Activity: Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident
The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account. The website was tested via a sandbox environment so as not to affect the company network. Then, tcpdump was used to capture the network and protocol traffic packets produced by interacting with the website. A download prompt for a file appeared claiming it would update the user's browser. The download was accepted and the file was executed. This redirected the to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com). The website was inspected using the tcpdump log and it was observed that the browser initially requested for the yummyrecipesforme.com IP address. Once the connection with the website was established over the HTTP protocol, a download was initiated, the file was then executed. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. The source code for the websites and the downloaded file were both analyzed, and it was discovered that an attacker had manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change 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 two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.