# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The incident involves two key network protocols:   1. DNS (Domain Name System, UDP/53) – Used to resolve suspicious domain names (yummyrecipesforme.com and greatrecipesforme.com) to fake IP addresses (203.0.113.22 and 192.0.2.17). 2. HTTP (Hypertext Transfer Protocol, TCP/80) – Used for unencrypted communication with the suspicious domains, including GET requests and sustained data transfers. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| * What happened?   + A machine on the network made DNS queries to two unusual domains (yummyrecipesforme.com and greatrecipesforme.com).   + The domains resolved to reserved/test IPs (not real websites), a strong sign of malicious activity.   + After DNS resolution, the machine established HTTP connections (port 80) and exchanged data, including GET requests.   + High volumes of traffic were observed, suggesting possible data exfiltration or malware communication. * Why is this suspicious?   + The IPs (203.0.113.22, 192.0.2.17) are fake (RFC 5737 test ranges).   + The domain names mimic recipe sites (common in phishing/malware).   + Traffic was unencrypted (HTTP), making it easier for attackers to intercept. * How was it detected?   + Multiple customers emailed to website helpdesk. * Possible causes:   + Malware infection (e.g., spyware, ransomware, or botnet communication).   + Phishing attempt (user clicked a malicious link). |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Implement Rate Limiting on Authentication Attempts   * Action: Configure firewalls or security systems (e.g., fail2ban, IPS) to block IPs after multiple failed login attempts. * Why? Prevents automated brute force attacks by slowing down or stopping repeated password guesses. |