وزارة التعليم العالي والبحث العلمي، العراق

جامعة بابل

كلية تكنولوجيا المعلومات

قسم امنية المعلومات

الدراسة: (الصباحية)

شبكة نظام كشف التسلل ومنع التسلل باستخدام أداة سنورت

Network intrusion detection system and intrusion prevention using Snort Tool

مشروع التخرج مقدم كجزء من متطلبات الحصول على درجة البكالوريوس في تخصص امنية المعلومات في تكنولوجيا المعلومات.

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

الطالب

زيد شفيق عبد الاله

بإشراف

م.م. أمير سمير حمود

2023-2024

Abstract

In the age of information, where each action results in data creation, the volume of digital content is skyrocketing. With over 300 thousand tweets and 4 million Facebook posts generated per minute, the demand for robust security measures has never been greater. This paper addresses the escalating concerns of security and reliability faced by individuals and organizations in the modern digital landscape.

The research delves into the intricacies of Intrusion Detection and Prevention Systems (IDPS), exploring various terminologies, techniques, and methodologies essential for safeguarding networks against unauthorized or malicious activities. A comprehensive analysis of the current state-of-the-art in IDPS is presented, drawing insights from a wide range of research endeavors.

Central to this study is the exploration of Snort, a leading open-source tool for network security, which has gained widespread acceptance in corporate sectors for enhancing organizational network security. The paper offers an in-depth understanding of Snort, covering its purpose, associated modes, implementation strategies, and practical applications.

Through a thorough review of existing literature and research studies, this paper synthesizes key findings, providing valuable perspectives on the effective implementation of IDPS based on the utilization of Snort. The insights derived from this research contribute to the advancement of network security practices, offering actionable recommendations for organizations and professionals striving to fortify their network defenses against evolving cyber threats.