Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in this incident include several key components that facilitated the attack and redirection of users to the malicious website. First, the Domain Name System protocol played a role in resolving the domain names to their corresponding IP addresses. When a user entered yummyrecipesforme.com in their browser, a DNS request was made to obtain the IP address of the legitimate website. Later in the process, another DNS request was initiated when the browser was redirected to greatrecipesforme.com, the malicious site containing the malware. Next, the Hypertext Transfer Protocol was used for communication between the browser and the web server. After receiving the correct IP address from the DNS server, the browser made an HTTP request to fetch the content of yummyrecipesforme.com. Once the malicious JavaScript executed, the browser downloaded the executable malware file via HTTP. Later, another HTTP request was sent to greatrecipesforme.com, where the infected users were redirected. Moreover, the Transmission Control Protocol was involved in establishing and maintaining the connection between the user's browser and the web server. Since both HTTP and DNS rely on TCP for reliable communication, TCP ensured the proper transmission of requests and responses between the devices. These network protocols were exploited during the attack, allowing the hacker to manipulate the website and redirect users to a fraudulent page. Understanding these protocols is crucial for diagnosing security incidents and implementing protective measures against future attacks.

Section 2: Document the incident
A former employee executed a brute force attack on the administrative account of the web host for yummyrecipesforme.com. The attacker successfully

guessed the default admin password and gained access to the website's source code. They embedded a malicious JavaScript function that prompted visitors to download a file, which redirected them to a fake website containing malware. Multiple customers reported slow computer performance after downloading and running the file. The hacker also changed the admin password, preventing the website owner from accessing the admin panel.

During the investigation, analysts observed that users who visited yummyrecipesforme.com were prompted to download a suspicious file disguised as a browser update. The file, once executed, caused the browser to redirect to greatrecipesforme.com, which contained additional malware. Network traffic analysis revealed that the attack followed a sequence of DNS queries and HTTP requests to resolve and load both websites. The security breach resulted from the absence of proper authentication measures, allowing the brute force attack to succeed. The hacker exploited the use of default credentials and the lack of rate limiting for login attempts, emphasizing the need for improved cybersecurity defenses, including multi-factor authentication, password policies, and active monitoring of login attempts.

To mitigate future risks, yummyrecipesforme.com should implement security best practices such as enforcing strong password policies, enabling multi-factor authentication for all administrative accounts, and setting up rate-limiting mechanisms to prevent brute force attacks. Regular security audits should be conducted to detect vulnerabilities, and web application firewalls should be deployed to monitor and block malicious activity. Additionally, incident response plans should be established to ensure rapid detection and remediation of security breaches, minimizing potential damage to users and the organization.

Section 3: Recommend one remediation for brute force attacks
One effective remediation for brute force attacks is implementing account lockout policies. By configuring the system to temporarily or permanently lock an account after a certain number of failed login attempts, organizations can prevent attackers from continuously guessing passwords. For example, after five incorrect attempts, the account could be locked for a set duration or require administrator intervention to unlock. This significantly reduces the effectiveness of brute force attacks by limiting the number of attempts an attacker can make, thereby enhancing overall security.