Activity Exemplar: 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 was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve HTTP traffic. Additionally, when we ran tcpdump and accessed the yummyrecipesforme.com website, the corresponding tcpdump log file showed the usage of the HTTP protocol. The malicious file was observed being transported to users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when they visited the site, they were prompted to download and run a file that claimed to offer new recipes. 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 cybersecurity analyst used a sandbox environment to open the website without impacting the company network. They ran tcpdump to capture the network traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming to provide access to free recipes, accepted the download, and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com). Inspecting the tcpdump log, the analyst observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. A senior cybersecurity professional analyzed the source code for the websites

and the downloaded file. They discovered that an attacker had manipulated the website to add code that prompted 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 or more remediations for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to disallow the use of previous passwords. Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it's important to prevent old or default passwords from being reused. Additionally, requiring more frequent password updates will help ensure that any unauthorized person who learns a password will have less time to exploit it before it is changed. Finally, implementing two-factor authentication (2FA) will add an extra layer of security. 2FA requires a password and a one-time passcode (OTP) sent to the user's email or phone. This way, even if a malicious actor guesses the password, they would still need the OTP to gain access, making brute force attacks much less likely to succeed.