Security Incident Report: Apply OS Hardening Techniques

Section 1: Identify the network protocol involved in the incident
The protocol involved in this incident is the Hypertext Transfer Protocol (HTTP). This protocol is responsible for accessing the web server for the web page involved in the HTTP traffic of yummyrecipesforme.com. When we ran tcpdump for the website, the corresponding log showed the use of the HTTP protocol and a malicious file being transported along with it to the user's computer at the application layer.

Section 2: Document the incident
Several users contacted the helpdesk of the website, stating that while accessing yummyrecipesforme.com, it prompted them to download and run an executable file, and the website redirected to another website. Ever since, their devices have been running slow. The website owner tried to log in, but the password had been changed. The cybersecurity analyst has inspected the website in a sandbox environment. They used tcpdump to capture website traffic packets produced by interacting with the website. It was observed that as soon as they landed on the website, they were prompted to download and run an executable file to get access to free recipes. Then it redirected to a fake website (greatrecipesforme.com). The analyst has analyzed tcpdump logs and observed that the browser initially requested an address for the yummyrecipesforme.com website. Once a connection was established with the HTTP protocol to the website, the analyst

recalled downloading and executing the file. The browser showed a sudden change in network traffic as it requested an IP address for another website, greatrecipesforme.com, and redirected to that site.

The senior cybersecurity professional analyzed the source code of the websites and the downloaded file. They observed that the attacker had manipulated the site and added a script to download an executable file disguised as a browser update. Since the website owner has been locked out of the administrative account, our team believes that the attacker used a brute force attack to access the website, made changes to it, and then changed the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to make it mandatory to change default password as soon as they get access to the admin panel. And password should be in accordance with latest password standards. To make authentication more secure we could implement 2FA for login such as OTP to their email address or phone number. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authentication.