

```
-- database_setup.sql

-- PostgreSQL database schema for Network Traffic Analyzer

-- Create database (run as superuser)

-- CREATE DATABASE network_analyzer;

-- Connect to the network_analyzer database and run the following:
```

```
-- Table for storing packet metadata
```

```
CREATE TABLE packets (
    id SERIAL PRIMARY KEY,
    timestamp TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    source_ip INET NOT NULL,
    destination_ip INET NOT NULL,
    source_port INTEGER,
    destination_port INTEGER,
    protocol VARCHAR(10) NOT NULL,
    packet_size INTEGER,
    tcp_flags VARCHAR(20),
    node_id VARCHAR(50) NOT NULL,
    raw_data TEXT
);
```

```
-- Table for storing security alerts
```

```
CREATE TABLE alerts (
    id SERIAL PRIMARY KEY,
```

```
timestamp TIMESTAMP DEFAULT CURRENT_TIMESTAMP,  
alert_type VARCHAR(50) NOT NULL,  
source_ip INET NOT NULL,  
destination_ip INET,  
severity INTEGER NOT NULL DEFAULT 1,  
description TEXT NOT NULL,  
node_id VARCHAR(50) NOT NULL,  
count INTEGER DEFAULT 1,  
resolved BOOLEAN DEFAULT FALSE  
);
```

-- Table for attack signatures (for future pattern matching)

```
CREATE TABLE attack_signatures (  
    id SERIAL PRIMARY KEY,  
    signature_name VARCHAR(100) NOT NULL,  
    pattern TEXT NOT NULL,  
    severity INTEGER DEFAULT 1,  
    enabled BOOLEAN DEFAULT TRUE,  
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP  
);
```

-- Indexes for performance optimization

```
CREATE INDEX idx_packets_timestamp ON packets(timestamp);  
CREATE INDEX idx_packets_source_ip ON packets(source_ip);  
CREATE INDEX idx_packets_dest_ip ON packets(destination_ip);  
CREATE INDEX idx_packets_protocol ON packets(protocol);
```

```
CREATE INDEX idx_packets_node_id ON packets(node_id);
```

```
CREATE INDEX idx_alerts_timestamp ON alerts(timestamp);
```

```
CREATE INDEX idx_alerts_type ON alerts(alert_type);
```

```
CREATE INDEX idx_alerts_source_ip ON alerts(source_ip);
```

```
CREATE INDEX idx_alerts_severity ON alerts(severity);
```

```
CREATE INDEX idx_alerts_resolved ON alerts(resolved);
```

```
-- Insert some sample attack signatures
```

```
INSERT INTO attack_signatures (signature_name, pattern, severity) VALUES
```

```
('Port Scan Detection', 'Multiple connection attempts to different ports', 3),
```

```
('SYN Flood Attack', 'High volume of TCP SYN packets from single source', 4),
```

```
('Brute Force Attack', 'Repeated connection attempts to same service', 3),
```

```
('ARP Spoofing', 'Inconsistent IP-MAC address mappings', 2);
```