Network Defense (Suricata)

1. Objective

The objective of this practical is to configure **Suricata** to detect and block malicious network traffic and map the alert to the MITRE ATT&CK framework.

2. Tool Used

- Suricata IDS/IPS
- Linux VM

3. Rule Creation

A custom Suricata rule was created to block traffic from a known malicious IP address.

```
drop ip 192.168.1.100 any -> any any (msg:"Block Malicious IP"; sid:1000001;)
```

This rule immediately drops packets originating from the specified.

4. Testing and Validation

Traffic was generated from the malicious IP to test the rule. The traffic was successfully blocked, and alerts were generated by Suricata.

Verification

- Network traffic from attacker VM was dropped
- Suricata logs confirmed rule activation

5. MITRE ATT&CK Mapping

Alert Description	Technique
Blocked malicious traffic	**T1071 – Command and Control**

6. Conclusion

This task demonstrated how network-level defenses can prevent command-and-control communication, reducing the impact of active threats.

7. Screenshots