Security incident report

OS Hardening techniques

Section 1: Identify the network protocol involved in the incident
Hypertext transfer protocol (HTTP) is the protocol that was involved in the incident. The evidence required to draw this conclusion was provided by the traffic activity in a DNS & HTTP traffic log file, the results of running tcpdump.

Section 2: Document the incident
A large number of customers emailed to the website owner stating that when they visited the website, they were prompted to download to update their browsers. After that, their personal computers began running slowly. The website owner tried logging into the web server but was unable to. The cybersecurity analyst used a sandbox environment to test the website. 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, 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 file. 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 discovered that an attacker had manipulated the website to add code that prompted the 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.

Section 3: Recommend one remediation for brute force attacks
One remediation to protect against brute force attacks is enabling MFA authentication. This will include an additional method for users to validate their identification, for example a one-time password will be sent to the admin's phone. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.