Security incident report

Section 1: Identify the network protocol involved in the incident

1. DNS (UDP Port 53):
    a. Observed in DNS requests/responses to resolve yummyrecipesforme.com and greatrecipesforme.com to their respective IP addresses (e.g., 203.0.113.22 and 192.0.2.17).
    b. Example log entries:

- 14:18:32.192571 IP your.machine.52444 > dns.google.domain: A? yummyrecipesforme.com.
- 14:20:32.192571 IP your.machine.52444 > dns.google.domain: A? greatrecipesforme.com.

2. HTTP (TCP Port 80):
    a. Unencrypted HTTP traffic facilitated communication between users and the compromised website.
    b. Observed during the download of the malicious executable and redirection to greatrecipesforme.com.
    c. Example log entries:

- 14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: GET / HTTP/1.1
- 14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: GET / HTTP/1.1

Section 2: Document the incident

A disgruntled former employee executed a brute force attack on the administrative account of yummyrecipesforme.com. The attacker exploited the use of a default password and the absence of brute force protections to gain access to the web host's admin panel. Post-compromise actions included:

- Injecting malicious JavaScript into the website's source code, prompting visitors to download a fake "browser update" executable.
- Redirecting users to greatrecipesforme.com, a fraudulent site hosting malware.

- Changing the admin password to lock out legitimate administrators.

Impact:

1. Users who downloaded the executable experienced malware infections (e.g., slowed computer performance, data theft).
2. The company's reputation suffered due to the breach and loss of customer trust.

Evidence from TCPdump Logs:

1. DNS Queries:
   - Initial resolution of yummyrecipesforme.com to 203.0.113.22.
   - Subsequent resolution of greatrecipesforme.com to 192.0.2.17 after the malicious download.
2. HTTP Traffic:
   - Unencrypted HTTP GET requests to both domains, confirming the download of the malicious file and redirection.

Source Code Analysis:

- Injected JavaScript code triggered forced downloads of the malware.
- Script embedded in the file redirected users to greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks

Implement Account Lockout Policies:

Action: Configure the system to lock administrative accounts after 3–5 consecutive failed login attempts for a minimum of 30 minutes.

Why This Works:

1. Disrupts automated brute force attacks by limiting repeated password-guessing attempts.
2. Forces attackers to abandon prolonged attacks due to account lockouts.

Additional Measures:

1. Eliminate default passwords: Enforce strong, unique passwords (e.g., 12+ characters with alphanumeric/symbol complexity).
2. Enable Multi-Factor Authentication (MFA): Add an extra layer of security to administrative accounts.