# Title: Triage Simulation Table

**Prepared by:** Mayuri Sawle
**Date:** 25 Nov 2025

## A. Triage Simulation Table

| Column | Data Entry | Notes |
|---|---|---|
| **Alert ID** | 002 | Mock Alert ID |
| **Description** | Brute-force SSH Attempts | Indicates an attack targeting the SSH service |
| **Source IP** | 192.168.1.100 | Mock attacker IP address |
| **Priority** | Medium | SSH brute-force is typically medium unless targeting a critical server |
| **Status** | Open / Assigned | Triage has started and the case is assigned for further analysis |
| **MITRE Technique** | T1110 (Brute Force) | Classification as per MITRE ATT&CK framework |

**OTX Summary (50 words)**

AlienVault OTX returned no reputation data for the provided IP, as it belongs to a private address range. No pulses, threat associations, or malicious indicators were linked to it. The alert likely represents internal testing or benign activity rather than an external threat, requiring continued monitoring but not escalation.