# Assignment No. 3

*Title: Snort IDS Installation, Configuration, and Attack Detection*

## Instructions

1. **Plagiarism is strictly prohibited**. You are expected to do this assignment yourself to understand both the attacker and defender perspectives
2. Expect a **live demo** of this assignment.
3. **Do not** present someone else's work; **originality is key.**
4. **Report**: PDF format with detailed explanations and screenshots containg a sticky note with your registration number.
5. **Rule Files**: Submit the custom Snort rule files you created.
6. Rule file should be named as **i22-XXXX_rules.txt**
7. Report should be named as **i22-XXXX_Report.pdf**
8. Follow the name and extension format or your assignment will **not be marked. (STRICTLY APPLIED)**

## Setup Guidelines :

1. Virtual Machines Setup:
    - You are required to build two virtual machines
    - **VM 1 (Ubuntu)**: Install and configure Snort.
    - **VM 2 (Kali Linux)**: Use this as the attacker machine to generate different attack scenarios.
2. Snort Installation:
    - Install snort on the Ubuntu VM.
    - Verify that Snort is configured correctly by running basic commands to detect network traffic
3. Kali Linux Attack Simulation:
    - Use Kali Linux to simulate various network attacks, targeting the Ubuntu VM running Snort.
    - Capture and analyze Snort's detection of these attacks using custom rule sets.

## Assignment Part No. 1: Snort Setup

- Task: Install and configure Snort on your Ubuntu VM.
- Expected Output: Snort runs in IDS mode and captures basic network traffic.

## Assignment Part No. 2: Custom Rules & Attack Scenarios

For each of the following attack scenarios, write and apply custom Snort rules. Then, generate the traffic using your Kali Linux VM and verify that Snort detects the attack.

1. **DDoS/DoS Attack on the Web Server**:
   - **Expected Output**: Snort should generate an alert when excessive traffic targets the web server.
2. **SQL Injection on a Web Application**:
   - **Expected Output**: Snort should alert on suspicious SQL injection attempts.
3. **Port Scanning and Information Gathering**:
   - **Expected Output**: Snort should detect the port scan activity and generate an alert for multiple connection attempts on different ports.
4. **Man-in-the-Middle (MITM) Attack**:
   - **Expected Output**: Snort should alert on suspicious ARP spoofing traffic or other abnormal network activity.
5. **Brute Force Login Attempts**:
   - **Expected Output**: Snort should detect multiple failed login attempts within a short period and generate an alert.
6. **Crafted Malicious Traffic**:
   - **Expected Output**: Snort should detect malformed or suspicious packets and generate an alert.
7. **Research-Based Custom Rule**:
   - **Simulate**: Research an additional attack that could be relevant to your network.
   - **Expected Output**: Snort should detect the chosen attack and log it appropriately.

## Deliverables

A report documenting the following:

1. Snort installation steps and confirmation of successful configuration.
2. Custom Snort rules for each attack scenario.
3. For each scenario:
   a. The Snort alert generated in response to the attack.
   b. Screenshots showing the attack from your attacker VM and the corresponding alert from Snort.
4. Reflection on the effectiveness of Snort in detecting these attacks.

**GOOD LUCK ☺**