# 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). The problem was with accessing the web server for yummyrecipesforme.com, which uses HTTP for web page requests. When we ran tcpdump and visited the yummyrecipesforme.com website, the log file confirmed the use of the HTTP protocol. The malicious file was seen being sent to users' computers through HTTP 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 file 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 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 it would 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 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.  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. The execution of the malicious file compromised the end users’ computers. |

|  |
| --- |
| **Section 3: Recommend one or more remediations for brute force attacks** |
| To protect against brute force attacks, the team plans to implement several security measures. First, they will disallow the reuse of old passwords, including default ones, as the vulnerability exploited by the attacker involved using a default password. By preventing the reuse of old passwords, they can enhance security significantly. Additionally, the team will require more frequent password updates to ensure that even if an unauthorized person learns a password, they are less likely to use it before it is changed. Finally, the team will implement two-factor authentication (2FA), which requires users to verify their identity with both a password and a one-time passcode (OTP) sent to their email or phone. This additional layer of security will make it much harder for malicious actors to gain access through brute force attacks. |