Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in the incident are DNS and HTTP. DNS (Domain Name System) was used to resolve the domain names yummyrecipesforme.com and greatrecipesforme.com to their respective IP addresses. Once the IP address for yummyrecipesforme.com was obtained, the browser used HTTP (HyperText Transfer Protocol) to request and load the webpage. The HTTP protocol was also used to initiate the download of the malicious executable file. After the file was executed, another DNS request resolved the IP for greatrecipesforme.com, followed by an HTTP request to load the malicious site.

Section 2: Document the incident
This afternoon, YummyRecipesForMe.com suffered a security breach initiated by a former employee who executed a brute force attack to gain administrative access. The attacker exploited the default password, successfully logged in, and modified the website's source code. Malicious JavaScript was embedded to prompt visitors to download a malware-laden executable file. When users executed this file, their browsers were redirected to GreatRecipesForMe.com, which hosted further malware. Customers reported suspicious activity, prompting an investigation by the cybersecurity team. Analysis in a sandbox environment using tcpdump confirmed the presence of malicious code and the redirection to the fake website. DNS and HTTP protocols were used to resolve domain names and load the webpages involved in the attack. The senior analyst identified the embedded JavaScript and confirmed the source code compromise.

Section 3: Recommend one remediation for brute force attacks
The team concluded that the attacker utilized weak password policies and the absence of brute force protection mechanisms. Recommendations include enforcing strong passwords, implementing account lockout mechanisms, enabling multi-factor authentication, and conducting regular security audits to prevent future incidents.