Security Incident Report

Section 1: Identify the network protocol involved in the incident

The primary network protocol involved in this incident is HTTP over TCP (port 80), which is used for transmitting web traffic. HTTP enables the transfer of website content, while TCP ensures a reliable connection between the client and server. Additionally, DNS (Domain Name System) was used to resolve the domain names into IP addresses before initiating web traffic. As confirmed by the tcpdump log, DNS requests were issued to resolve domain names, followed by TCP handshakes and HTTP GET requests to retrieve content from the resolved IP addresses.

Section 2: Document the incident

The tcpdump logs show that the machine first resolved the domain 'yummyrecipesforme.com' to IP address 203.0.113.22, then established a TCP three-way handshake and initiated an HTTP GET request. This activity initially appeared normal.

However, shortly afterward, the same system made a second DNS request for 'greatrecipesforme.com', which resolved to a different IP (192.0.2.17). Another TCP handshake and HTTP GET request followed. The sudden shift in domains and mirrored behavior suggests the user may have been redirected to a spoofed or malicious website.

While reviewing the logs, there was no direct evidence of a file download in this case. However, this redirection behavior is commonly used in phishing attacks or to serve malware. If users were prompted to download content or enter credentials, it could compromise the system. The redirection implies an attempt to move users away from a legitimate site toward a controlled, possibly malicious, domain.

In a real-world scenario, users might report slow system performance or suspicious downloads. In addition, the website owner might find themselves locked out, potentially due to brute force or credential stuffing techniques.

Section 3: Recommend one remediation for brute force attacks

To prevent brute force attacks, it is recommended to implement a host-based intrusion prevention system (HIPS) capable of monitoring suspicious HTTP behavior and blocking unauthorized access attempts. HIPS solutions can detect patterns such as repeated login attempts or domain redirects and prevent further exploitation.

Additionally, enabling two-factor authentication (2FA) can significantly reduce the risk of unauthorized access. Preventing the reuse of previous or default passwords, enforcing password complexity, and increasing password rotation frequency are all best practices that provide layered security against brute force attacks.