Security incident report

Section 1: Identify the network protocol involved in the incident
In the security incident given, two network protocols can be identified : 1. DNS (Domain Name System) Server : A network protocol that translates internet domain names into IP addresses Steps involving DNS : 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 a DNS request for greatrecipesforme.com. 4. The DNS server responds with the IP address for greatrecipesforme.com. 2. HTTP (Hypertext Transfer Protocol) : Used for communication between the browser and the web servers Steps involving HTTP : 1. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server. 2. The browser initiates the download of the malware. 3. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

Section 2: Document the incident
Security Activity Detection : System recorded entry of several known default administrative passwords until the login credentials were obtained. Access to the admin panel and changes to the website's source code had been detected right after. Indication of a Brute force attack. Customers redirected to another malware website (greatrecipesforme.com) and were prompted to download a file, which impacted the users' device.

Security Activity Information : Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

Security Activity Analysis : A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They noticed that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.
The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Section 3: Recommend one remediation for brute force attacks
Recommended Remediation : 1. Security hardening : The process of strengthening a system to reduce its vulnerability and attack surface 2. OS Hardening : Regular Patch Updates are necessary 3. Penetration Testing : A simulated attack that helps identify vulnerabilities in networks, systems, websites and processes.