Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involved HTTP, as web requests to yummyrecipesforme.com use this protocol. tcpdump logs confirmed HTTP traffic, with the malicious file delivered to users' computers via HTTP at the application layer.

Section 2: Document the incident
Customers reported that when visiting the website, they were asked to download a file with new recipes. After downloading, their computers slowed down. The website owner couldn't log into their account. A analyst checked the website in a safe environment and captured network traffic using tcpdump to analyze the issue. The analyst downloaded a file offering free recipes, which redirected them to a fake site (greatrecipesforme.com). Reviewing the tcpdump log, the analyst saw traffic shifted from yummyrecipesforme.com to the fake site after the file was run. A senior professional found that a hacker had added code to the site to prompt users to download a malicious file disguised as a browser update. The hacker likely used a brute-force attack to change the admin password, compromising users' computers.

Section 3: Recommend one remediation for brute force attacks
The team plans to block the reuse of previous passwords, especially default ones, to prevent brute-force attacks. They will also require more frequent password changes to reduce the risk of unauthorized access. Additionally, implementing two-factor authentication (2FA) will add another layer of security, requiring both a password and a one-time passcode (OTP) sent to the user's email or phone, making it harder for attackers to gain access.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Implementing multi-factor authentication 2. Making and enforcing strong password policies 3. Conducting firewall upkeep regularly

Part 2: Explain your recommendations
Enforcing MFA strengthens security by requiring multiple authentication steps, making brute force attacks and password sharing less effective. A strong password policy, including account lockouts, complex passwords, regular updates, and no reuse, reduces unauthorized access risks. Regular firewall updates help defend against emerging threats.Traffic from sources that are suspicious should be placed on a denied traffic list.