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 tra c activity in a DNS & HTTP tra c log le provided the evidence needed to come to this conclusion. The malicious le 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 le 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 cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol tra c packets produced by interacting with the website. The analyst was prompted to download a le claiming it would update the user's browser, 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 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 recalled downloading and executing the le. The logs showed a sudden change in network tra c as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network tra c 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 le. The analyst discovered that an a acker had

manipulated the website to add code that prompted the users to download a malicious le disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the a acker used a brute force a ack to access the account and change the admin password. The execution of the malicious le compromised the end users' computers.

Section 3: Recommend one remediation for brute force a acks

One security measure the team plans to implement to protect against brute force a acks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identi cation by con rming a one-time password (OTP) sent to either their email or phone. Once the user con rms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that a empts a brute force a ack will not likely gain access to the system because it requires additional authorization.