Security incident report

Section 1: Identify the network protocol involved in the incident

Protocols involved in the incident were DNS and HTTP protocols.
DNS was used to resolve the IP addresses for the domains yummyrecipesforme.com and greatrecipesforme.com. HTTP was then used to transmit the web content.

Section 2: Document the incident

The incident involved a brute force attack on the administrative account of the website. A former employee was able to gain unauthorized access by guessing the default password through repeated attempts. Once the former employee successfully logged in, they modified the website's source code by adding a JavaScript function that prompted users to download and run a malicious file.

When website visitors downloaded and ran the file, their browsers redirected them to a fake website, greatrecipesforme.com, which contained malware. This redirection led to user complaints reporting unusual download prompts and degraded performance on their personal computers.

Section 3: Recommend one remediation for brute force attacks

It is recommended to enforce two-factor authentication for all administrative accounts.