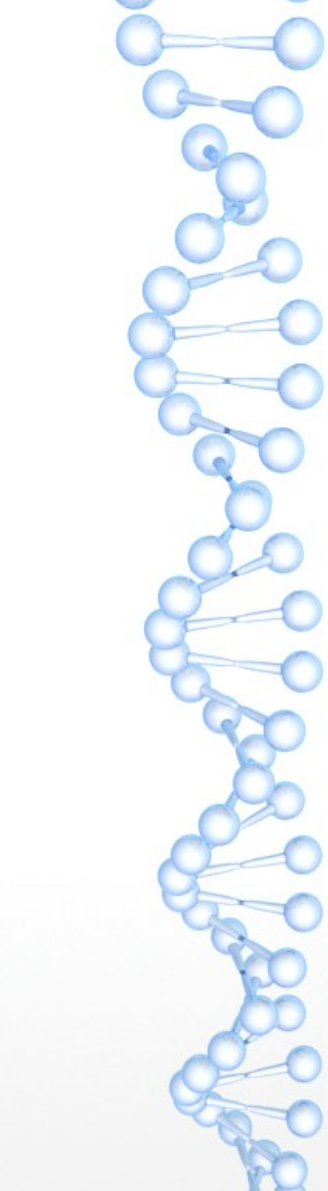
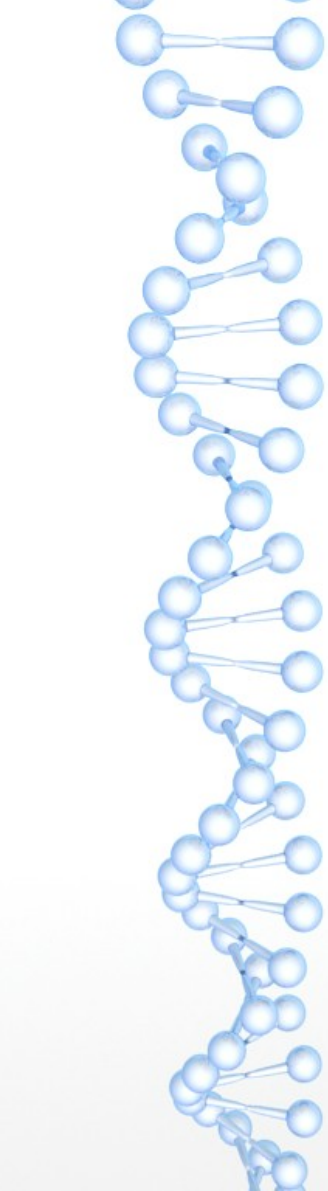


TIS13534P KOMUNIKASI DAN KEAMANAN DATA
Minggu 7 - NIDS

Definisi

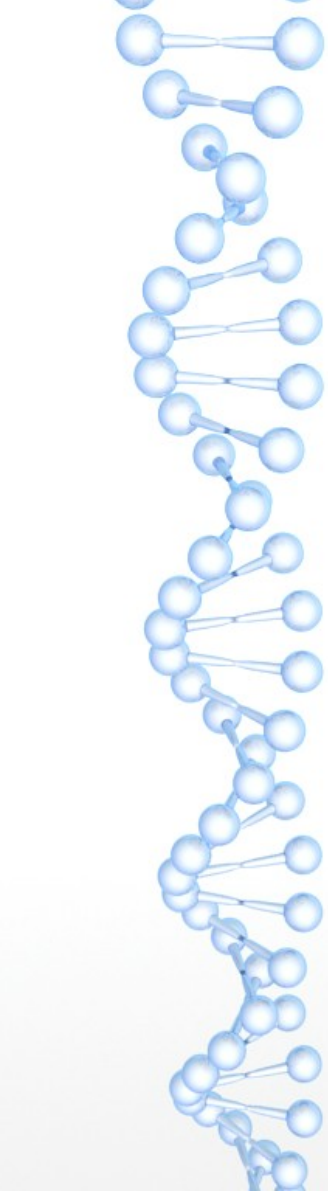
- Intrusion adalah sebuah Aktivitas yang tak dikenali di jaringan komputer yang menyedot sumber daya jaringan, dan membahayakan keamanan jaringan/data

- Intrusion jika tidak dihentikan bisa merusak sistem, mencuri data berharga, bahkan menular ke sistem lainnya yang ada dalam satu jaringan



Jenis Intrusion

- **Traffic Flooding**
- **Protocol-specific Attack**
- **Trojan**



Traffic Flooding

Serangan ini paling umum, dan paling sering digunakan untuk melumpuhkan target (host, atau router) dengan **membanjiri paket-paket data**.

Serangan ini mampu melumpuhkan jaringan yang dilewatinya. Termasuk router dan computer target.

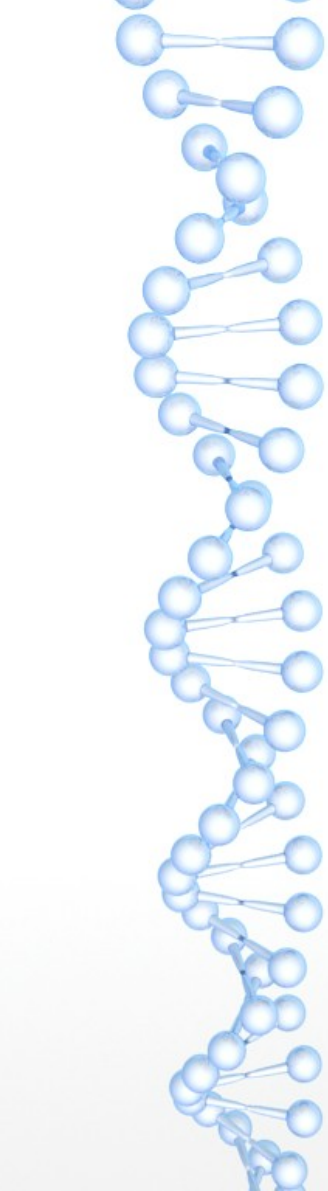
Namun bisa diatasi dengan menutup port computer target yang digunakan oleh penyerang

Contoh: Denial-of-Service, Ping of Death

Protocol-specified Attack

Serangan di mana **penyerang mengirimkan data palsu** (spoofing) atau paket tidak lengkap (malformed message) **melalui protokol-protokol yang umum dipakai.**

Serangan ini dapat mengganggu target jikai dilakukan.



Trojan

- Trojan muncul sebagai program baik-baik, namun aslinya tidak
- Dapat membuka channel ke orang lain, menghapus data, dan bahkan mencurinya

Melawan Intrusion

- Intrusion dapat dikenali, dideteksi, dihentikan dengan Intrusion Detection System.

- Intrusion Detection System adalah sebuah system yang berfungsi untuk mendeteksi aktivitas hacking, serangan denial-of-service, dan port scanning.

IDS

- IDS mendeteksi lalu lintas data/ paket data yang mengalir di saluran masuk (incoming), keluar (outcoming), dan lokal.
- IDS dapat bekerja sama dengan Firewall dalam mengatasi serangan-serangan jaringan

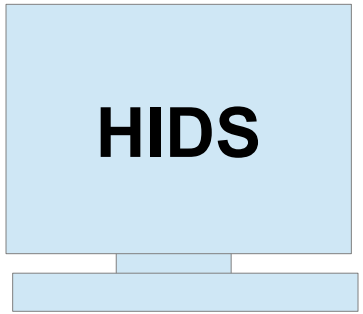
Jenis IDS Menurut Lokasi

- Host-based Intrusion Detection System – HIDS
  - IDS satu ini bekerja di dalam node komputer/host, dia bekerja satu tempat dengan Firewall mencegah serangan internet
- Network Intrusion Detection System – NIDS
  - IDS satu ini berkerja sebagai sniffer di dalam sebuah jaringan, lokasinya sangat beragam disesuaikan dengan kegunaannya.

Cara Kerja IDS

- HIDS
    - Memperhatikan tingkah laku program-program, dan lalu lintas yang ditujukan ke komputer
- NIDS
    - Bekerja sebagai sniffer yang lalu kemudian paket-paket tersebut di analisa dengan database

Host-based Intrusion Detection System (HIDS)



HIDS:
Memonitor Perilaku Dinamis
Memonitor Keadaan Komputer
Memonitor Paket yang ditargetkan ke Host ini

HIDS bahkan dapat mendeteksi word-prosesor yang mengakses sumber daya tertentu, contohnya database password sistem

HIDS

Karakteristik:
- Hanya berjalan di satu host
- Untuk menganalisa audit, log, integritas file dll

Kelebihan:
- Lebih akurat dibanding NIDS
- Volume lalu lintas data minim

Contoh HIDS

- INTRUST Event admin
- ELM 3.0
- GFI LANguard S.E.L.M
- Comodo Internet Security

Network Intrusion Detection System

- Sebuah system keamanan yang berguna untuk membaca paket-paket data yang mengalir di jaringan. Jika ada paket-paket data yang terdeteksi oleh NIDS, maka NIDS akan memberikan peringatan beserta dengan catatannya (logging)
- NIDS bisa diletakkan di mana pun sesuai dengan konfigurasi jaringan itu sendiri.
- Berbeda dengan HIDS, NIDS ditujukan untuk melindungi satu jaringan bukan satu host saja

NIDS

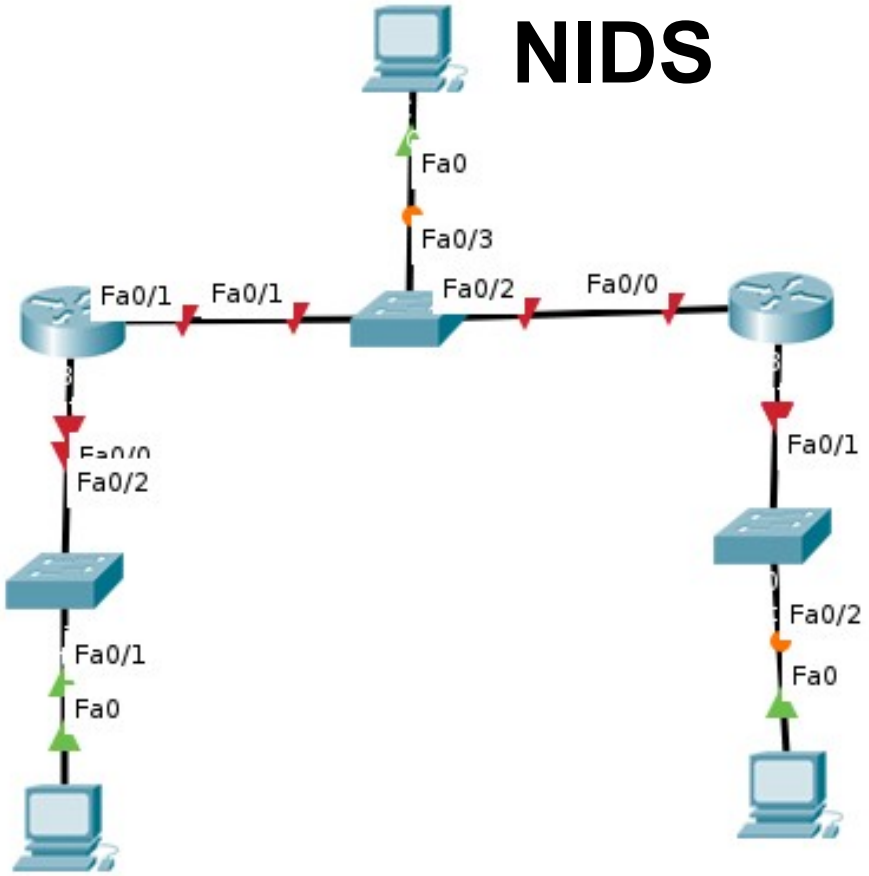
Kelebihan:
- Butuh sedikit sistem untuk menutupi jangkauan IDS
- Lebih murah dibanding HIDS
- Bisa melihat semua lalu lintas data yang mengalir

Kekurangan:
- Tidak bisa berjalan di jaringan terenkripsi
- Tidak bisa melihat lalu lintas yang tidak dilewati

NIDS VS Firewall

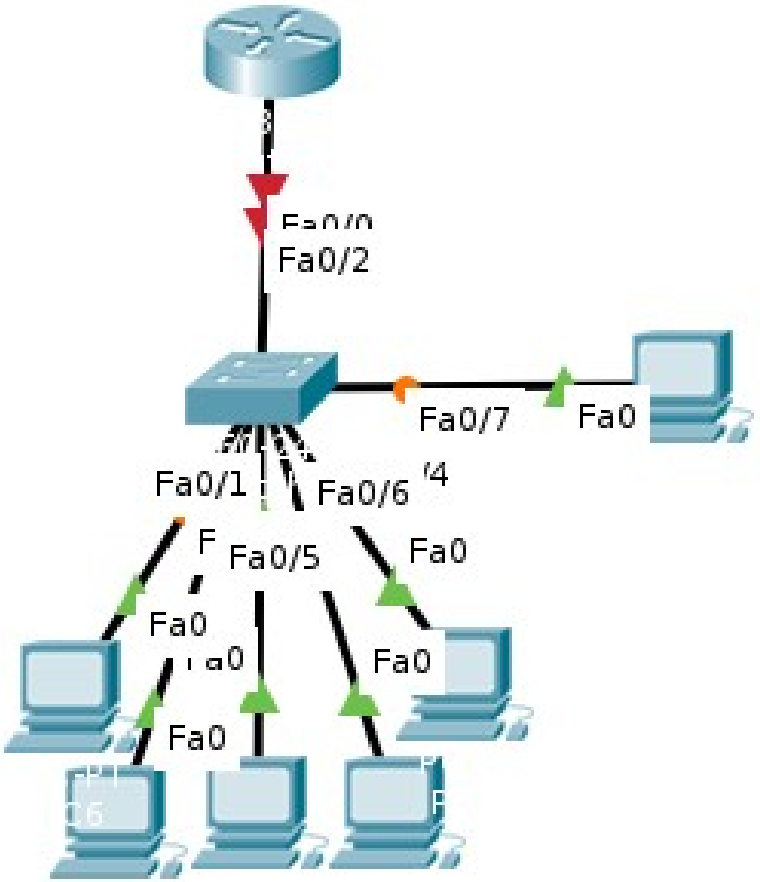
- Firewall
  - Secara aktif memfilter paket-paket yang melalui nya
  - Jika terjadi kegagalan, lalu lintas akan ditutup
- NIDS
  - Secara pasif memonitor lalu lintas data
  - Jika terjadi kegagalan, lalu lintas tetap berjalan

Lokasi-Lokasi NIDS



NIDS terletak di antara
2 Jaringan LAN

Lokasi NIDS

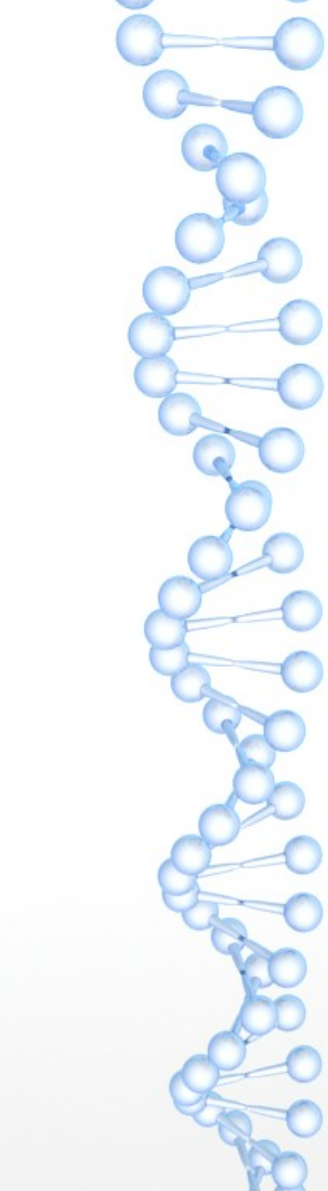


NIDS

NIDS terletak di jaringan LAN

Penjelasan

Di mana pun NIDS berada, Switch tempat dia tersambung harus dikonfigurasi sehingga paket-paket data yang mengalir juga di kopi kan ke NIDS



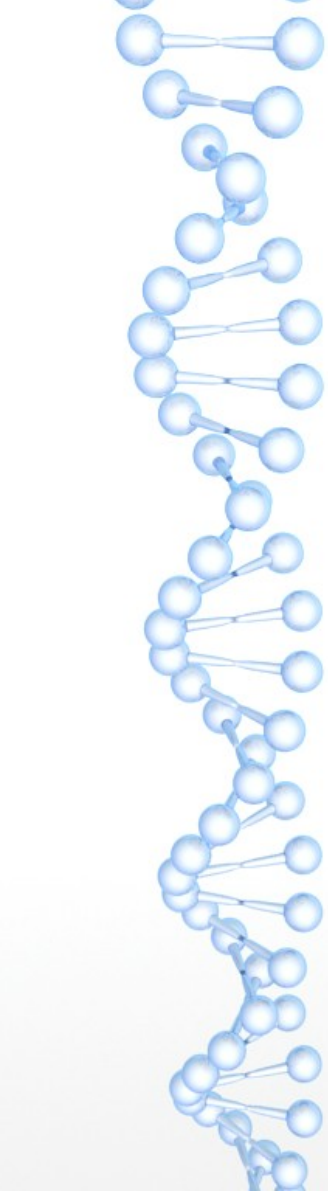
Database HIDS & NIDS

- Pada dasar NIDS dan HIDS bekerja menggunakan database sebagai acuannya, namun bukan berarti tidak dilengkapi dengan teknologi Heuristic.

- Sebagian dari mereka dilengkapi dengan Heuristic untuk mendeteksi anomaly paket (menggunakan teknologi AI)

Contoh Rule NIDS

- alert udp $HOME_NET any -> $EXTERNAL_NET 53
- (msg:"BLACKLIST DNS request for known malware domain xixbh.net - Win.Trojan.Dorkbot";
- content:"|05|xixbh|03|net";
- fast_pattern:only;
- classtype:trojan-activity;
- sid:26405;
- rev:2;)



Hasil Deteksi NIDS

Istilah-istilah berikut ini juga digunakan oleh Antivirus, dan Anti Malware:

- **True Positive**: Paket Tersebut adalah benar-benar Intrusion, dan NIDS memberi respons
- **True Negative**: Alarm Palsu
- **False Positive**: Paket adalah Intrusion tapi NIDS tidak memberikan respons
- **False Negative**: Paket bukan Intrusion dan tidak ada respons dari NIDS

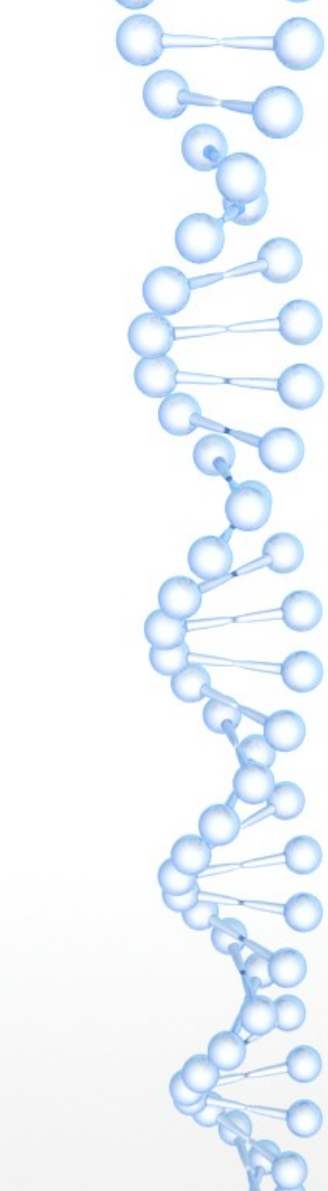
SNORT

Snort adalah aplikasi NIDS yang gratis untuk di download dan digunakan di mana pun.

Snort dijalankan menggunakan metode CLI, namun laporan yang disajikan oleh Snort ditampilkan baik GUI via Web maupun CLI

Snort

- Snort dapat diletakkan di mana pun sesuai kebutuhan, dan biasanya diletakkan sebelum router untuk mencegah serangan masuk ke dalam jaringan
- Snort menggunakan Database yaitu kumpulan rules yang sudah didefinisikan sesuai jenis serangan yang ada hingga saat ini.
- User juga dapat menambahkan rule mereka sendiri



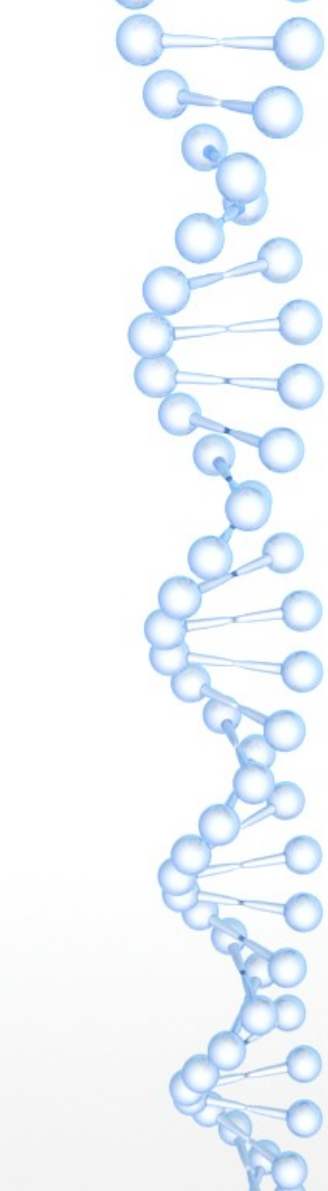
Contoh Rule Snort

alert icmp any any -> any any (msg:"PING JUGA FLOODING”)

- Alert: Beri notifikasi
- Icmp: Protokol
- Any any: Semua IP Semua Port
- -> : arah paket
- Msg: Pesan Logging Jika Terdeteksi

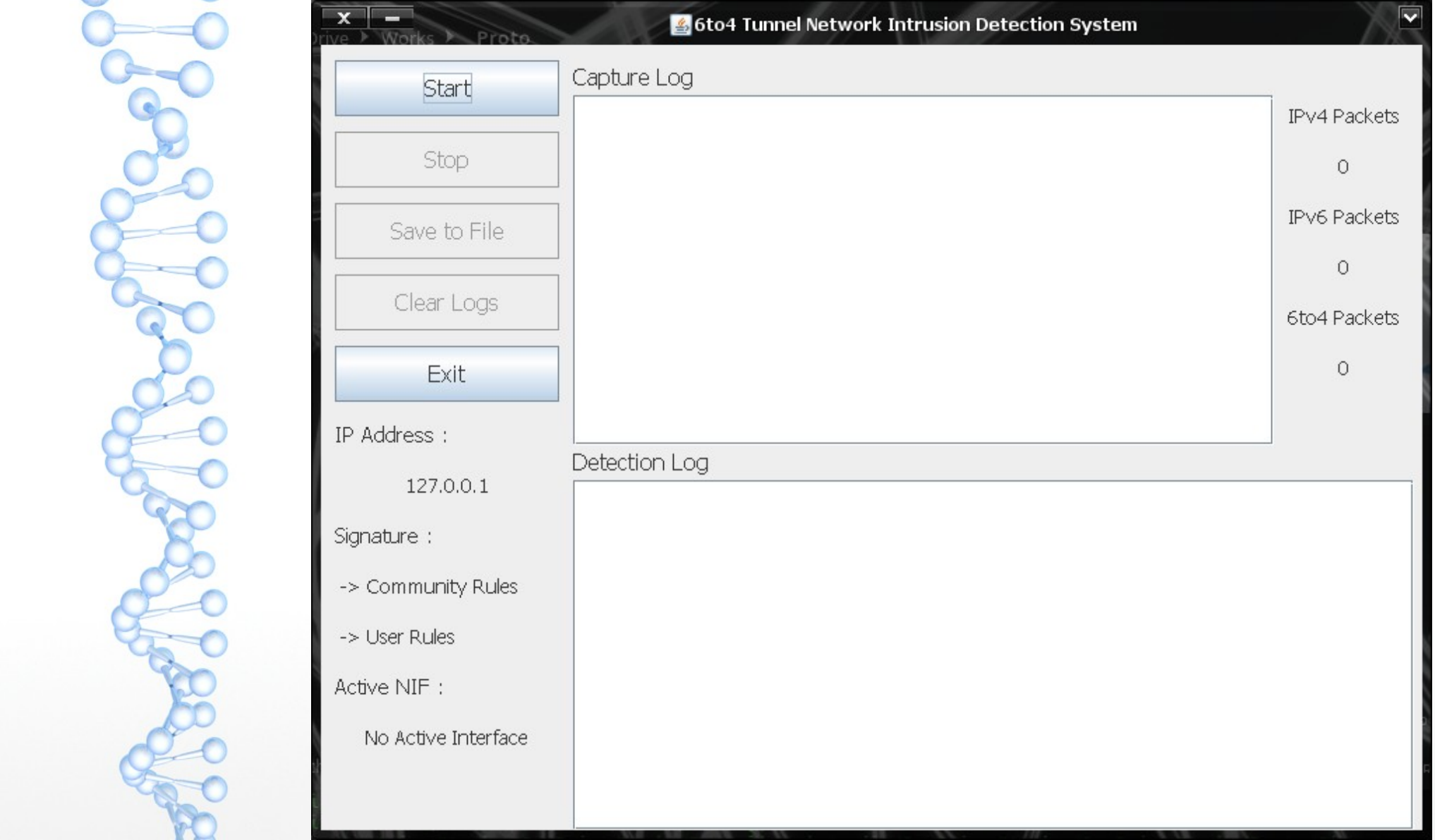
Kelebihan dan Kekurangan Snort

- +
- Tersedia untuk semua OS
- Gratis
- Reaksi Cepat
- -
- Butuh pemahaman dasar jaringan
- Tidak bagus untuk jaringan tertentu



Java-based NIDS

- Software ini adalah prototyping untuk implementasi algortima yang saya buat
- Ditulis dengan bahasa Java sehingga bisa dipakai di mana-mana, namun harus dibantu dengan Library dari bahasa C
- Memerlukan jaringan khusus untuk bekerja

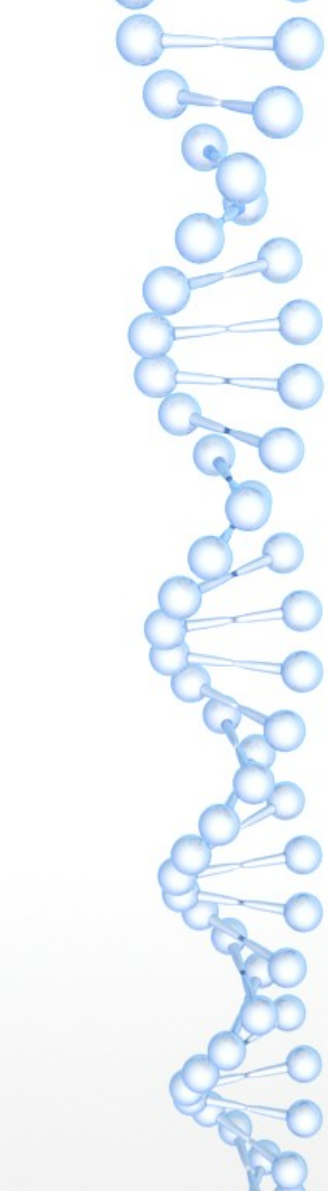

6to4 Tunnel Network Intrusion Detection System
Start
Stop
Save to File
Clear Logs
Exit
IP Address :
127.0.0.1
Signature :
-> Community Rules
-> User Rules
Active NIF :
No Active Interface
Capture Log
IPv4 Packets
0
IPv6 Packets
0
6to4 Packets
0
Detection Log

Java-based NIDS

- Software ini akan mengeluarkan ERROR jika:
  - Tidak ada koneksi jaringan (tertulis IP lokal 127.0.0.1)
  - File Signature Hilang
  - Dan beberapa error lainnya yang dikarenakan oleh alpha protoyping

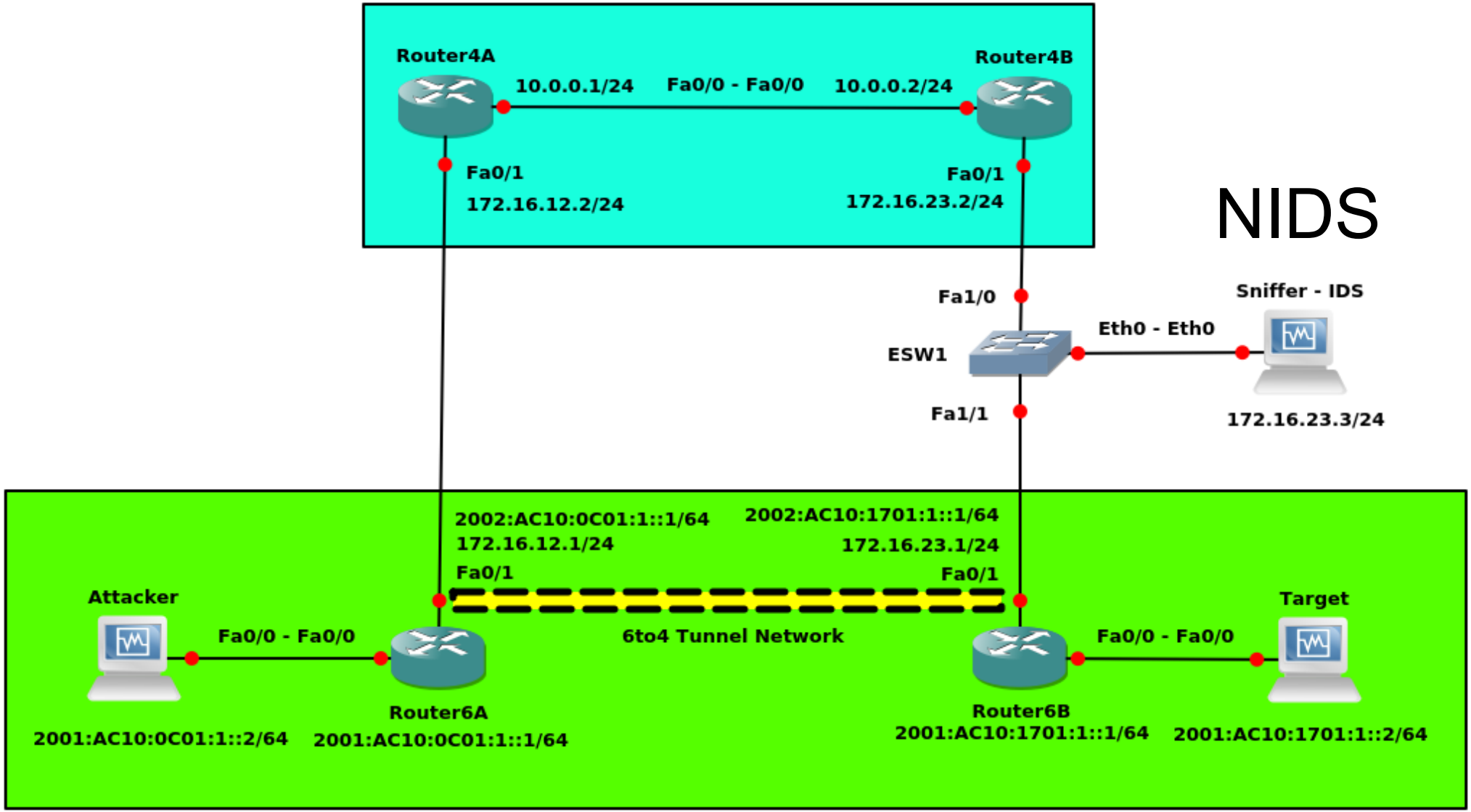
Java-based NIDS

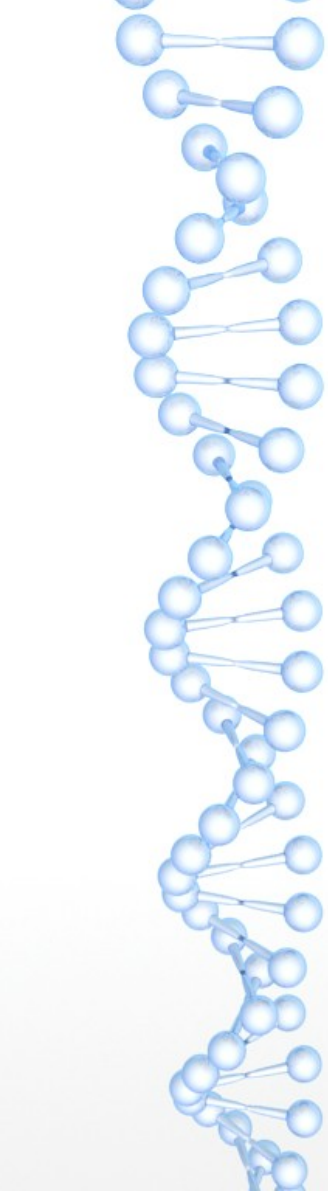
- Software ini akan mengeluarkan ERROR jika:
  - Tidak ada koneksi jaringan (tertulis IP lokal 127.0.0.1)
  - File Signature Hilang
  - Dan beberapa error lainnya yang dikarenakan oleh alpha protoyping



Java-based NIDS

- Dia akan melakukan dua jenis logging:
  - Paket data yang lewat (baik Intrusion maupun tidak)
  - Paket data yang terdeteksi sebagai Intrusion

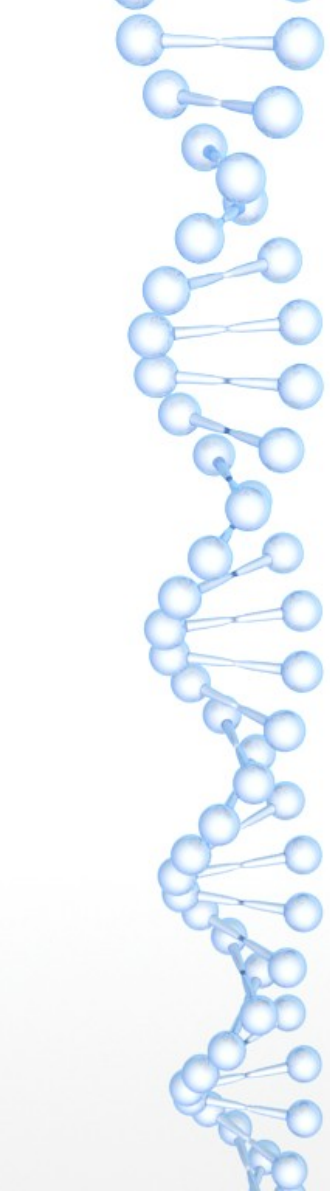

Router4A
10.0.0.1/24
Fa0/0 - Fa0/0
10.0.0.2/24
Router4B
Fa0/1
172.16.12.2/24
Fa0/1
172.16.23.2/24
NIDS
Fa1/0
Sniffer - IDS
Eth0 - Eth0
ESW1
Fa1/1
172.16.23.3/24
2002:AC10:0C01:1::1/64
172.16.12.1/24
2002:AC10:1701:1::1/64
172.16.23.1/24
Fa0/1
Fa0/1
Attacker
Target
Fa0/0 - Fa0/0
6to4 Tunnel Network
Fa0/0 - Fa0/0
Router6A
Router6B
2001:AC10:0C01:1::2/64
2001:AC10:0C01:1::1/64
2001:AC10:1701:1::1/64
2001:AC10:1701:1::2/64



Java-based NIDS

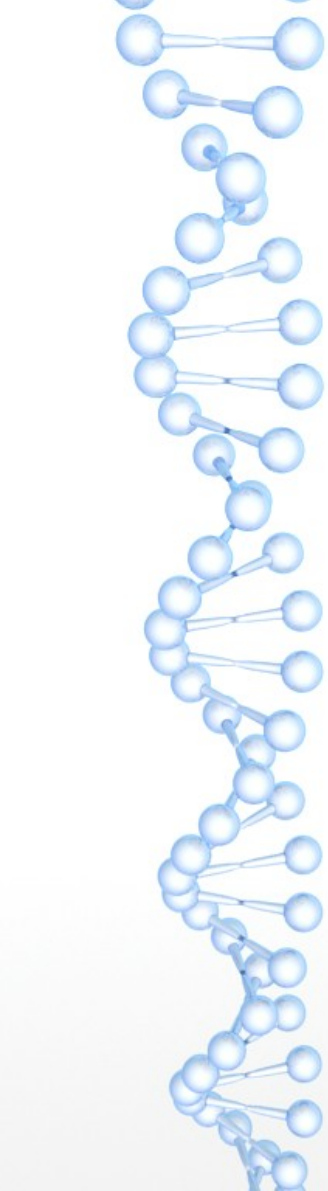
Kelebihan:
- Mampu membaca rule dari Snort (sebagian)
- Portable
- Ada tampilan GUI

Kelemahan:
- Hanya untuk Jaringan 6to4
- Lambat prosesing Intrusion
- Rule yang digunakan tidak lengkap



Saya Tertarik Ingin Buat, Apa Yang Harus Disiapkan?

- Satu Bahasa Pemrograman
- Library Untuk Capturing dari NIC
- Database Intrusi (bisa menggunakan database Snort)
- Algortima untuk mendeteksi Intrusion
- Sampel Data Intrusion (jika ingin lebih spesifik untuk intrusion tertentu)



Bersambung...