# **Security incident report**

| Section | Summary |
| --- | --- |
| Section 1: Identify the Network Protocol | The incident investigation identifies the use of the DNS (Domain Name System) protocol. TCPdump logs show DNS resolution requests from the source computer to DNS servers for URLs like "yummyrecipesforme.com" and "greatrecipesforme.com." |
| Section 2: Document the Incident | A disgruntled attacker performed a brute force attack on "yummyrecipesforme.com," guessing the admin password. This allowed access to the admin panel, enabling changes to the source code. A javascript function was added, redirecting users to "greatrecipesforme.com" where recipes were offered for free. Customers reported slower computers. The cybersecurity team investigated using tcpdump logs in a sandbox environment. DNS and HTTP requests, as well as the malicious code, were identified. |
| Section 3: Recommend One Remediation | To prevent brute force attacks, the organization should enforce strong password policies: requiring complex passwords with upper/lower case, numbers, and special characters. Default passwords must be changed on system setup, and account lockout mechanisms should temporarily suspend accounts after failed attempts. Implement Multi-Factor Authentication (MFA) and conduct regular security audits to identify vulnerabilities. |