Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved Hypertext Transfer Protocol (HTTP). By using tcpdump and accessing the yummyrecipiesforme.com website to investigate the problem the suspicious activity has been detected. Traffic activity in a DNS and HTTP traffic log was enough to come to the conclusion that the malicious file is being transferred to the users' computers using the HTTP protocol.

Section 2: Document the incident
Multiple customers contacted the website owner stating that when they tried to visit the website, they were prompted to download and run a file that asked them to update the browser. After this action their personal computers have been operating slower than before. The website owner tried logging into the server but they were locked out of their account. The cybersecurity analyst used a sandbox environment to test the website. The analyst ran tcpdump to capture the network and protocol traffic packets. The analyst was prompted to download a file claiming it would update the browser, accepted the download and ran it. The browser then redirects the analyst to fake website (greatrecipiesforme.com) that looked identical to the original one (yummyrecipiesforme.com) After inspection of the log file produced by tcpdump the analyst observed that the browser initially requested the IP address for the yummyrecipiesforme.com website. Once the connection was established over the HTTP, the analyst downloaded and executed the file provided by the website. The logs show a change in network traffic as the browser requests the IP address for the greatrecipiesforme.com URL. The network traffic then is routed to the new IP address. The senior cybersecurity professional analyzed the source code for the website and the downloaded file. After analysis it has been discovered that an attacker has manipulated the source code of the website to prompt the users to download a malicious file. Since the website owner stated that they had been locked out of their administrator account, the security team believes that the

attacker used the brute force attack to access the account and change the administrator password. The execution of the malicious file compromised the end users.

Section 3: Recommend one remediation for brute force attacks
The brute force attack was successful due to a weak administrator account password. First step to mitigate a future risk of compromising the administrator account is change of password to other then default, also the password should follow the NIST 800-63b guidelines for password creation: ● It should be at least six characters in length ● It must contain characters from three of the following four categories: ○ English uppercase characters (A through Z) ○ English lowercase characters (a through z) ○ Base 10 digits (0 through 9) ○ Non-alphabetic characters (for example, !, $, #, %)