Security incident report

Section 1: Identify the network protocol involved in the incident
Based on the logs, DNS protocol and HTTP protocol are involved in the incident. This is evident based on the tcpdump logs captured during network traffic analysis.

Section 2: Document the incident
The incident occurs yummyrecipesforme.com helpdesk receives a complain about the company website that prompted visitors to download a file to access free recipes. After running the file, the website address changed, and the performance of the affected device drastically declined. This was witnessed by the owner who tries to login to the admin page to address the issue but they are unable to login. The website provider tasked us to investigate this security event. The logs show the following process: 1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server. 2. The DNS replies with the correct IP address. 3. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server. 4. The browser initiates the download of the malware. 5. The browser initiates a DNS request for greatrecipesforme.com. 6. The DNS server responds with the IP address for

greatrecipesforme.com.

7. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

When the senior team received this, the source code was inspected and noticed that a JS code has been added to prompt website visitors to download an executable file that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks
One recommendation to prevent brute force attack is enforcing two-factor authentication (2FA). By enforcing 2FA, it adds another layer of protection to the account.