IoT Hacking :

1. **Application Layer** : Delivery of Various applications to different users in IoT
2. **Middleware Layer** : Device management and information management
3. **Internet Layer** : Connection between Endpoints
4. **Access Gateway Layer** : Protocol Translation and messaging
5. **Edge Technology Layer** : sensors, machines

AMIAE

Exploiting HVAC :

- Many Organizations uses internet connected heating, ventilation and air conditioning (HVAC) system without implementing security mechanism this gives attacker a gateway to hack corporate systems
- HVAC systems have many security vulnerability that are exploited by attackers to steal login credentials, gain access to the HVAC system , and perform further attacks on the organization's network.

Jamming Attack :

- Jamming is a type of attack in which the communication between wireless IoT devices are jammed so that they can be compromised
- An attacker transmit radio signal randomly with the same frequency as the sensor node for communication
- As a result, the network gets jammed, which disable the endpoints from sending or receiving any messages

SDR-Based Attacks on IoT :

- The attacker use software define radio (SDR) to examine the communication signal in the IoT network and sends spam content or text to the interconnected devices
- This software based radio system can also change the transmission and reception of signals between the devices based on their software implementation.

1. **Replay Attack :**
    1. The attacker obtain the specific frequency used for sharing information between connected device and captures the original data when the command is initiated by these device.
    2. the attacker segregates the command sequence and inject it into the IoT Device

2. **Cryptanalysis Attack :**
    1. The attacker uses the same procedure as that follow in the replay attack along with reverse engineering of the protocol to capture the original signal
    2. The attacker must be skilled at cryptography, communication theory, and modulation scheme to perform this attack

3. **Reconnaissance Attacks :**

What is OT ??

- Operational Technology (OT) is the software and hardware designed to detect or cause changes in industrial operation through direct monitoring and/or controlling of industrial physical device.
- OR Consist of Industrial Control system (ICS) that includes supervisory control and data acquistion (SCADA) , Remote Terminal Unit (RTU), Programable Logic Controller, Distributed Control System (DCS), etc to monitor and control the industrial operation.

Introduction to ICS :

- ICS is often referred to as a collection of different types of Control system and their associated equipment such as systems devices, network and controls used to operate and automate server industrial processes
- An ICS consists of several types of control systems like SCADA, DCS, BPCS, SIS, HMI, PLCs, RTU, IED etc
- The operation of ICS System can be configured in three modes, namely Open Loop, Closed Loops, and manual mode.

Distributed Control Systems (DCS) :

- DCS is a highly engineered and large scale control system that is often used to perform industry specific task.
- it contains a centralized supervisory control unit used to control multiple local controller
- it operates using a centralized supervisory control loop (SCADA, MTU etc) that connect a group of localized controller (RTU/PLC) to executes the overall task required for the working of an entire production process.

Supervisory Control and Data Acquisition (SCADA) :

- It is centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure
- It provides centralized controlling and monitoring of multiple process. input and outputs by integrating the data acquisition system with the data transmission system and Human machine interface (HMI) software.

The SCADA architecture comprises the following hardware .

1. Control Server (SCADA-MTU)
2. Communication devices (network cables, radio devices, telephone lines, cables)
3. Field Site distributed geographically consisting of PLCs, RTU, etc which are used to monitor control operation of industrial equipment.

Components of an ICS - Programmable Logic Controller (PLC)

A Programmable Logic Controller is a small solid-state control computer where instruction can be customized to perform a specific task.

PLC Consist of Three Modules :

1. **CPU Module** : it comprises of a central processor and its memory component
2. **Power Supply Module** : It provide a necessary supply of power required for the CPU and I/O modules by converting the power from AC to DC
3. **I/O Module** : Thses are used in connecting the censors and actuators with system for sensing and controlling the real-time values such as pressure, temp., and flow.

Modbus is a communications protocol published by Modicon in 1979 for use with its Programmable Logic Controllers (PLCs).
A device operating as a master will poll one or more devices operating as a slave

Hacking Modbus Slaves :

- Modbus Master and slaves communicate in plaintext, without an authentication
- Attacker can exploit this vulnerability to generate and send similar query packets to Modbus Slaves to access and manipulate the registers and coil of the slave.

metasploit :

```
scanner/scada/modbus_findunitid
scanner/scada/modbusclient
```