IOT

(INTERNET OF THINGS)

Module 18 IOT and OT

1 what is IOT and OT /How the IOT works

2 Explain IOT Architecture

- Perception (Device/Sensing) Layer
- Network/Transport Layer
- Edge/Fog or Middleware Layer
- Data Processing & Analytics Layer (Cloud or Middleware)
- Application/Business/User Layer
- Cross-Cutting Security & Management

3 Explain IOT Operating Systems

4 Types of IOT Protocol

Task1 how to perfrome Rolling cabe attack

Task2 Types of IOT and OT Attacks

- Botnets / DDoS
- Man-in-the-Middle (MitM)
- Eavesdropping / Data Breach
- Firmware Manipulation & Zero-Day
- Physical Tampering & Side-Channel
- Device Spoofing / Credential Attacks

OT (Operational Technology) Attacks

- Malware in ICS/SCADA
- Supply-Chain & Third-Party Exploits
- Ransomware & Disruption
- Physical/Sabotage Access
- Network Intrusion & Data Manipulation

1 what is IOT and OT /How the IOT works

IOT (Internet of Things)

The Internet of Things refers to a network of **actual physical "things"**—from wearables, appliances, vehicles to large industrial machines—each embedded with sensors, software, and connectivity. These devices collect, exchange, and act on data, often without human intervention.

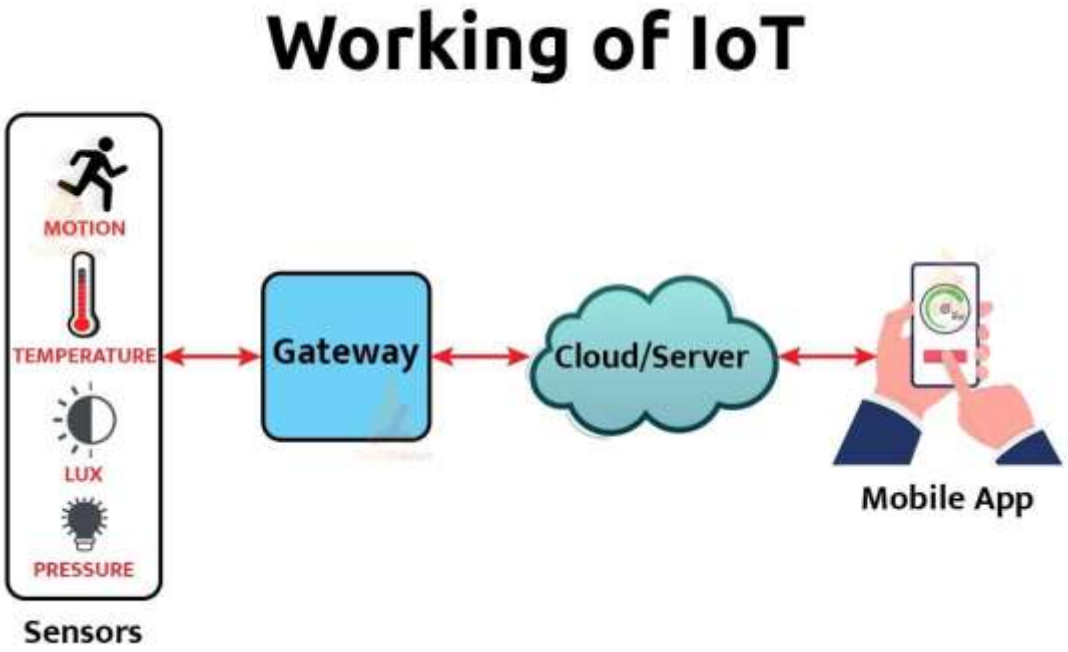
- **Purpose**: Seamless data-driven automation and insights.
- **Scope**: Ranges from smart home gadgets like thermostats and cameras to industrial sensors and city-wide systems .

OT (Operational Technology)?

- Operational Technology refers to hardware and software that **directly monitor and control physical processes**. This includes systems like PLCs, SCADA, DCS, RTUs—used across manufacturing, utilities, transportation, and infrastructure

Key characteristic: Operates in real-world environments to manage machinery, safety systems, and building automation

⚙ How Does IoT Work?



A typical IoT system consists of:

1. **Devices with sensors/actuators** – these collect data from environments or perform actions (e.g., temperature sensors, motion detectors).

2. **Connectivity –** devices send data through Wi-Fi, Bluetooth, cellular, LoRa, NB-IoT, or Ethernet to gateways or the cloud .

3. **Data processing** – either in the cloud or at network edges (like gateways); includes running analytics or AI, and taking decisions .

4. **User interface –** dashboards, mobile apps, or alerts present insights and allow interaction with devices

2 Explain IOT Architecture

Perception (Device/Sensing) Layer 🌱

- What it is: The "physical world" interface—sensors (e.g. temperature, humidity, cameras) gather data; actuators (e.g. motors, relays) perform actions based on commands. Devices include microcontrollers like Arduino, ESP32, Raspberry Pi

Network/Transport Layer

- Responsibility: Delivers data between devices and central systems using communication links.

- **Technologies**: Wi-Fi, Bluetooth/BLE, ZigBee, LoRaWAN, cellular (4G/5G, NB-IoT), Ethernet, NFC, MQTT, CoAP, DDS, AMQP depending on use-case

Edge/Fog or Middleware Layer

- **Pre-processing location**: Closer to data sources (like gateways or edge devices) to reduce latency.
- **Tasks**: Filter raw data, perform immediate analytics, protocol conversion, caching, and security—only relevant data gets sent to the cloud

Data Processing & Analytics Layer (Cloud or Middleware)

- **Core functions**:
  - Receive, store, and manage incoming data streams (e.g., in data lakes or time-series databases)

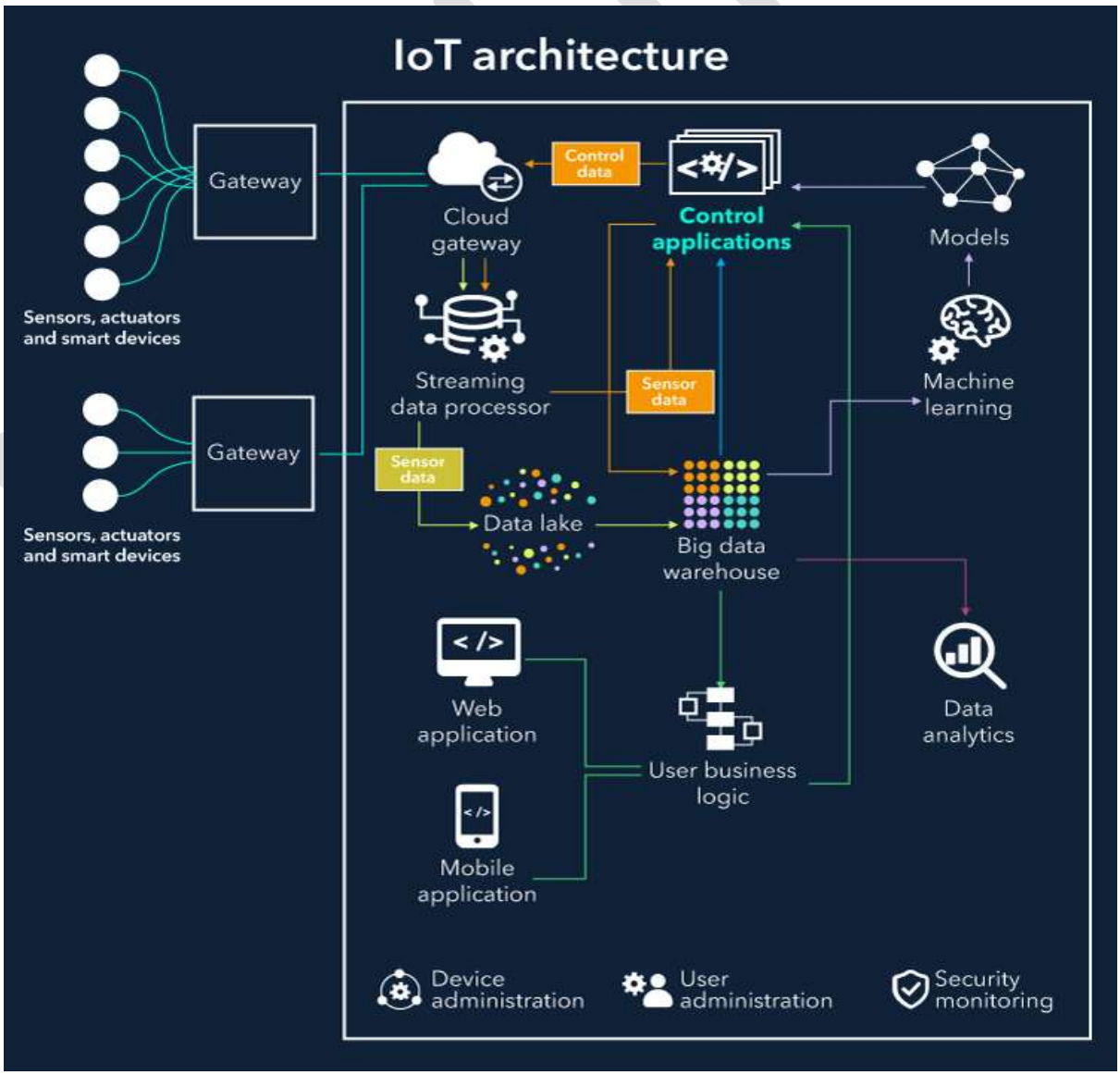
Application/Business/User Layer

- **What it delivers**: End-user interfaces—web/mobile dashboards, enterprise apps, APIs for domain-

specific use cases (smart home, health, industrial automation, smart cities) .

Cross-Cutting Security & Management

- **Scope**: Spans all layers to ensure integrity, confidentiality, and trustworthy device operation.
- **Capabilities**: Access control, encryption, firmware updates, authentication, monitoring



3 Explain IOT Operating Systems

⚙ 1. RIOT

A microkernel-based OS for deeply constrained devices.

- **Highlights**: Multi-threading, network protocols (IPv6, 6LoWPAN, CoAP), tiny footprint (1.5 KB RAM minimum) .
- **Use cases**: Sensor networks, mesh systems, smart metering, research.

2 .Tizen & Windows

Tizen – Linux-based, backed by Samsung/Linux Foundation, modular, supports HTML5/C/C++, BLE/Wi-Fi/Matter.
Windows IoT – Comes in "Core" (for Raspberry Pi) and "Enterprise" versions (industrial PCs); good for signage, kiosks, embedded x86/ARM systems .

3 Ubuntu Core & Linux

Ubuntu Core – A minimal, secure OS using Snap packages, built for OTA updates, containerization, ARM/x86 platforms .
General Linux – Full-featured distributions like Debian or Raspbian are also common in larger-scale IoT devices.

4. Arm Mbed OS

Designed specifically for ARM Cortex-M microcontrollers.

- **Highlights**: Lightweight RTOS, supports cloud integration (AWS, Azure), secure boot, OTA updates, drivers and connectivity stacks

Use cases: Commercial IoT products, prototypes scaling to production

5 Huawei LiteOS

A lightweight RTOS from Huawei (now evolved into HarmonyOS/OpenHarmony).

- **Highlights**: Very tiny (~10 KB), zero config, supports LTE, NB-IoT, Wi-Fi, 6LoWPAN; POSIX compliant

4 Types of IOT and OT Protocol

IoT Protocols

Network & Connectivity

- Wi-Fi (802.11)
- Bluetooth / BLE
- Zigbee
- Z-Wave

- LoRa / LoRaWAN
- NB-IoT / LTE-M
- 6LoWPAN
- NFC
- Cellular (2G/3G/4G/5G)

Transport

- TCP/IP
- UDP

Messaging & Application

- MQTT
- CoAP
- AMQP
- DDS
- XMPP
- HTTP / HTTPS
- WebSocket
- LwM2M
- SensorThings API
- OPC UA
- SMS / SMPP
- USSD
- SSI (Simple Sensor

🏭 OT (Operational Technology) / Industrial Protocols

Field / Process Automation

- Modbus (RTU, ASCII, TCP)
- HART
- Profibus
- PROFINET
- EtherNet/IP
- EtherCAT
- CC-Link
- DeviceNet
- ControlNet
- FOUNDATION Fieldbus
- AS-i
- CANopen
- BACnet
- DNP3

Task1 how to perfrome Rolling code attack

A Rolling Code Attack is a technique used by attackers to break into cars, garages, or other devices that use wireless key fobs with rolling codes (also called hopping codes). Rolling codes are designed to prevent simple

replay attacks by changing the code every time the button is pressed. However, attackers can still exploit this system using special devices.

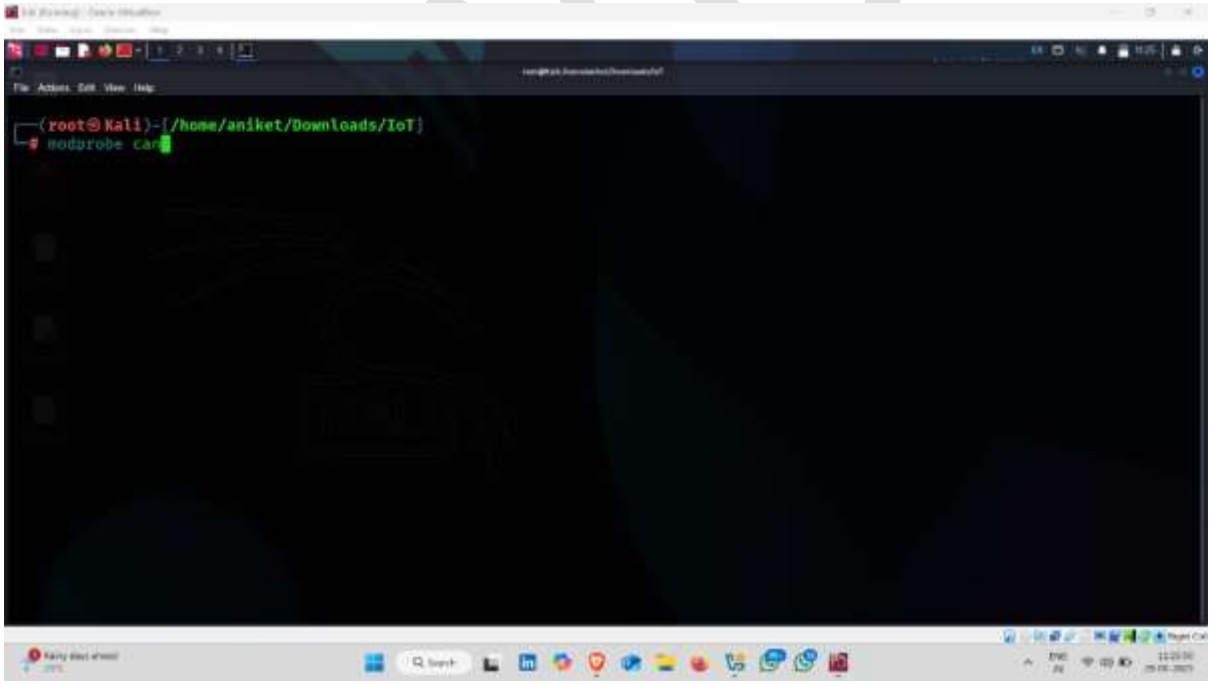
Step1 : start the kali Linux open the terminal type the commands:

apt-get install Can_utils

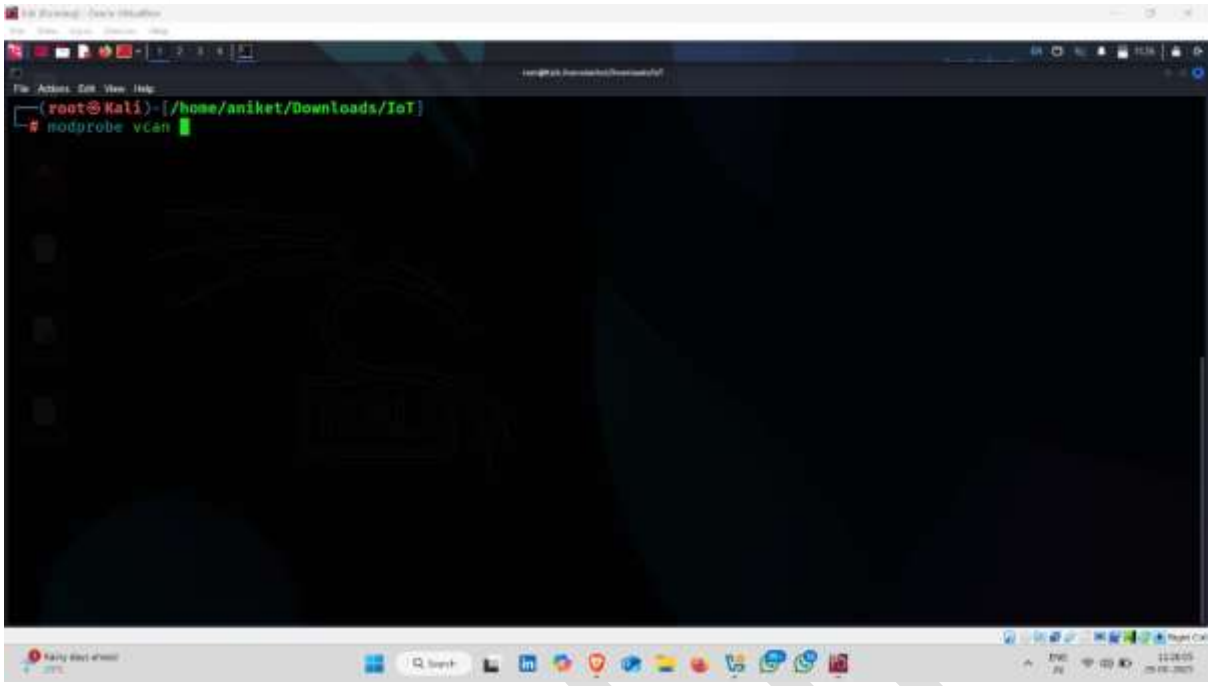
Download the this tool

Step2 : sudo modprobe can

This command are use virual invorment command

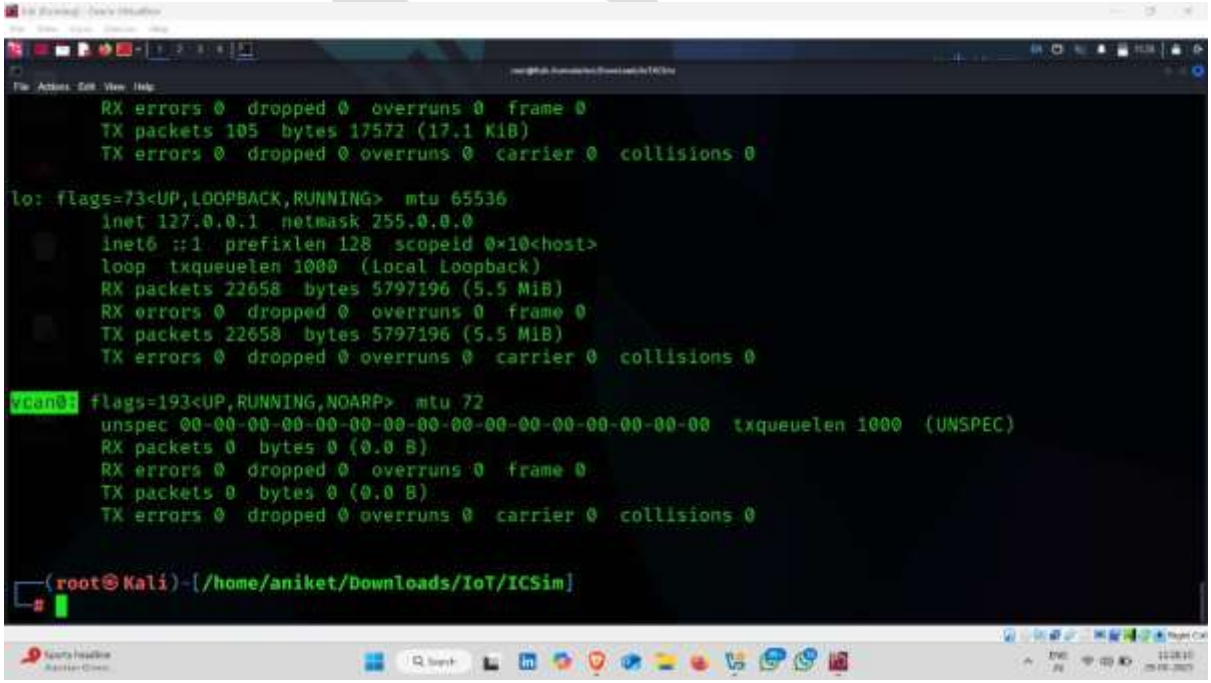


Step3 : sudo modeprobe vcan

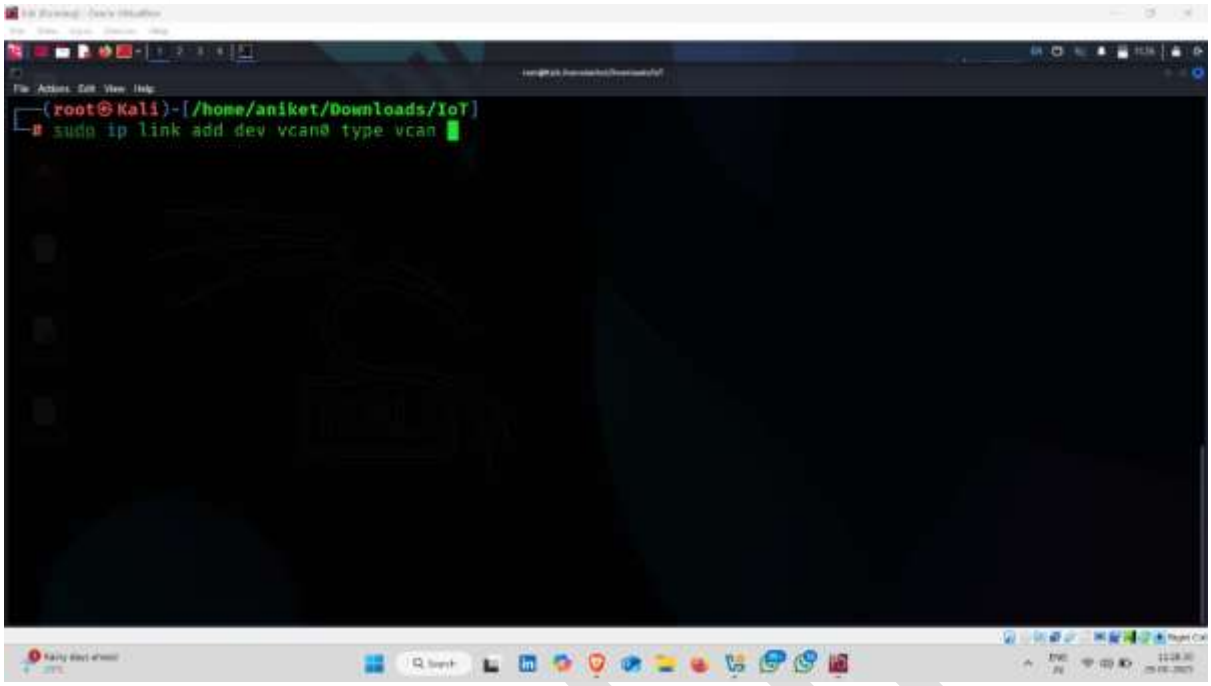


Step4: ifconfig

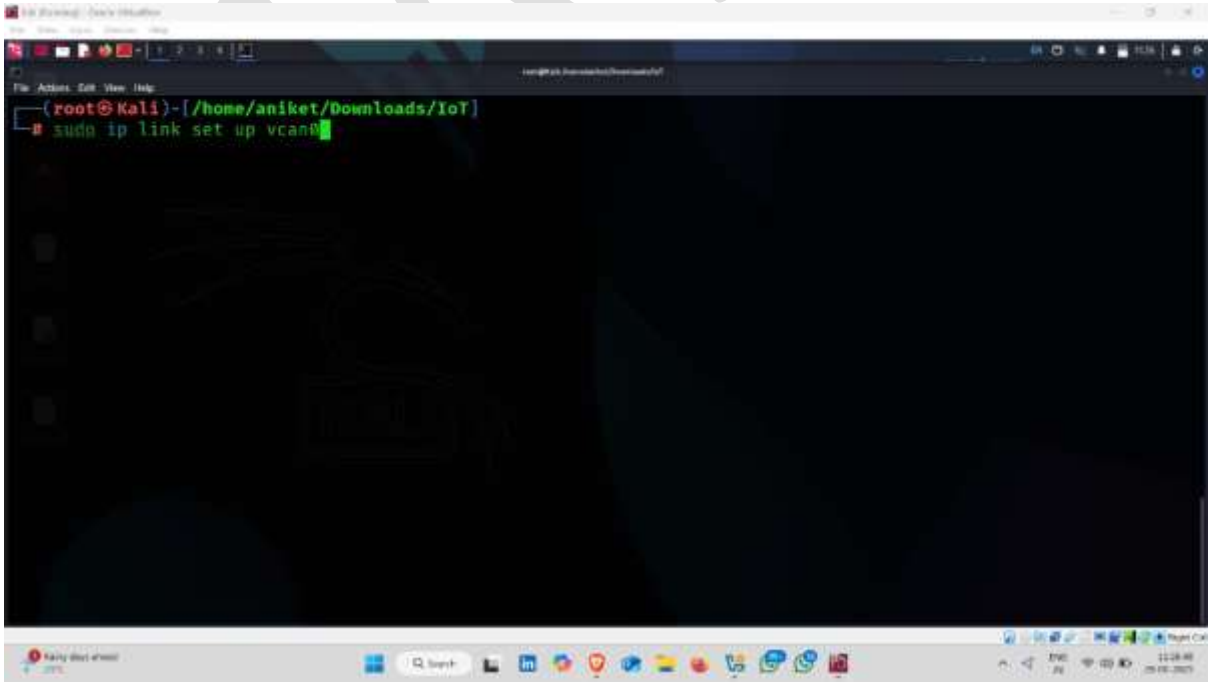
This command are use check vitual invorment ready



Step5: sudo ip link add dev vcan0 type vcan



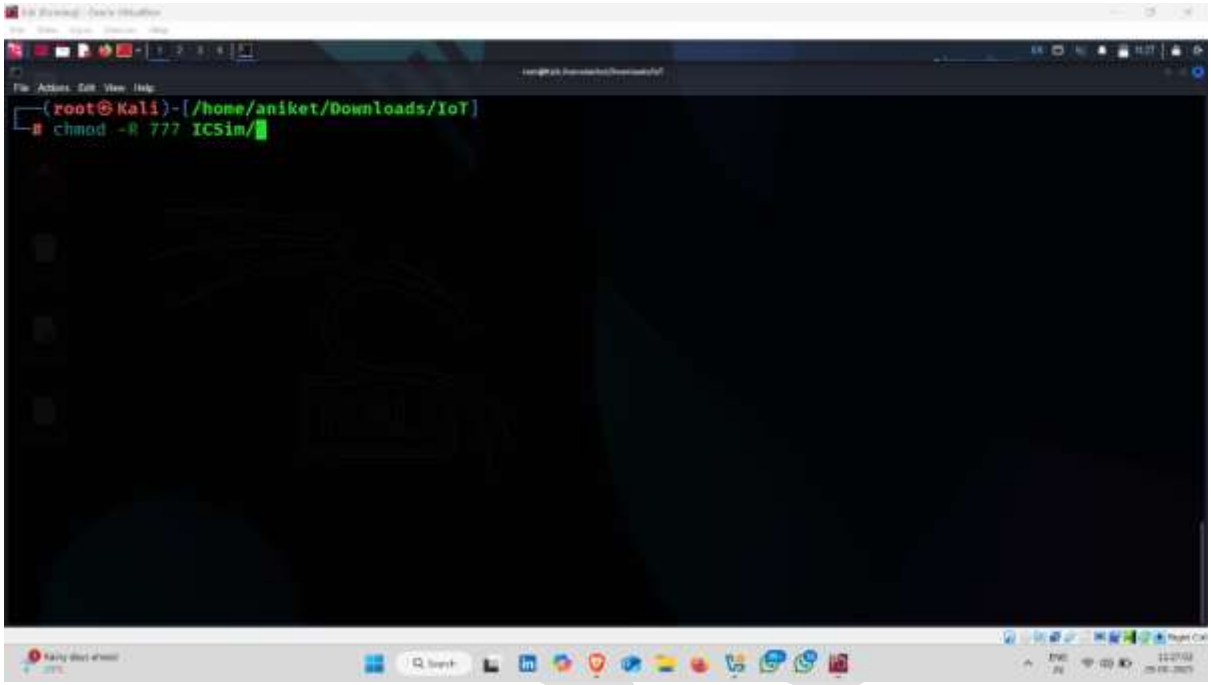
Step6: sudo ip link set up



Step7: download the gitthub ICSim tool

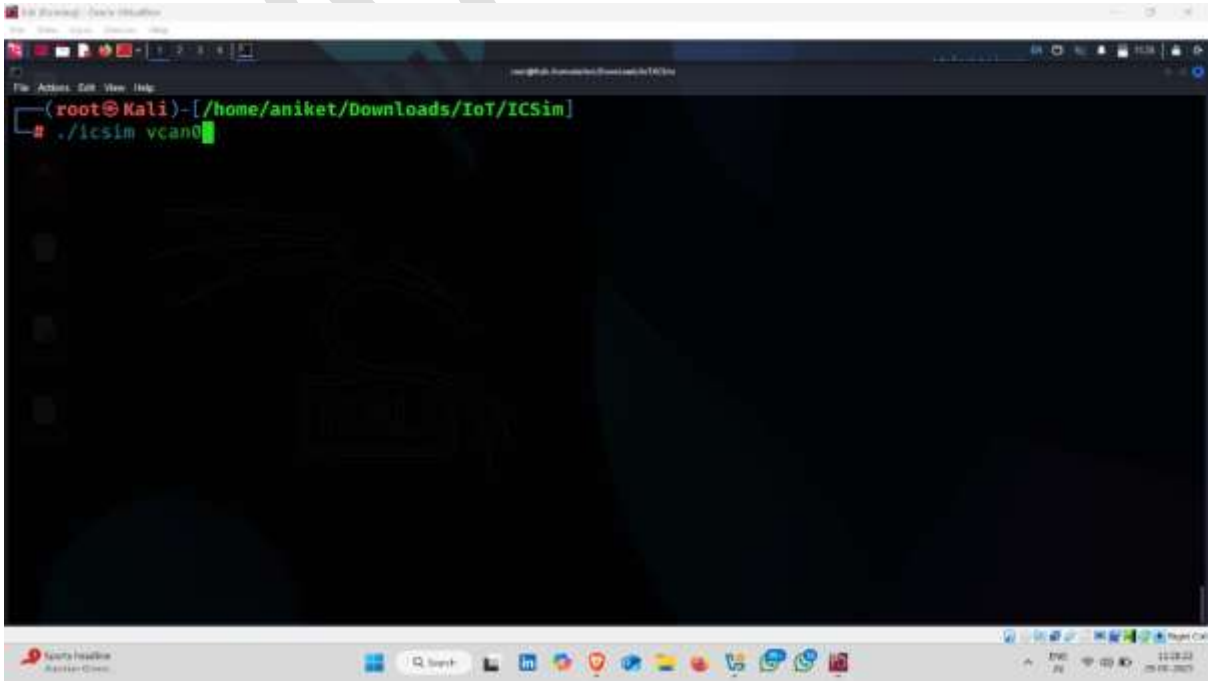
Step8: chmod –R 777 Icsim

This command are use to enable to permission

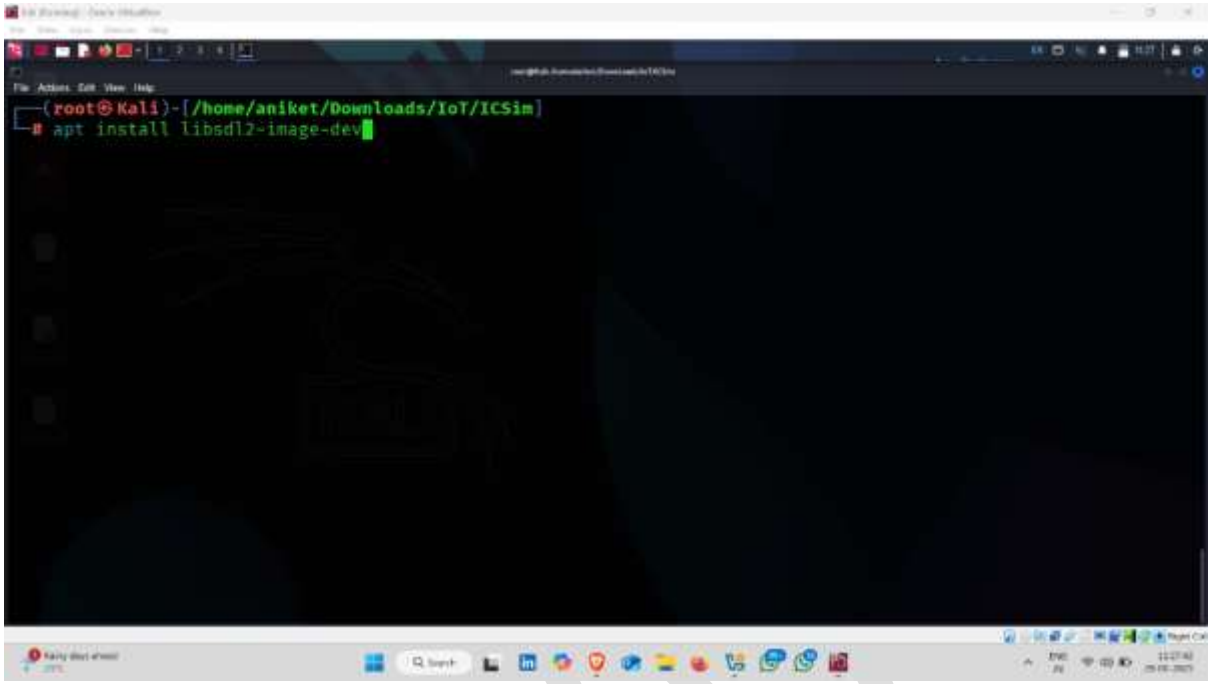


Step9: cd ICSim

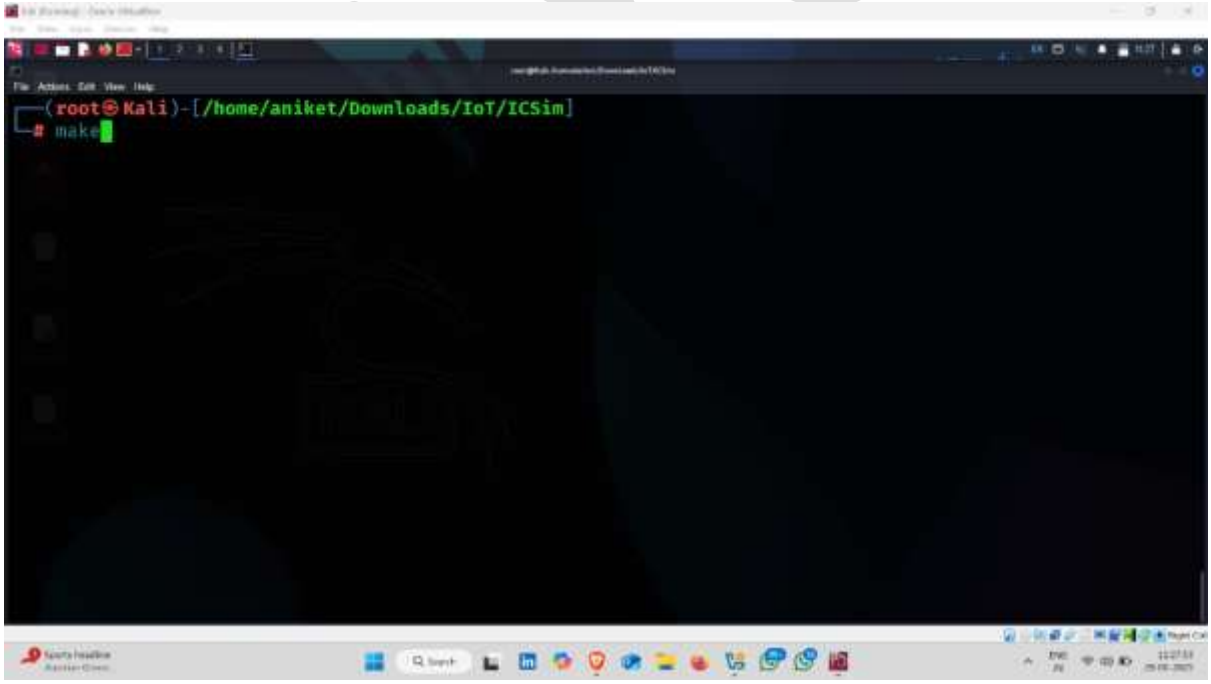
This command are use to go to directory of Icsim



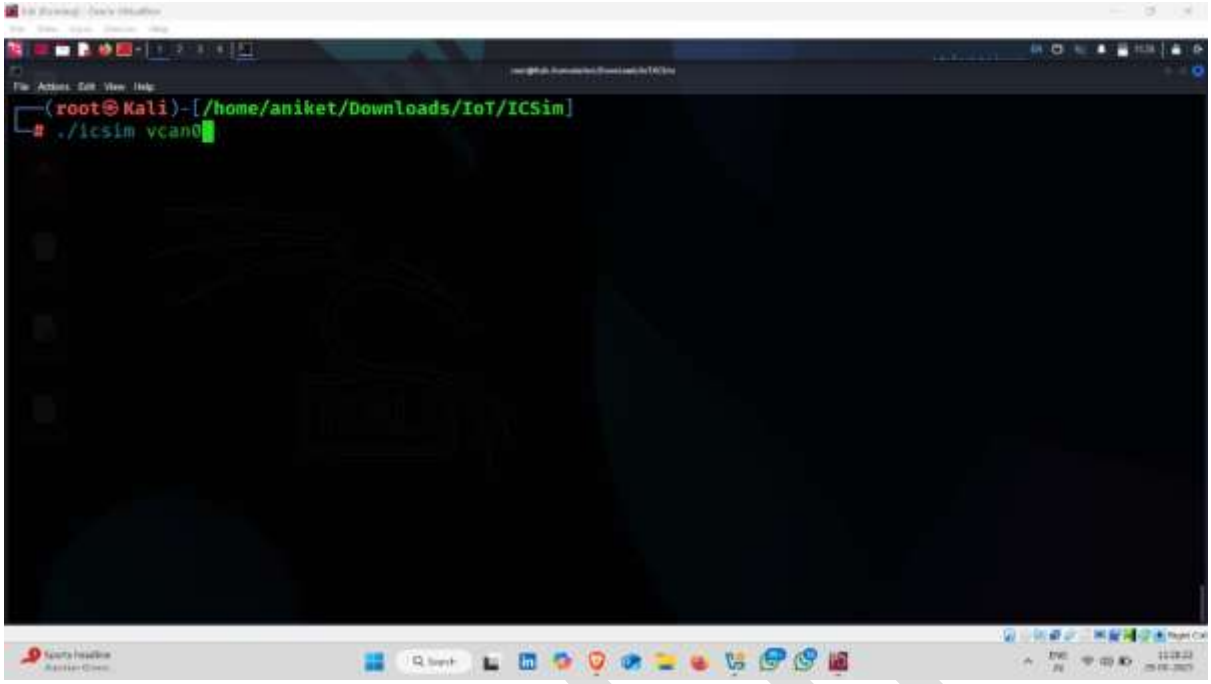
Step10: apt install libsdl2=image-dev



Step11 make

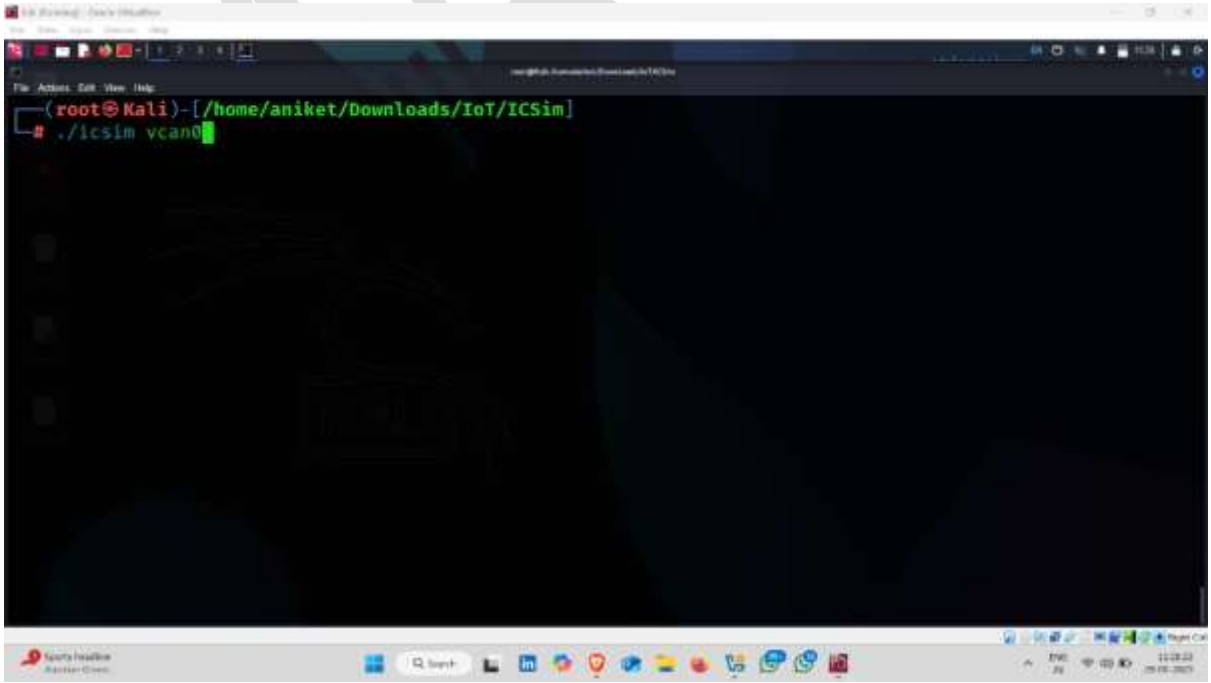


Step 12 ./ icsim vcan0



Step13 open the next terminal open go to Iscim directory

Step14: ./ controls vcan0

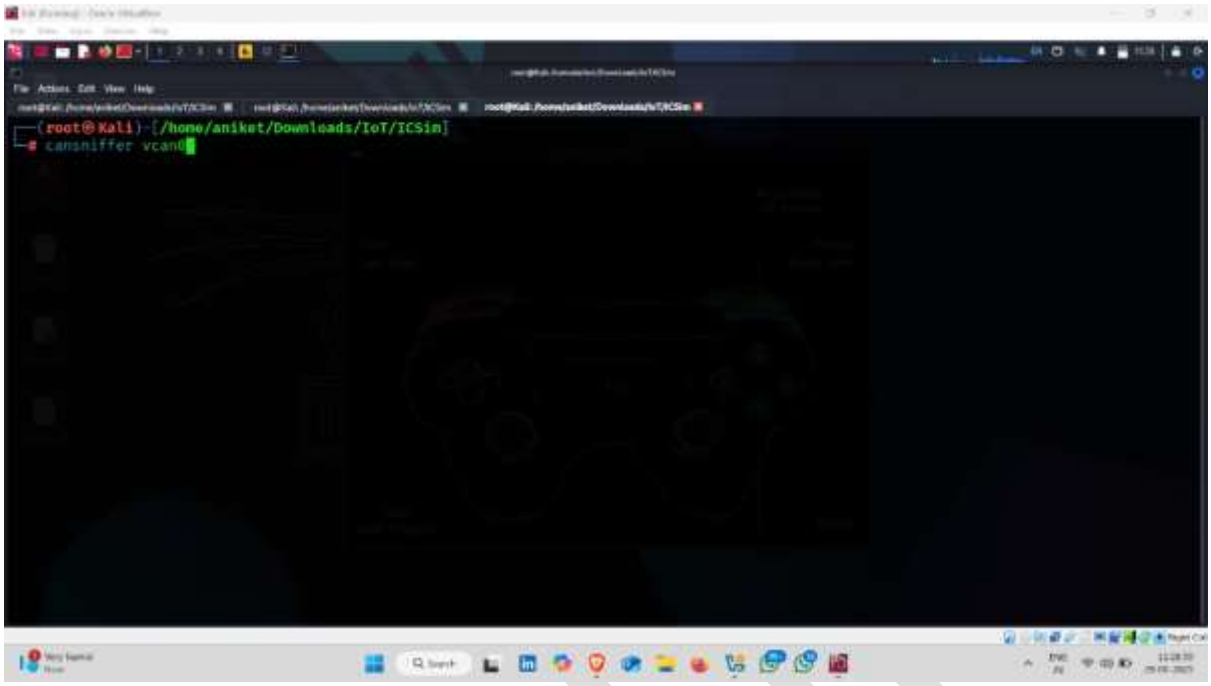


Step15 open next terminal /sniiffeg cpatute

Go to Icsim

Command: cd ICSIM

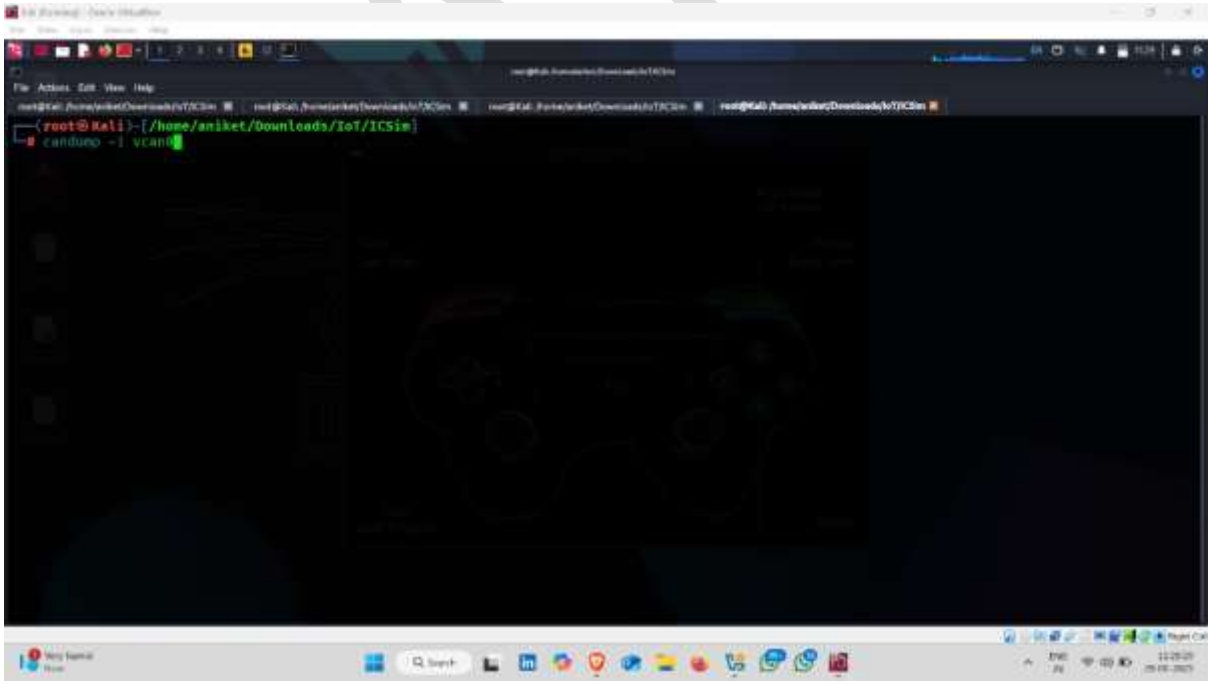
Step16: can sniffer vcan0



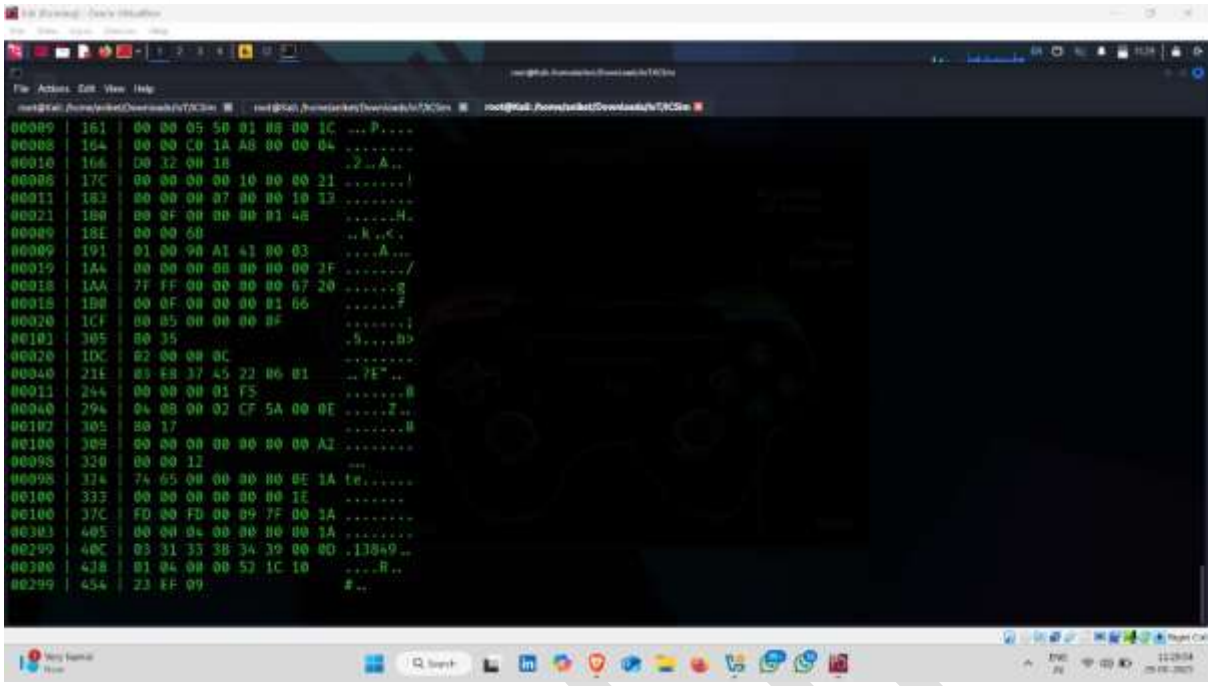
Step17 open the next terminal

Command: candump –I vcan0

This command are use to log maintain



Result:



Types of IOT and OT Attacks

1. **Botnets / DDoS**
   Compromised IoT devices (like cameras, routers) form a botnet to flood targets with traffic, knocking services offline. The Mirai malware famously used this tactic to take down Dyn in 2016.

2. **Man-in-the-Middle (MitM)**
   Attackers intercept and possibly alter communications between IoT devices and servers,

enabling data theft or command injection. Common when network security is weak **Eavesdropping / Data Breach**
Passive interception of sensitive data—like video, audio, personal info—transmitted from IoT devices. Prevalent in smart-home devices with unencrypted channels

3. **Firmware Manipulation & Zero-Day**
   Attackers exploit unknown vulnerabilities or push malicious firmware updates, gaining control at the hardware level. These exploits are stealthy and difficult to defend against.
4. **Physical Tampering & Side-Channel**
   Direct interaction with devices (ports, circuit boards) to extract data or inject malware; side-channel techniques use power or electromagnetic leaks to glean secrets .

5. **Device Spoofing / Credential Attacks**
   Fake devices impersonate legitimate ones using stolen IP/MAC addresses or weak default credentials, gaining unauthorized network access .

⚙ OT (Operational Technology) Attacks

1. **Malware in ICS/SCADA**
   Specialized malware targets industrial control systems—Stuxnet in 2010 disrupted Iran's centrifuges, showing malware can physically damage equipment.

2. **Supply-Chain & Third-Party Exploits**
   Attackers compromise vendors or software components to introduce vulnerabilities into OT infrastructure—these often go unnoticed until disaster strikes .

3. **Ransomware & Disruption**
   OT environments are hit by ransomware that locks out controllers or halts processes—this can shut down production lines or utilities until ransom is paid .

4. **Physical/Sabotage Access**
   Intrusions at substations or control rooms allow direct manipulation or sabotage of hardware and physical processes—seen in attacks like Ukraine's 2015 power outag.

5. **Network Intrusion & Data Manipulation**
   Using IT-OT convergence, attackers infiltrate OT networks via exposed interfaces, then alter critical data or commands—manipulating system behavior with far-reaching effects