visited the company's website, they were asked to download a file offering "new recipes." After running it, their computers started to slow down significantly. The website owner also noticed they could no longer log in to their administrator account.

To analyze the situation, I used a **sandbox environment** to visit the website safely, without putting the company network at risk. While monitoring the activity with **tcpdump**, I was also prompted to download a file that claimed to contain free recipes. After running it, I was redirected to another fake site called *greatrecipesforme.com*.

By reviewing the **tcpdump logs**, I saw that my browser first connected to *yummyrecipesforme.com* using HTTP, and then, right after the file was executed, the traffic switched to the new address *greatrecipesforme.com*.

Later, the senior cybersecurity analyst checked the website's **source code** and the downloaded file. They discovered that the attacker had modified the site to make users install a malicious program disguised as a browser update. Since the admin account had been locked, it's very likely that the attacker used a **brute force attack** to break into the account and change the password. As a result, the downloaded file compromised users' devices.

Section 3: Recommend one remediation for brute force attacks
To protect against brute force attacks, we plan to implement several security measures: ● **Disallowing the reuse of old passwords**, especially default ones, to prevent attackers from exploiting known credentials. ● **Enforcing regular password updates**, so even if a password is leaked, it becomes unusable quickly. ● **Implementing two-factor authentication (2FA)**, requiring users to confirm their identity using both a password and a one-time passcode (OTP) sent via email or phone. These measures will make it much harder for attackers to gain unauthorized access, even if they attempt a brute force attack.