{Intrusion detection system}

An IDS is a security tool or software application designed to monitor network or system activities for malicious or unauthorized activities . The main purpose of an IDS is to detect and respond to potential security threats in real-time

Setting goals:

the types of activities
want to identify:
(hacking attacks)
(unauthorized use of the system)

Study system requirements:

Determine the basic requirements for the system, such as the language used and the tools needed.

C language and data structures:

*Master the basics of the C language : working with variables and functions.
*Understand and use data structures: linked lists.

Networks and Internet protocols:

*Understand how networks and data flow work
*Knowledge of Internet protocols :
TCP/IP and UDP.

Study networking libraries and tools:

Check out libraries and tools for analyzing and monitoring network traffic,Libpcap in Python or Wireshark

Database design:

Design a database containing information on monitoring and analysis activities.

Network traffic analysis:

He began analyzing network traffic using libraries Libpcap to read data packets.

Fundamental analysis application:

Build a prototype to analyzen basic activities using defined rules.

Integration of automated analysis techniques:

Rely on automated analysis techniques :
machine learning to improve detection accuracy.

Alert and Notice:

Implement an alert system that notifies the user when abnormal activity is detected

System testing:

Test the system using various scenarios to verify its effectiveness.