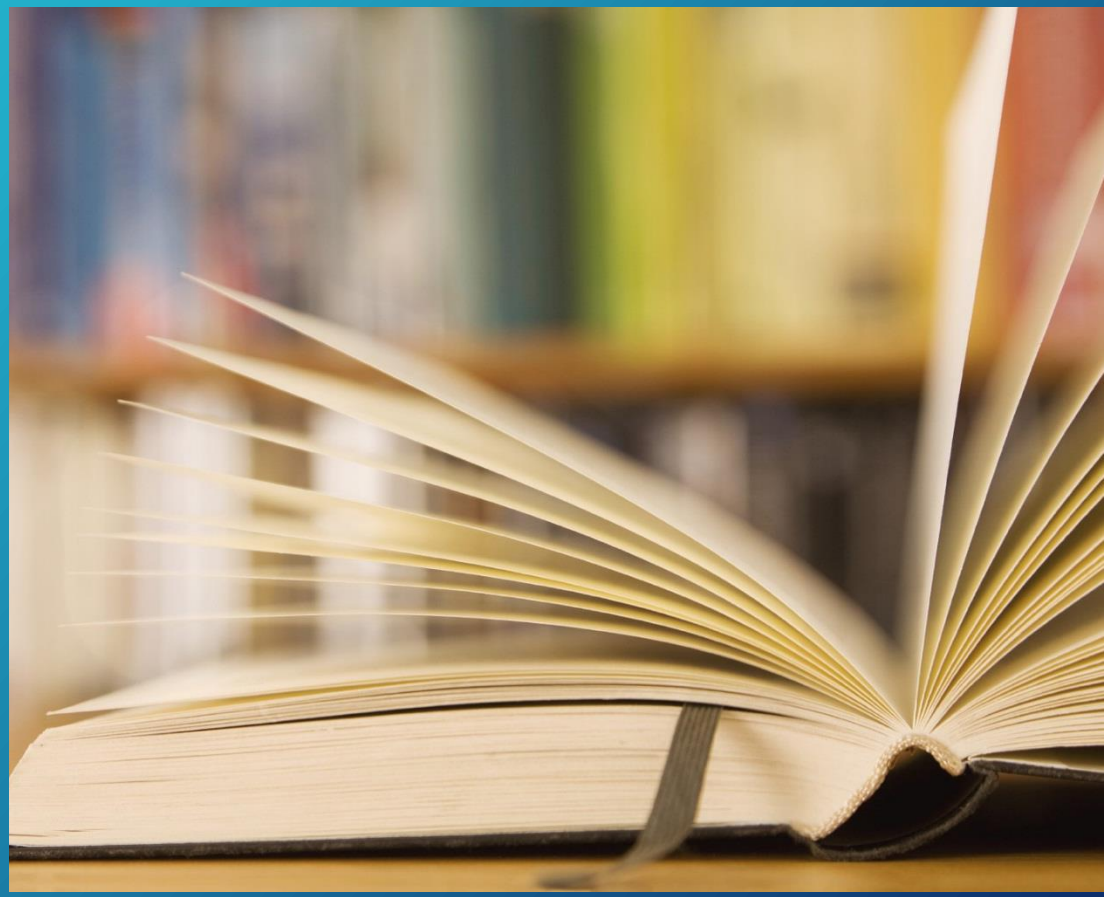
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

INTRUSION DETECTION SYSTEM



Keamanan Sistem Informasi – Aditya Putra, ST., MT.

Agenda

- Konsep IDS/IPS
- Komponen Network IDS/IPS
- Metode Deteksi IDS/IPS
- Deploying Network-based IDS
- Akurasi Sensor
- Dealing with False Positive and False Negative
- Karakteristik IDS yang Baik

Konsep IDS/IPS

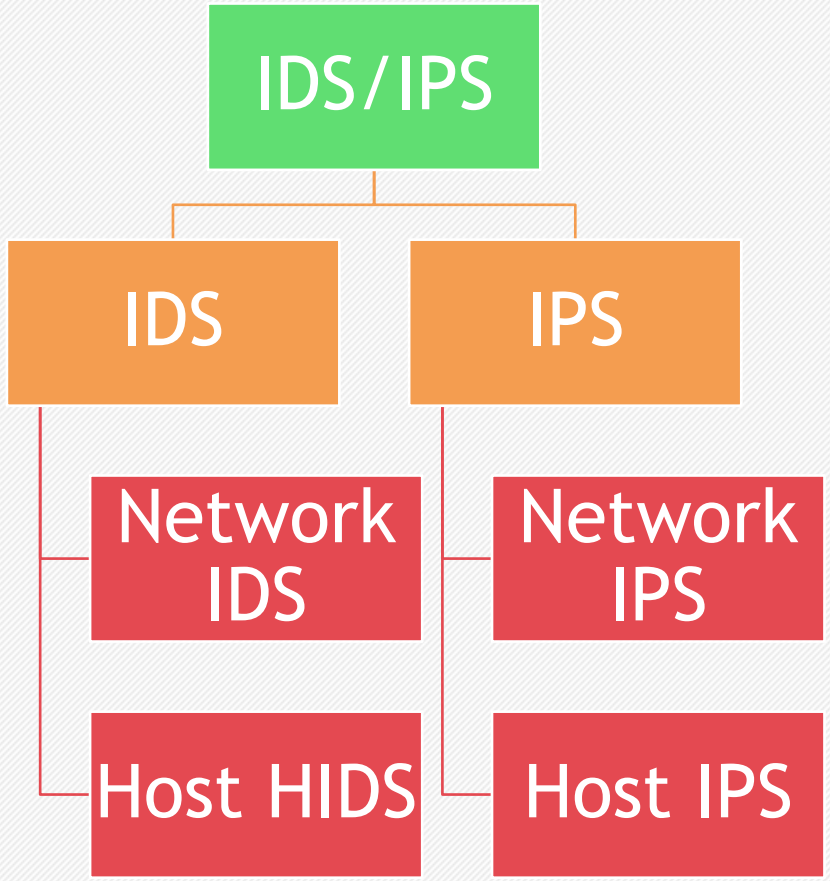
Intrusion Detection/Prevention System (IDS/IPS)

Intrusi adalah upaya illegal untuk merusak nilai CIA dan membahayakan keamanan asset yang dilindungi

Tipe Intrusi pada Jaringan

- Koneksi dari Lokasi (IP) yang tidak biasa
- Percobaan login yang berulang secara remote
- Upaya DDoS/premintaan service berulang dalam jumlah besar

IDS/IPS digunakan untuk mengedalikan intrusi pada jaringan. IDS berperan mendeteksi intrusi sedangkan IPS selain deteksi, memiliki kemampuan untuk mencegah intrusi pada Jaringan



Konsep IDS/IPS

Kemampuan IDS/IPS

- menyediakan layer keamanan tambahan pada jaringan berdasarkan prinsip **defense-in-depth**
- melakukakn hal-hal di luar kemampuan Firewall
- Mengenali pola behaviour dari sebuah serangan
- Meminimalisir peluang ancaman keamanan yang lolos dari ruleset firewall

IDS bukanlah

- Network Logging System
- Produk Antivirus
- Vulnerability Assessment Tools
- Security/Cryptographic System

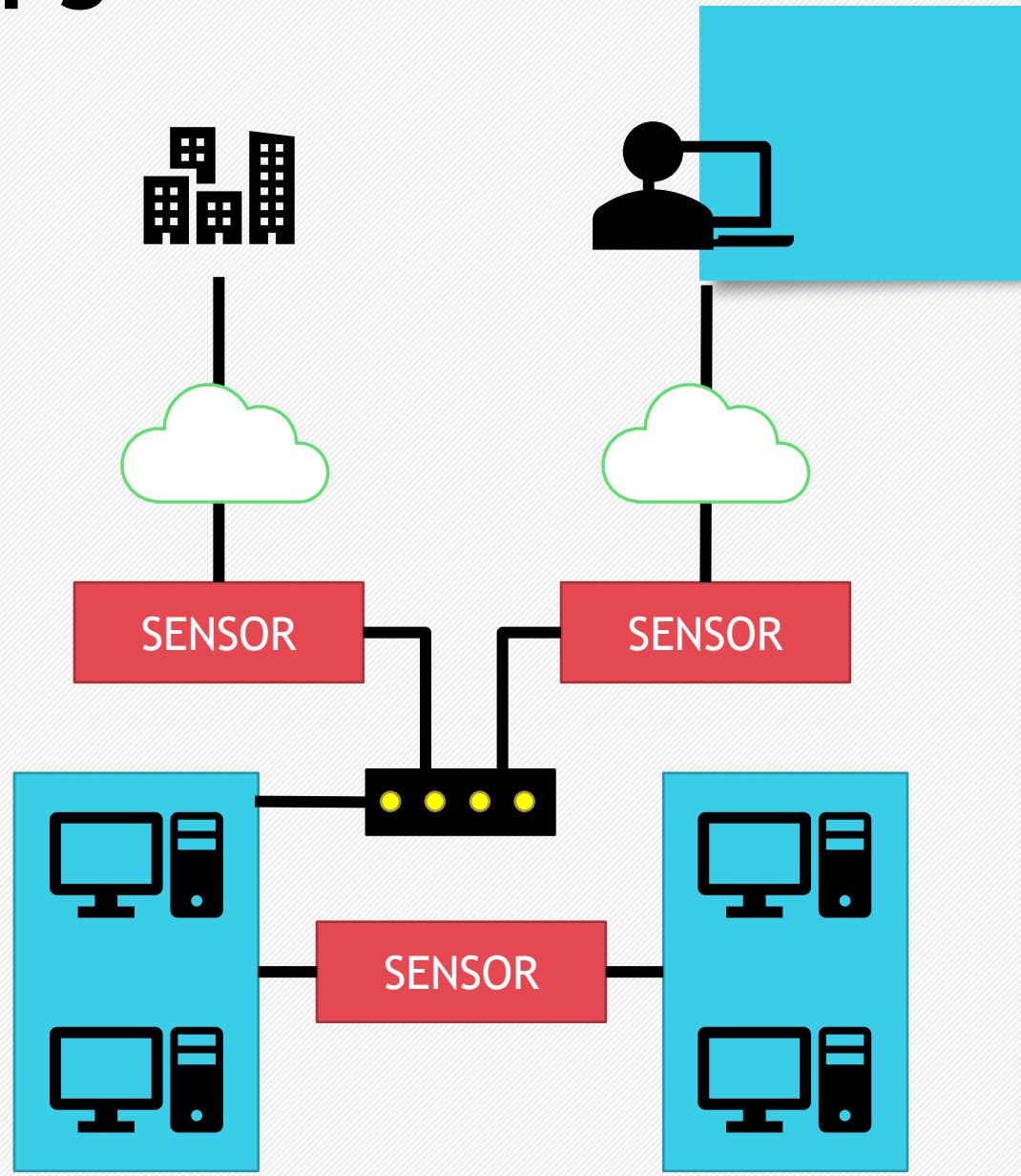
Komponen Network IDS/IPS

Tidak seperti Firewall, IDS/IPS memiliki beberapa komponen:

1. Network Sensor

   Perangkat ini adalah komponen yang melakukan monitoring trafik dan menginisiasi alert jika ada aktivitas abnormal yang terdeteksi. Biasanya diletakkan pada

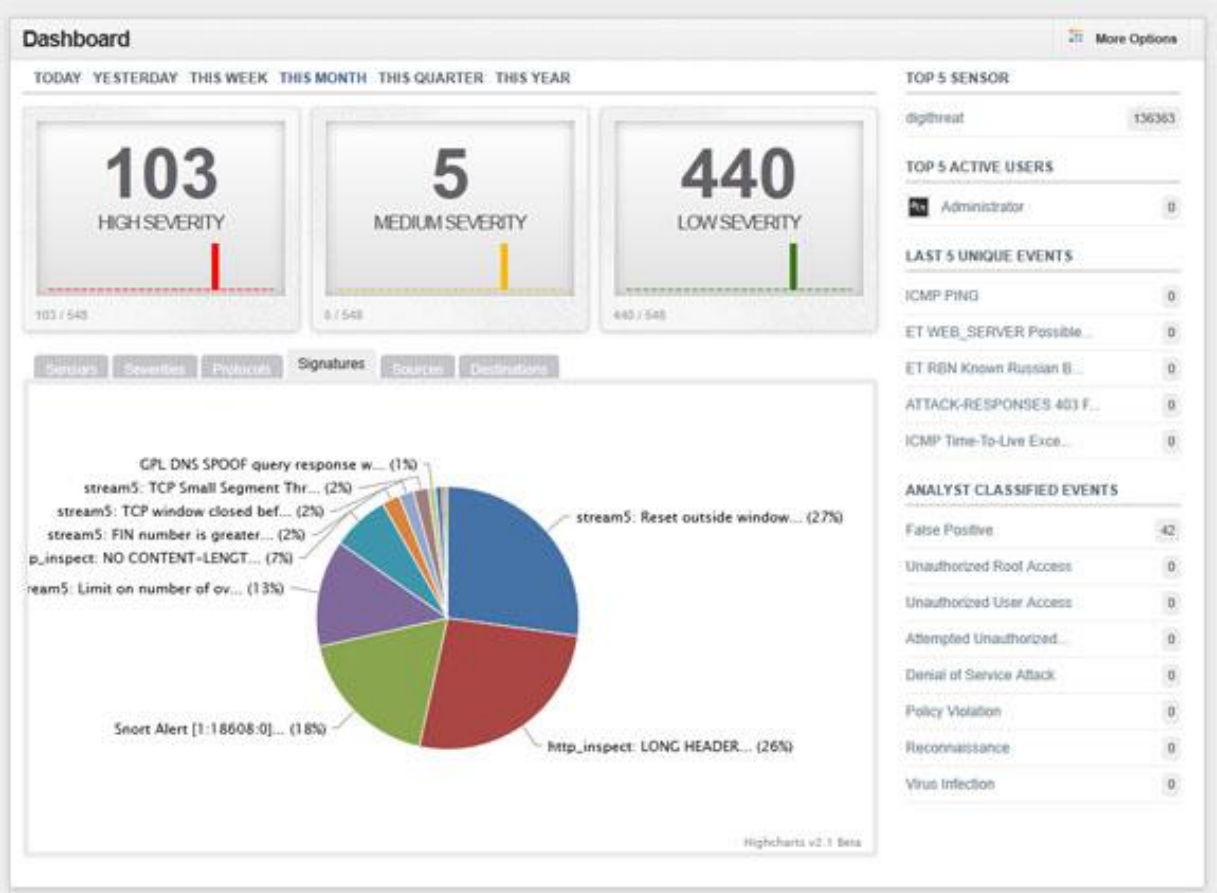
   - Antara remote user dengan jaringan
   - Antara kantor cabang dengan jaringan
   - Antar subnet di jaringan kantor



Komponen Network IDS/IPS

2. Command Console

- Perangkat ini adalah komponen yang terpisah dari Sensor dan diinstall software untuk menampilkan User Interface
- User Interface ini juga membantu administrator untuk menganalisa security event, pesan alert dan log file
- Security event, pesan alert, dan log file didapatkan dari berbagai sensor yang telah dideploy



Command Console karena membutuhkan resource yang besar sehingga perlu diinstall pada dedicated server. Kurangnya resource dapat mengurangi performanya untuk memproses data yang dikirimkan oleh Sensor

Komponen Network IDS/IPS

3. Response System

- Response System berperan dalam melakukan penindakan
- Response system bukan pengganti administrator karena Response system harus memiliki kemampuan dalam menentukan keputusan apa yang diambil dan meresponnya secara otomatis
- Administrator akan membuat keputusan saat menemukan kasus False Positif atau respon lain yang memerlukan eskalasi

4. Attack Signature Database

- Komponen inilah yang membuat IDS memiliki kemampuan untuk membuat keputusan
- Database ini memuat daftar attack signature yaitu karakteristik trafik yang abnormal. Dengan mencocokkan trafik real dengan database ini, IDS dapat mengetahui apakah suatu trafik dapat dikatakan intrusi atau bukan. Lalu memberikan respon yang tepat untuk trafik tersebut

Administrator yang baik tidak bergantung sepenuhnya pada IDS Response Systems untuk merespon intrusi

Metode Deteksi IDS/IPS

IDS pada umumnya menggunakan Signature untuk mengenali pola serangan yang terjadi

- Memonitor pola paket data pada jaringan dan membandingkannya dengan pola serangan jaringan yang dikenal dengan signature
- Metode ini melakukan operasi perbandingan string untuk mengamati dan membandingkan aktivitas jaringan yang sedang terjadi seperti paket atau log entry dengan signature yang ada

Keuntungan:

- False alarm deteksi serangannya yang rendah
- Dapat mengenali penggunaan tool atau teknik tertentu
- Membantu administrator untuk melacak potensi isu security dan menginisiasi prosedur incident handling

Kerugian:

- Pendekatan ini hanya berbasis threat yang telah didefinisikan, database harus terus diupdate dengan pola serangan terbaru
- Penggunaan signature yang kaku membuatnya tidak dapat mengenali varian serangannya secara spesifik

Deploying Network-based IDS

Lokasi deployment Sensor IDS yang memungkinkan	
1. Di belakang **Firewall External** dan **network DMZ**	Memonitor serangan dari luar
	Menunjukkan celah firewall dan policy-nya dalam bertahan terhadap serangan
	Dapat mengamati serangan yang menuju server yang ada di DMZ
	Memonitor outgoing trafik dari server yang compromised
2. Di depan **Firewall External**	Mampu mengenali total jumlah dan tipe serangan yang mengarah ke jaringan
3. Di Backbone Jaringan	Memonitor dan Menginspeksi trafik dalam jumlah besar, meningkatkan tingkat deteksi serangan
	Mendeteksi upaya illegal dari luar organisasi
4. Di Critical Subnet	Mendeteksi serangan yang subnet tersebut
	Fokus memonitor pada subnet tersebut

STT - NF

Akurasi Sensor

Masih ingat dengan ilustrasi di samping?

Setiap sensor memiliki akurasinya masing-masing dan Sensor yang Baik adalah yang memiliki Nilai TP dan TN tinggi serta FP dan FN yang rendah

- FP Rate (FPR) ➔ Tingkat kesalahan Ketika serangan benar-benar terjadi

$$FPR = \frac{FP}{FP + TN} = 1 - TNR$$

*FP + TN adalah 2 kondisi dimana serangan **BENAR** terjadi*

- FN Rate (FNR) ➔ Tingkat kesalahan Ketika serangan tidak terjadi

$$FNR = \frac{FN}{FN + TP} = 1 - TPR$$

*FN + TP adalah 2 kondisi dimana serangan **TIDAK** terjadi*

An Aesop's Fable: The Boy Who Cried Wolf (*compressed*)

A shepherd boy gets bored tending the town's flock. To have some fun, he cries out, "Wolf!" even though no wolf is in sight. The villagers run to protect the flock, but then get really mad when they realize the boy was playing a joke on them.

[Iterate previous paragraph *N* times.]

One night, the shepherd boy sees a real wolf approaching the flock and calls out, "Wolf!" The villagers refuse to be fooled again and stay in their houses. The hungry wolf turns the flock into lamb chops. The town goes hungry. Panic ensues.

Let's make the following definitions:

- "Wolf" is a **positive class**.
- "No wolf" is a **negative class**.

We can summarize our "wolf-prediction" model using a 2x2 confusion matrix that depicts all four possible outcomes:

True Positive (TP): • Reality: A wolf threatened. • Shepherd said: "Wolf." • Outcome: Shepherd is a hero.	**False Positive (FP):** • Reality: No wolf threatened. • Shepherd said: "Wolf." • Outcome: Villagers are angry at shepherd for waking them up.
False Negative (FN): • Reality: A wolf threatened. • Shepherd said: "No wolf." • Outcome: The wolf ate all the sheep.	**True Negative (TN):** • Reality: No wolf threatened. • Shepherd said: "No wolf." • Outcome: Everyone is fine.

Dealing with False Positive

False Positive mengurangi reputasi dan urgensi alert yang valid Ketika serangan benar-benar terjadi. Hal ini tentunya mengurangi legitimasi alert IDS

Sumber-sumber yang menjadi penyebab terjadinya false positive

- Protocol violations
- Network equipment
- Software bugs
- Non-malicious Traffic

Hal-hal yang dapat dilakukan

- Tidak adanya customization atau konfigurasi dapat meningkatkan false alarm hingga 90%
- Konfigurasi yang baik dapat menurukan False Alarm menjadi 60% atau lebih rendah lagi

Dealing with False Negative

False Negative lebih berbahaya dibanding False Positive. Administrator harus mampu menurunkan False Negative tanpa meningkatkan False Positive

Sumber-sumber yang menjadi penyebab terjadinya false positive

- Design network
- Encrypted traffic
- Komunikasi antar department yang rendah (human)
- Format penulisan signature yang tidak sesuai
- Serangan yang tidak dipublish (baru)

Hal-hal yang dapat dilakukan

- Design network, manajemen, dan maintenance yang baik
- Penulisan dan update database signature IDS
- Komunikasi yang baik antar departemen

Karakteristik IDS yang Baik

Karakteristik IDS yang Baik

- Dapat berjalan terus menerus dengan intervensi manusia yang minimal
- Fault tolerant
- Overhead time yang minimal pada system
- Dapat mengenali perlilaku anomali trafik
- Tidak mudah tertipu (Minim FP dan FN)
- Terkonfigurasi sesuai dengan kebutuhan organisasi

Kesalahan IDS yang Perlu Dihindari

- Penempatan sensor bukan pada titik observasi
- Mengabaikan alarm/alert dari IDS
- Tidak memiliki response policy terhadap suatu event
- Konfigurasi/tuning yang tidak baik pada FN dan FP
- Tidak mengupdate database signature IDS
- Hanya memonitor koneksi inbound

Product IDS/IPS

IBM Security Network IPS	Peek & Spy	INTOUCH INSA-Network Security Agent	SilverSky
IDP8200 Intrusion Detection and Prevention Appliances	Check Point Threat Prevention Appliance	Cisco Intrusion Prevention Systems	AIDE (Advanced Intrusion Detection Environment)
SNARE (System iNtrusion Analysis & Reporting Environment)	Vanguard Enforcerd	SNORT	