Security incident report

Section 1: Identify the network protocol involved in the incident

The incident began when the browser initiated an HTTP GET request to yummyrecipesforme.com using HTTP/1.1. This request likely initiated the download of a malicious file, as evidenced by the subsequent unusual traffic patterns in the logs, including significant data exchange on port 80.

Section 2: Document the incident

Several customers reported to the website's helpdesk that they were prompted to download a document claiming to contain new recipes, which infected their computers with malicious code and caused significant slowdowns. The website owner attempted to log in but discovered their account was locked. A cybersecurity analyst used a sandbox environment to safely interact with the website, capturing network traffic with `tcpdump`. During the analysis, the analyst was prompted to download the same file, which redirected the browser to a fake website, `greatrecipesforme.com`.
A senior cybersecurity specialist reviewed the captured traffic and analyzed the malicious file and the website's source code. They determined that a former employee likely executed a brute force attack to exploit weak, default-like passwords, gaining unauthorized access to the administrator account. Once inside, the attacker changed the admin password and deployed a script to redirect users to a malware-hosting page. This activity was consistent with both the anomalous network traffic and user complaints.

Section 3: Recommend one remediation for brute force attacks

To mitigate brute force attacks, implement a robust password policy requiring the use of unique, complex passwords with a minimum length of 12 characters, incorporating uppercase and lowercase letters, numbers, and symbols. Passwords should be changed periodically, with a recommended interval of 90 days.