**Security Incident Report**

**1. Network Protocol Identified**

The network protocols identified in the tcpdump log during the investigation include:

* **DNS (Domain Name System):** This protocol was used to resolve domain names (yummyrecipesforme.com and greatrecipesforme.com) to their respective IP addresses. The log shows DNS requests and responses.
* **HTTP (Hypertext Transfer Protocol):** This protocol was used for the transfer of web pages and the executable file. The log indicates HTTP requests for the website and the file download.

**2. Incident Documentation**

**Incident Summary:**

On September 09 of 2024, yummyrecipesforme.com, a website selling recipes and cookbooks, was compromised by a former employee. The attacker executed a brute force attack to gain access to the administrative account of the website. Using known default passwords, the attacker successfully accessed the admin panel and modified the website’s source code.

**Details of the Incident:**

* **Initial Compromise:** The attacker exploited a vulnerability in password security. The administrative account used a default password, which was easily guessed through a brute force attack.
* **Malicious Actions:** After gaining access, the attacker embedded a malicious JavaScript function into the website’s source code. This code prompted visitors to download a file, which was disguised as a browser update.
* **Redirect Behavior:** Once the file was executed, it redirected users from yummyrecipesforme.com to a fake website, greatrecipesforme.com, which contained additional malware. This caused users' computers to slow down and potentially suffer further issues.
* **Detection and Response:** Several hours after the attack, customers reported issues to the helpdesk, describing prompts to download a file and subsequent redirection. The website owner was unable to log into the admin panel, leading to an investigation.
* **Investigative Actions:** The tcpdump log was analyzed, revealing DNS and HTTP traffic patterns. The logs showed DNS requests for both domains and HTTP requests for the file download and subsequent redirection to the fake website.

**Sources of Information:**

* Tcpdump log analysis
* Customer complaints reported to the helpdesk
* Examination of the modified source code

**3. Recommendation**

**Recommendation for Preventing Brute Force Attacks:**

**Implement Strong Password Policies**

**Explanation:**

To prevent future brute force attacks, it is essential to implement robust password policies. The following measures should be adopted:

* **Password Complexity:** Require passwords to include a combination of uppercase and lowercase letters, numbers, and special characters to enhance complexity.
* **Minimum Length:** Enforce a minimum password length (e.g., twelve characters) to make passwords more resistant to guessing attempts.
* **Regular Changes:** Implement a policy for regular password changes (e.g., every 60 or 90 days) to limit the window of opportunity for unauthorized access.
* **Password Reuse Restrictions:** Prevent the reuse of previous passwords to ensure that old, potentially compromised passwords cannot be used again.

By enforcing these strong password policies, the organization will significantly improve its defense against brute force attacks and enhance overall security. Strong, complex passwords make it more difficult for attackers to gain unauthorized access, thereby protecting sensitive administrative accounts from future breaches.