Apply OS hardening techniques

Section 1: Identifiy the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfier protocol (HTTP). Since the issue was with accessing the web server fior yummyrecipesfiorme.com, we know that requests to web servers fior web pages involve http trafifiic. Also, when we ran tcpdump and accessed the yummyrecipesfiorme.com website the corresponding tcpdump log fiile showed the usage ofi the http protocol when contacting the . The malicious fiile 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's helpdesk stating that when they visited the website, they were prompted to download and run a fiile that contained access to 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 ofi 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 trafifiic packets produced by interacting with the website. The analyst was prompted to download a fiile claiming it would provide access to firee recipes, accepted the download and ran it. The browser then redirected the analyst to a fiake website (greatrecipesfiorme.com). The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address fior the yummyrecipesfiorme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the fiile. The logs showed a sudden change in network trafifiic as the browser requested a new IP address fior the greatrecipesfiorme.com URL. The network trafifiic was then rerouted to the new IP address fior the greatrecipesfiorme.com website.

The senior cybersecurity profiessional analyzed the source code fior the websites and the downloaded fiile. The analyst discovered that an attacker had manipulated the website to add code that prompted the users to download a malicious fiile disguised as a browser update. Since the website owner stated that they had been locked out ofi their administrator account, the team believes the attacker used a brute fiorce attack to access the account and change the admin password. The execution ofi the malicious fiile compromised the end users' computers.

Section 3: Recommend one or more remediations fior brute fiorce attacks
One security measure the team plans to implement to protect against brute fiorce attacks is to disallow previous passwords firom being used. Since the vulnerability that lead to this attack was the attacker's ability to use a defiault password to log in, it's important that we prevent any old passwords such as defiault passwords firom being used to reset the password. Another supportive measure is to require more firequent password updates, so in case any unauthorized person becomes aware ofi the password, they are less likely to be able to use that password ifi the password is updated sooner than later. Finally, another helpfiul solution is to implement two-fiactor authentication (2FA). 2FA requires authentication via a password and also by confiirming a one-time passcode (OTP) sent to either their email or phone. Once the user confiirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute fiorce attack will not likely gain access to the system because it requires additional authentication.