# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| 14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?  yummyrecipesforme.com. (24)  14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A  203.0.113.22 (40) |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Incident: Suspected brute force attack on [Affected System/Service] detected around 16:30-16:45 BST, April 30, 2025.  Activity: High volume of failed login attempts from [Source IP(s) or distributed].  Detection: tcpdump traffic file log analysis.  Impact (Preliminary): Potential resource exhaustion (DoS risk), unauthorised access risk, and temporary unauthorised account lockouts. No data compromise yet.  Immediate Actions: Alert verification, potential source IP blocking, rate limiting review, account lockout review, and log analysis ongoing.  Conclusion: Ongoing threat requires strengthened controls and monitoring. Further investigation is underway. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Recommendations: Enforce strong passwords, implement MFA, review lockout policies, use CAPTCHA, employ IP blocking/rate limiting, enhance monitoring/alerting, and provide user security training. |