Security incident report

Activity Exemplar: Apply OS Hardening Techniques

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). Since the issue was related to accessing the web server for yummyrecipesforme.com, we can infer that requests to web servers for web pages typically 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 reporting that when they visited the website, they were prompted to download and run a file that supposedly contained access to new recipes. Their personal computers began operating slowly afterward. The website owner attempted to log into the web server but found they were locked out of their account.The cybersecurity analyst used a sandbox environment to open the website without impacting the company network. Then, the analyst 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). The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst downloaded and executed 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.

The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst 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 remediation for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to disallow previous passwords from being used. Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it's crucial to prevent any old passwords, such as default passwords, from being used to reset the password. Another supportive measure is to require more frequent password updates, ensuring that if any unauthorized person becomes aware of the password, they are less likely to be able to use it if the password is updated sooner. Finally, another effective solution is to implement two-factor authentication (2FA). 2FA requires authentication via a password and also by confirming a one-time passcode (OTP) sent to either the user's 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 attempting a brute force attack is unlikely to gain access to the system because it requires additional authentication.