Security Incident Report – Brute Force Attack and Website Compromise

Objective

This report documents a cybersecurity incident affecting yummyrecipesforme.com, in which a former employee gained unauthorized administrative access to the company's web host. The attacker modified the website's source code to redirect users to a malicious domain and deliver malware. This report identifies the network protocols involved, explains how the attack occurred, and recommends security controls to prevent similar incidents in the future.

Incident Overview

Incident Type	**Brute Force Attack / Web Server Compromise**
Date Detected	Within hours of multiple customer complaints
Systems Affected	Web hosting server for yummyrecipesforme.com
Impact	Website redirection, malware delivery, and user system compromise
Detection Method	Customer helpdesk reports and tcpdump log analysis

Step 3: Identifying the Network Protocols Involved

Analysis of the tcpdump logs revealed that multiple network protocols were used during the interaction between the user's browser and the compromised website. These protocols align with the TCP/IP model and describe how communication occurred across the network.

Network Layer	**Protocol Identified**	**Purpose / Observation**
Application Layer	DNS, HTTP	DNS used to resolve domain names; HTTP used for web page
Transport Layer	TCP	Facilitates reliable data transfer between client and web server.
Network Layer	IP	Handles packet delivery between user device and website server.
Data Link Layer	Ethernet	Enables packet transmission within the local network.

Step 4: Incident Documentation

The attacker performed a brute force attack on the administrative account of the company’s website using known default passwords. After gaining access, the attacker injected malicious JavaScript into the site’s source code. The injected code prompted visitors to download an executable file containing malware, redirecting them to a fake site (greatrecipesforme.com). Multiple users reported system slowdowns and redirects after interacting with the site.

The investigation confirmed DNS and HTTP traffic between the original and fake websites. Evidence included tcpdump packet captures, access logs, and customer reports. The analysis indicated that weak credentials and lack of brute force prevention were primary vulnerabilities.

Step 5: Recommended Remediation – Preventing Brute Force Attacks

Recommended Measure: Implement Two-Factor Authentication (2FA) for Administrative Access

Two-factor authentication strengthens authentication security by requiring a second form of verification in addition to the password. Even if an attacker obtains valid credentials, they cannot log in without the secondary factor. This drastically reduces unauthorized access risks.

Benefits of 2FA:

- Prevents unauthorized access even if credentials are compromised.
- Mitigates brute force and credential-stuffing attacks.
- Increases accountability for administrative logins.
- Protects privileged accounts critical to web and system security.

Additional Security Recommendations

1. Enforce Strong Password Policies – Require complex passwords and regular rotation. 2. Limit Login Attempts – Configure lockout thresholds for repeated failed attempts. 3. Deploy Web Application Firewall (WAF) – Detects and blocks malicious traffic. 4. Monitor and Log Administrative Activity – Alert on logins from unknown IPs. 5. Conduct Security Awareness Training – Educate staff on password hygiene and phishing risks.

Conclusion

The incident at yummyrecipesforme.com was a result of a brute force attack exploiting weak default credentials. The attacker injected malicious JavaScript that redirected users to a fake website containing malware. Implementing two-factor authentication, combined with password hardening and access monitoring, would have prevented this attack. This event highlights the need for layered authentication and proactive monitoring to protect web infrastructure.

Cybersecurity Relevance

This investigation demonstrated practical tcpdump traffic inspection, understanding of TCP/IP layers, detection of web-based attack vectors, and effective incident response documentation aligned with SOC analyst and incident responder responsibilities.