Activity: Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident
The protocol in the incident is Hypertext transfer protocol (HTTP). We run tcpdump and access the yummyrecipesforme.com website to detect the problem, capture protocol and traffic activity in a DNS & HTTP traffic log file. The malicious file is seen being transported to the users' computers using the HTTP protocol in the application layer.

Section 2: Document the incident
Customers contacted the website owner stating that when they went on the website, they were prompted to download and run a file that asked them to update their browsers. Their computers have been operating slowly ever since. The website owner tried logging into the web server but they were locked out of their account. The cybersecurity analyst used a sandbox environment to test the website without affecting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user's browser. He accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com). The cybersecurity analyst inspected the tcpdump log and saw that the browser had first requested the IP address for the yummyrecipesforme.com website. 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 senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst saw that the attacker had manipulated the website to add code that prompted the users to download a malicious file masked 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). Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.