**Kịch bản triển khai**

**1. Kịch bản dò mật khẩu ứng dụng Web (Brute Force)**

* **Mô tả**: Attacker (Kali) sử dụng Hydra để tấn công brute-force vào trang login của Web Server.
* Snort: Rule theo dõi POST nhiều lần → cảnh báo/dropping.
* *Mục tiêu*: Phát hiện và chặn tấn công brute-force.

**2. Kịch bản SQL Injection vào Web Server**

* **Mô tả**: Kali gửi payload độc qua form nhập trên Web Server.
* Snort: Rule phát hiện chuỗi SQLi (' OR ‘1’=’1--, v.v...).
* *Mục tiêu*: Kiểm tra khả năng IDS/IPS tầng ứng dụng.

**3. Kịch bản tải mã độc từ Web Server (Malware Download)**

* **Mô tả**: Web Server bị chiếm quyền, chèn liên kết tải .exe độc hại cho Client 1.
* Anti-Virus: Quét nội dung tải về.
* Squid: Ghi log URL và file tải về.
* *Mục tiêu*: Kiểm tra hiệu quả AV + Proxy khi lọc malware.

**4. Kịch bản scan hệ thống từ Attacker**

* **Mô tả**: Kali dùng nmap scan Client 1/Web Server/LDAP.
* Snort: Rule phát hiện scan+
* *Mục tiêu*: Phát hiện các hành vi reconnaissance.

**5. Kịch bản traffic bất thường (Anomaly Detection)**

* **Mô tả**: Kali tạo lượng lớn traffic lạ hoặc độ trễ bất thường (Slowloris, DoS...).
* Snort: Rule cho DoS/Slow HTTP.
* *Mục tiêu*: Phát hiện hành vi tấn công mạng tầng transport.