Security Incident Report

1. Network Protocol Identified

The network protocol identified during the investigation is HTTP (Hypertext Transfer Protocol), which operates over TCP/IP.

Using the tcpdump packet capture logs, it was observed that communication between the client and the compromised website yummyrecipesforme.com occurred over port 80, indicating standard HTTP traffic. Additionally, DNS queries (over UDP/TCP port 53) were also present, resolving both the legitimate domain and the attacker-controlled domain greatrecipesforme.com.

This confirms use of the following TCP/IP stack layers:

- Application Layer: HTTP, DNS
- Transport Layer: TCP (for HTTP), UDP/TCP (for DNS)
- Internet Layer: IP
- Network Access Layer: Ethernet (assumed)

2. Incident Summary

On [Insert Date], a cybersecurity incident was discovered involving the company website yummyrecipesforme.com. Logs revealed that an attacker gained unauthorized access to the website's administrative panel via a brute force attack, exploiting the fact that the admin password was still set to the default credentials.

After gaining access, the attacker:

- Modified the website's source code.
- Embedded malicious JavaScript that prompted users to download a file.

- The downloaded file contained malware that redirected users to a fake website: greatrecipesforme.com.

The attack was discovered when internal monitoring tools flagged suspicious file downloads and customer reports began to surface. A senior analyst manually inspected the websites source code and confirmed the presence of malicious JavaScript.

Packet captures using tcpdump showed:

- DNS requests to yummyrecipesforme.com
- HTTP GET requests for the website
- HTTP-triggered download of an executable file
- A subsequent DNS request and HTTP connection to greatrecipesforme.com, confirming redirection

There were no brute force protections, no CAPTCHA, and no multi-factor authentication in place at the time of the attack. This allowed the attacker to gain full admin access with minimal effort.

3. Security Recommendation

Recommendation: Implement Two-Factor Authentication (2FA) for all administrative accounts.

Justification:

2FA significantly reduces the risk of unauthorized access, even if login credentials are compromised. By requiring a second verification method (such as a mobile authentication code), 2FA ensures that only verified users can gain access to sensitive systems. This would have prevented the attacker from accessing the admin panel after brute-forcing the password.