# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The tcpdump traffic log reveals the use of several key **network protocols**, each operating at different layers of the **TCP/IP model**. The primary protocols identified in the packet captures during the investigation are:  **1.** **DNS (Domain Name System)**   * **Function:** Resolves domain names (e.g., yummyrecipesforme.com, greatrecipesforme.com) to IP addresses. * **Evidence from log:**   + 14:18:32.192571 IP your.machine.52444 > dns.google.domain: A? [yummyrecipesforme.com](http://yummyrecipesforme.com).   + 14:20:32.192571 IP your.machine.52444 > dns.google.domain: A? greatrecipesforme.com.   **2.** **TCP (Transmission Control Protocol)**   * **Function:** Establishes reliable connections between the client and server using the TCP three-way handshake. * **Evidence from log:**   + IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S] (SYN)   + IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.] (SYN-ACK)   + IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.] (ACK)   **3.** **HTTP (Hypertext Transfer Protocol)**   * **Function:** Transfers website content between server and client. In this incident, it was used to deliver the malicious web page and executable. * **Evidence from log:** HTTP: GET / HTTP/1.1 | |
|

| **Section 2: Document the incident** |
| --- |
| **Incident Summary:** Several users reported being prompted to download a file when visiting **yummyrecipesforme.com**. After running it, their browsers redirected to **greatrecipesforme.com**, and system performance slowed. The issue was reported via helpdesk emails. **Where the Incident Occurred:** The incident took place on the website’s main server, hosted externally. Unauthorized access was gained through the admin panel. **How the Incident Happened:** A former employee performed a brute-force attack using default credentials. Once logged in, they embedded malicious JavaScript in the site, which triggered a file download and redirected users to a spoofed site containing malware.  **tcpdump log shows:**   1. DNS request for yummyrecipesforme.com 2. HTTP GET request to site 3. JavaScript triggers file download 4. DNS request for greatrecipesforme.com 5. Redirected HTTP request to fake site  **How the Incident Was Discovered:** Discovered through multiple customer complaints. Admin access was also blocked, indicating possible password change. The cybersecurity team analyzed traffic logs and website source code. **Sources of Information and Evidence:**  * Customer helpdesk emails * tcpdump network logs * Source code review * Malware behavior in sandbox * Analyst confirmation  **Conclusion:** The attack exploited default credentials and lacked brute-force protections. Malware was spread through the compromised website and redirected users to a malicious site. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| **Recommended Security Measure:** Limit the Number of Login Attempts**Explanation:** Limiting login attempts helps prevent brute force attacks by locking out or delaying access after a set number of failed login attempts. This makes it significantly harder for attackers to try multiple password combinations. It also alerts the security team to suspicious login behavior and reduces the risk of unauthorized access through password guessing. Implementing this measure, along with account lockouts or CAPTCHA, adds a strong layer of protection against credential-based attacks. |