# ABSTRAK


| | | |
|---|---|---|
| Judul | : | IMPLEMENTASI INTRUSION DETECTION AND PREVENTION SYSTEM DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI STUDI KASUS: POLITEKNIK XYZ |
| Nama | : | Yehovan Nugra Agave |
| Program Studi | : | Teknik Informatika |



Politeknik XYZ sebagai salah satu institusi pendidikan yang sangat mengandalkan jaringan komputer pada operasionalnya membutuhkan sebuah sistem keamanan jaringan yang dapat melindungi sistem jaringan komputer. Disamping itu diperlukan juga penilaian terhadap kesiapan Politeknik XYZ dalam penerapan sistem keamanan yang berguna untuk mengukur dan meningkatkan tingkat kesiapan keamanan jaringan komputer. Intrusion Detection and Prevention System (IDPS) sebagai salah satu sistem keamanan jaringan yang berfungsi sebagai sistem pendeteksi serangan dan sebagai sistem pencegahan serangan dalam jaringan komputer. Pada penelitian ini IDPS diimplementasikan dengan menggunakan *software* snort yang berjalan diatas sistem operasi pfSense dan menggunakan metode pengembangan Network Development Life Cycle (NDLC) pada proses implementasi jaringan komputer. Sebelum dan setelah implementasi dilakukan survei tingkat kesiapan keamanan yang berdasarkan Indeks KAMI (Keamanan Informasi) versi 4.2 yang berfungsi untuk mengukur tingkat kesiapan keamanan setelah implementasi IDPS. Penetration Testing dilakukan dengan simulasi serangan yang bersifat Denial of Services (DoS) dan Man in the Middle (MITM) untuk menguji sistem IDPS. Hasil yang didapat adalah IDPS dapat mendeteksi dan melakukan tindakan bloking terhadap serangan yang bersifat DoS seperti SSH Bruteforce, SYN Flood, dan UDP Flood, sedangkan serangan yang bersifat MITM seperti ARP Poisoning, dan DHCP Rogue IDPS tidak dapat terdeteksi. Hasil dari implementasi IDPS pada Politeknik XYZ berhasil meningkatkan penilaian Indeks KAMI pada kategori Teknologi dan Keamanan Informasi dari tingkat kesiapan pada level I+ menjadi level II+ pemenuhan kerangka kerja dasar.


Kata Kunci: IDS/IPS, IDPS, SNORT, Indeks KAMI

## *ABSTRACT*


| | | |
|---|---|---|
| *Title* | : | *IMPLEMENTATION OF INTRUSION DETECTION AND PREVENTION SYSTEM AND ITS IMPLICATIONS ON INFORMATION SECURITY INDEX CASE STUDY: POLYTECHNIC XYZ* |
| *Name* | : | *Yehovan Nugra Agave* |
| *Study Program* | : | *Technical Information* |


*XYZ Polytechnic as one of the educational institutions that relies heavily on computer networks in its operations requires a network security system that can protect computer network systems. In addition, it is also necessary to assess the readiness of XYZ Polytechnic in implementing a security system that is useful for measuring and increasing the level of computer network security readiness. Intrusion Detection and Prevention System (IDPS) as one of the network security systems that functions as an attack detection system and as an attack prevention system in a computer network. In this research, IDPS are implemented using snort software that runs on the pfSense operating system and uses the Network Development Life Cycle (NDLC) development method in the computer network implementation process. Before and after implementation, a survey of the level of security readiness based on KAMI Index (Information Security) version 4.2 which serves to measure the level of security readiness after the implementation of IDPS. Penetration Testing is done by simulating Denial of Services (DoS) and Man in the Middle (MITM) attacks to test the IDPS system. The results obtained are IDPS can detect and take blocking action against DoS attacks such as SSH Bruteforce, SYN Flood, and UDP Flood, while MITM attacks such as ARP Poisoning, and DHCP Rogue IDPS cannot be detected. The results of the IDPS implementation at XYZ Polytechnic succeeded in improving the KAMI Index assessment in the Information Technology and Security category from the level of readiness at level I + to level II + fulfillment of the basic framework.*

*Keywords: IDS/IPS, IDPS, SNORT, KAMI Index*