Ministry of Higher Education and Scientific Research, Iraq

University of Babylon

information technology collage

Information Security Department

SDN-Based Intrusion Detection Using Correlation Analysis

A Graduate Project Submitted to the Department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology

STUDENT'S NAME

Sumaya Mohammed Hamza

Supervised by

Dr. Suadad S. Mehdi

2023-2024

Abstract

Software Defined Networking (SDN) is a networking paradigm that separates network hardware (such as routers and switches) from the software that manages traffic flow. This enables network administrators to have centralized and flexible control through software interfaces, allowing for more efficient configuration of the network and better responsiveness to application needs, and it has many security problems.

The major security issue in Software Defined Networking (SDN) is Centralized Control Threats, where attacks targeting the central controller unit can lead to a loss of control over the entire network.

and Denial of Service (DoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic. Essentially, the attacker floods the target with an excessive amount of data, requests, or connections, causing it to become slow, unresponsive, or even completely inaccessible to legitimate users. This type of attack doesn't aim to breach security or steal data directly but rather to disrupt the availability of the targeted resource, There are many detection methods for this issue.

We will use Correlation analysis for detecting DoS attacks involves examining multiple network parameters to identify abnormal patterns that could indicate an ongoing attack. By correlating various metrics such as packet rates and traffic patterns, it helps distinguish between normal and malicious activities, enabling prompt response to mitigate the impact of the attack.

In this project, the approach was implemented using Python, Mininet emulator, POX controller, and SDN control plane.