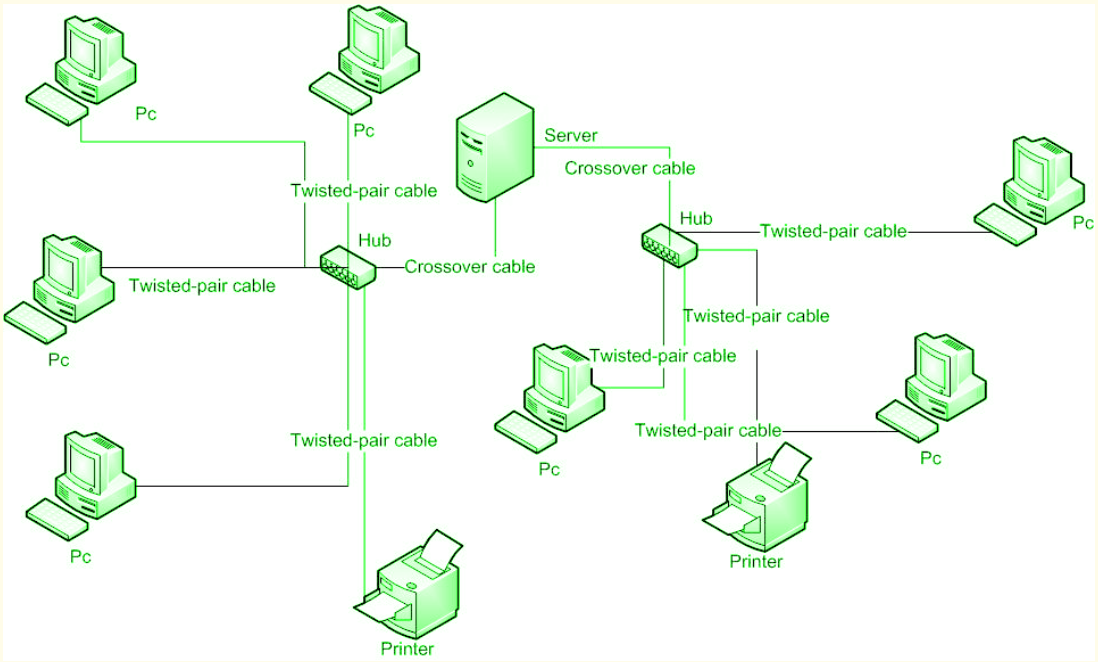
incident report

apply OS hardening techniques

Completed on
Mar 22, 2025

Prepared by
Ronel Peter

summary



Section 1: *Identify the network protocols involved in the incident*

- **DNS (UDP Port 53):**
  - Used to resolve domain names (*yummyrecipesforme.com and greatrecipesforme.com*) to their respective IP addresses.
  - Observed in DNS requests and responses (*e.g.,*
  - *14:18:32.192571 and 14:20:32.192571* in the TCPdump log).
- **HTTP (TCP Port 80):**
  - Facilitated unencrypted communication between users and the compromised website.
  - Logs show HTTP GET requests (e.g., *GET / HTTP/1.1*) to download the malicious file and load the fraudulent site.
- **TCP (Transport Layer Protocol):**
  - Established reliable connections via the three-way handshake (SYN, SYN-ACK, ACK flags).
  - Observed in TCPdump entries with flags [S], [S.], and [P.].

Section 2: *Document the incident*

Incident Overview:

On Tuesday, March 14th 2025, a disgruntled former employee compromised yummyrecipesforme.com via a brute force attack targeting the administrative account. 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:

1. Injecting malicious JavaScript into the website's source code, forcing visitors to download an executable file disguised as a browser update.

2. Redirecting users to greatrecipesforme.com, a fraudulent site hosting malware.

3. Changing the admin password to prevent legitimate access.

Discovery:

- The incident was reported by customers who experienced unexpected redirects and slow computer performance after downloading the file.

- The cybersecurity team confirmed the breach via TCPdump logs and source code analysis.

Evidence:

1. **TCPdump Logs:**

    a. DNS requests/responses for yummyrecipesforme.com (IP 203.0.113.22) and greatrecipesforme.com (IP 192.0.2.17).

    b. HTTP traffic (port 80) confirming unencrypted data transfers and redirection.

2. **Source Code Analysis:**

    a. Malicious JavaScript embedded in the website's code, triggering forced downloads.

Impact:

- Users' devices were infected with malware, leading to performance degradation and potential data theft.
- The company's reputation and customer trust were significantly damaged.

Section 3: Recommend one remediation for brute force attacks

Implement Account Lockout Policies:

- **Action:** Configure administrative accounts to lock after 3–5 consecutive failed login attempts for a minimum of 30 minutes.
- **Why This Works:**
    - Disrupts automated brute force attacks by limiting repeated password-guessing attempts.
    - Forces attackers to abandon prolonged attacks due to account lockouts.
- **Additional Measures:**
    - **Eliminate default passwords:** Enforce strong, unique passwords (12+ characters with alphanumeric/symbol complexity).

- **Enable Multi-Factor Authentication (MFA):** Add an extra verification layer for admin access.

The breach stemmed from weak authentication practices (default passwords) and inadequate brute force protections. Implementing account lockout policies and enhancing password requirements will mitigate future attacks. Documentation of this incident will serve as a reference for audits and employee training.