Report: Network Security Fundamentals Implementation

1. Firewall Rule Implementation

- **Objective**: Block unauthorized access to a server while allowing HTTPS traffic.
- **Firewall Rule**:
    1. **Action**: Allow
    2. **Protocol**: TCP
    3. **Port**: 443 (HTTPS)
    4. **Source IP**: Any
    5. **Destination IP**: `192.168.1.10` (Internal Server)
    6. **Description**: Allow secure web traffic to the internal web server.
    7. **Default Rule**: Block all other incoming traffic.
- **Implementation Steps**:
    1. Access the firewall management interface.
    2. Add a rule in the "Inbound Traffic" section with the above specifications.
    3. Test by accessing the server using HTTPS and attempting connections on blocked ports.

---

2. IDS Configuration

- **Objective**: Detect suspicious login attempts to the server.
- **Tool Used**: Snort (open-source IDS).
- **Rule**: Monitor failed SSH login attempts.

- ```
  alert tcp any any -> 192.168.1.10 22 (msg:"SSH Brute Force Attempt"; detection_filter:track by_src, count 5, seconds 60; sid:1000001; rev:1;)
  ```
    1. **Explanation**:
        - **Source**: Any (any external IP).
        - **Destination**: `192.168.1.10`, port 22 (SSH).
        - **Trigger Condition**: 5 failed login attempts within 60 seconds.
        - **Action**: Log the event and generate an alert.
- **Implementation Steps**:
    1. Install Snort and configure the network interface for monitoring.
    2. Add the rule to the Snort configuration file.
    3. Start Snort in detection mode and monitor logs for alerts.
  ```

---

3. IPS Configuration

- **Objective**: Block traffic from sources performing suspicious activities like port scanning.
- **Tool Used**: Suricata (open-source IDS/IPS).
- **Rule**: Drop traffic identified as a port scan.

- `drop tcp any any -> any any (msg:"Potential Port Scan Detected"; detection_filter:track by_src, count 20, seconds 10; sid:1000002; rev:1;)`
    1. **Explanation**:
        - **Source/Destination**: Any.
        - **Trigger Condition**: More than 20 connection attempts within 10 seconds from a single source.
        - **Action**: Drop the packets and log the event.
- **Implementation Steps**:
    1. Install and configure Suricata.
    2. Add the rule to the Suricata rule set.
    3. Restart the service and enable inline mode to block suspicious traffic.

---

4. Example of Detected Event

- **Scenario**:
    - An external IP (`203.0.113.45`) performed a port scan on the internal network.
- **Detected Event Log (from Suricata)**:

- `Timestamp: 2024-12-02T10:15:23Z Alert: Potential Port Scan Detected Source IP:203.0.113.45 Destination IP: 192.168.1.10 Action: Dropped Rule SID: 1000002`
- **Action Taken**:
    - The IPS blocked further traffic from the source.
    - Security team investigated and identified the activity as malicious. Source IP was added to a blacklist.