Activity: Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident

The incident involved the Hypertext Transfer Protocol (HTTP). This was confirmed through tcpdump logs when accessing yummyrecipesforme.com, which showed HTTP protocol usage for web server communication. The malicious file was transported to users' computers using HTTP at the application layer.

Section 2: Document the incident

Multiple customers reported being prompted to download a "recipe access" file when visiting the website, resulting in slower computer performance afterward. The website administrator discovered they were locked out of their account.

A cybersecurity analyst investigated by accessing the website in a sandbox environment while running tcpdump to capture network traffic. Upon accepting the download prompt for free recipes, the browser redirected to a fraudulent website (greatrecipesforme.com).

Analysis of tcpdump logs revealed the initial request for yummyrecipesforme.com's IP address, followed by HTTP connection establishment. After file execution, traffic was redirected to greatrecipesforme.com. Senior security staff discovered that attackers had modified the website code to prompt users to download malicious files disguised as browser updates. The team concluded that attackers likely used a brute force attack to gain administrative access and alter the password.

Section 3: Recommend one or more remediations for brute force attacks

The security team proposes several measures to prevent future brute force attacks. First, implementing a policy that prevents the reuse of previous passwords, including default ones. Second, requiring more frequent password updates reduces the window of opportunity for compromised passwords. Finally, implementing two-factor authentication (2FA) adds an extra security layer by requiring both a password and a one-time passcode sent via email or phone, making brute force attacks significantly less effective.