Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in this incident are DNS and HTTP, both of which operate over the TCP/IP model. DNS (Domain Name System) was used to resolve the IP addresses of yummyrecipesforme.com and greatrecipesforme.com, while HTTP (Hypertext Transfer Protocol) was used to request and load the web content from both domains. The tcpdump logs show that the browser sent a DNS query for yummyrecipesforme.com, received the corresponding IP address, and then established a TCP connection over port 80 (HTTP) to load the website. After the malicious JavaScript was executed and the file was downloaded, a second DNS request was made for greatrecipesforme.com. The system then initiated another HTTP connection to this domain, indicating a redirection to a malicious site.

Section 2: Document the incident
The incident began when a former employee performed a brute force attack against the admin login panel of the yummyrecipesforme.com web server. By repeatedly attempting known default credentials, they were able to successfully log in due to the admin password still being set to the default value. Once access was gained, the attacker modified the website's source code by injecting a malicious JavaScript function. This script prompted visitors to download what appeared to be a browser update. When executed, the file redirected the victim's browser from yummyrecipesforme.com to a fake site, greatrecipesforme.com, which hosted further malware. The attacker also changed the admin credentials to lock out the legitimate owner. The tcpdump logs confirm this behavior. Initially, a DNS request was made to

resolve yummyrecipesforme.com, followed by an HTTP GET request to load the site. Shortly after, another DNS request for greatrecipesforme.com is visible, followed by a second HTTP session with that domain. This sequence confirms that the browser was redirected after executing the malware.

As a result, visitors were unknowingly redirected to a malicious website and infected with malware, which led to symptoms like system slowdowns. The attacker exploited poor password hygiene and the absence of brute force protection, causing both a reputational and security risk for the company.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks in the future, the organization should implement account lockout policies combined with multi-factor authentication (MFA). Account lockout policies limit login attempts and temporarily disable the account after repeated failed logins, slowing down or blocking brute force attempts. MFA ensures that even if a password is guessed or stolen, unauthorized access is still blocked by requiring a second verification method, such as an authentication app or SMS code. Additionally, it's critical to disable default credentials, enforce strong password requirements, and implement intrusion detection systems (IDS) to alert the security team of suspicious login patterns.