

# Introduction

Pengertian Intrusion Detection System

- Menurut **Badan Siber dan Sandi Negara (BSSN)**, **IDS** merupakan komponen penting dalam pertahanan jaringan yang berfungsi untuk **mengawasi dan menganalisis lalu lintas jaringan serta mendeteksi pola serangan** yang telah dikenali, seperti scanning, malware, atau akses tidak sah (BSSN, Modul Pelatihan Keamanan Jaringan, 2021).



# Introduction

Pengertian Intrusion Detection System

- Sementara itu, menurut **National Institute of Standards and Technology (NIST)** dalam publikasi Guide to Intrusion Detection and Prevention Systems (IDPS) (SP 800-94), IDS adalah: “**A system that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.**”



# Introduction

Pengertian Intrusion Detection System

- **Fungsi IDS:**

- Menganalisis data dan lalu lintas untuk mencari pola serangan.
- Memberikan peringatan (alert) kepada administrator sistem jika ditemukan aktivitas yang berpotensi berbahaya.
- Membantu analisis forensic setelah terjadi insiden keamanan.
- Mengidentifikasi pola serangan untuk keperluan evaluasi keamanan sistem.



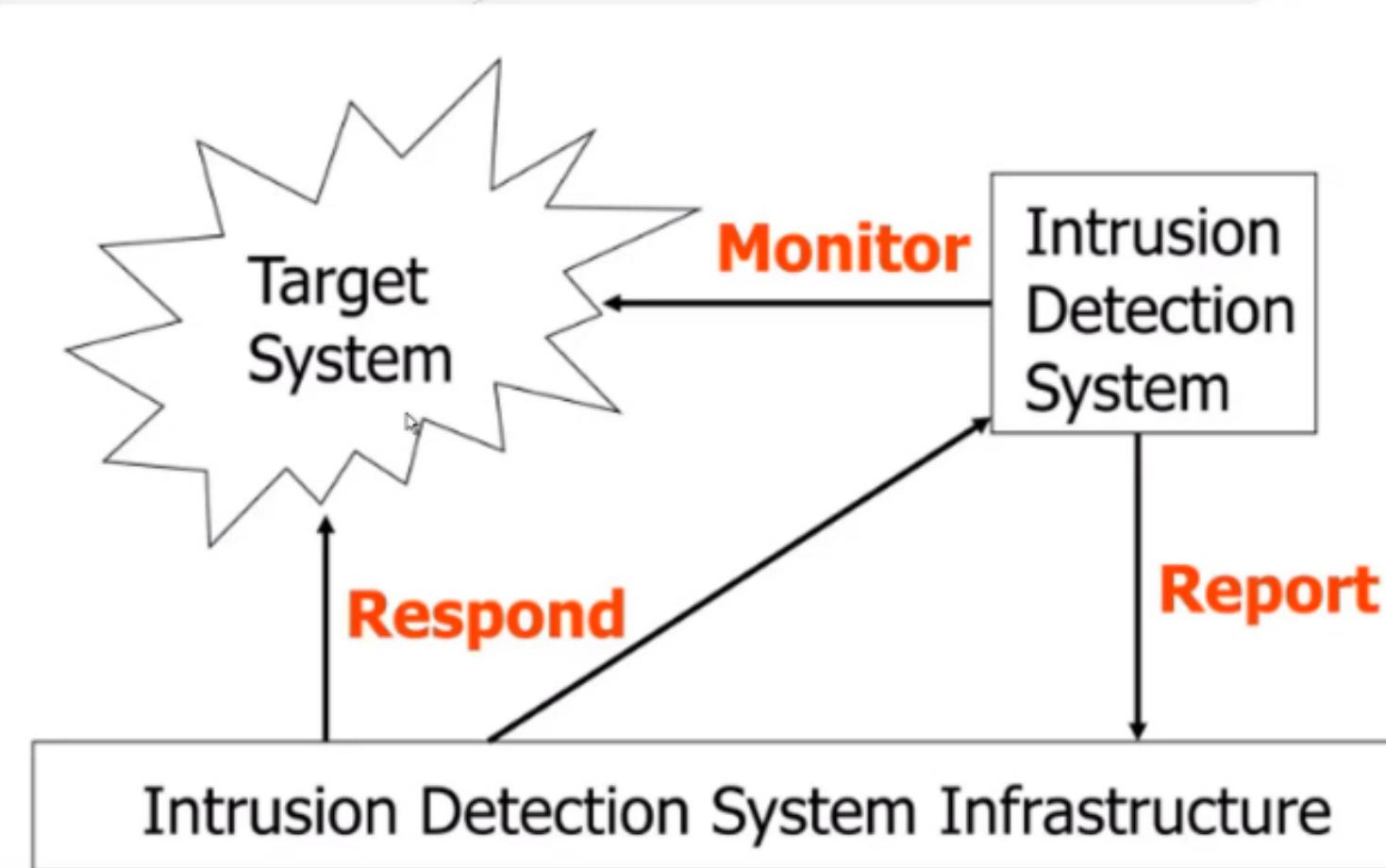
# Kenapa Butuh Sistem Pendeksi Intrusi?

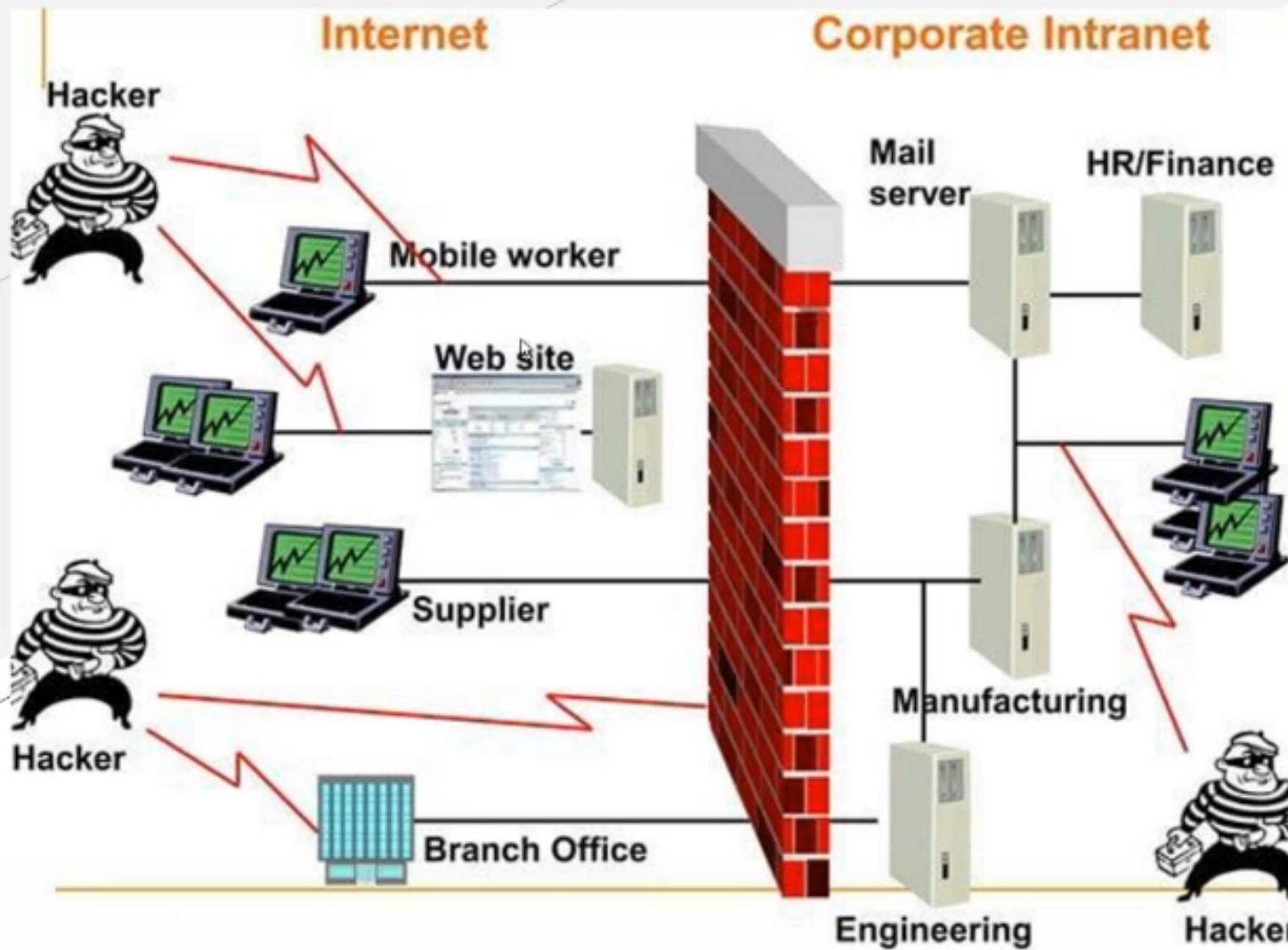
- Firewall tidak bisa mendekksi semua jenis ancaman.
- Ada beberapa aplikasi yang memang diloloskan oleh firewall:
  - Web (HTTPP/HTTPS)
  - Serangan seperti **SQL Injection**, **Cross Site Scripting (XSS)**, atau malware melalui lampiran email bisa lolos karena **tidak melanggar aturan firewall**.
- Tidak semua ancaman berasal dari luar firewall, tapi dari dalam jaringan sendiri.
  - Pegawai yang menyalahgunakan hak akses
  - Perangkat yang telah terinfeksi malware di dalam jaringan
  - Kesalahan konfigurasi yang membuka celah keamanan
  - IDS mampu memantau aktivitas jaringan internal dan memberikan peringatan jika ada perilaku yang menyimpang dari normal.
- Firewall bisa menjadi target serangan.
- Perlu aplikasi sebagai pelengkap Firewall yang bisa **mendeteksi ancaman yang tidak bisa mendeksi oleh sistem防火墙**.

# Kenapa Butuh Sistem Pendeteksi Intrusi?

- Firewall bisa menjadi target serangan.
  - Firewall adalah titik sentral pengendali lalu lintas, sehingga juga menjadi target utama serangan. Jika firewall berhasil disusupi atau dijatuhkan (DoS/DDoS), maka jalur pertahanan utama bisa lumpuh.IDS akan tetap memantau aktivitas jaringan meskipun firewall terganggu, dan bisa memberikan notifikasi dini terhadap upaya penyerangan firewall.
- IDS Memberikan perlindungan tambahan dan deteksi lebih dalam
  - IDS bisa mendeteksi serangan signature-based dan anomaly-based
  - Mencatat log aktivitas berbahaya
  - Membantu analisis forensik insiden
  - Melengkapi firewall dalam strategi pertahanan berlapis (defense-in-depth).

## Basic IDS





Gemma Cahya H. S

# Pendekatan IDS

Terdapat 2 Pendekatan

## Preemptory

- Pendekatan preemptory adalah pendekatan yang bersifat langsung (real-time), di mana IDS secara aktif mendengarkan lalu lintas jaringan saat data mengalir.
- IDS akan menganalisis traffic jaringan secara langsung (live packet inspection).
- Ketika mendeteksi aktivitas mencurigakan, sistem segera mencatat kejadian dan dapat mengambil tindakan otomatis seperti memutus koneksi, mengirim alert, atau men-trigger firewall.

### Karakteristik:

- Bersifat real-time monitoring.
- Mendeteksi serangan saat sedang berlangsung.
- Dapat langsung merespons (jika terintegrasi dengan sistem respon otomatis).

Contoh tools: Snort (Network-based IDS) Suricata Zeek (Bro IDS)

Gemma Cahya H. S

# Pendekatan IDS

## Reactionary (Pendekatan Reaktif)

- Pendekatan yang berbasis analisis terhadap log atau rekaman aktivitas sistem setelah kejadian terjadi.
- IDS ini mengamati file log dari sistem, aplikasi, atau jaringan, bukan lalu lintas langsung.
- Ketika menemukan pola aktivitas mencurigakan di log, IDS akan mencatat dan melaporkan.
- Tindakan bisa diambil setelah kejadian dianalisis.

## Karakteristik:

- Bersifat post-event analysis (setelah kejadian).
- Tidak mengganggu performa jaringan karena tidak menganalisis live traffic.
- Cocok untuk host-based IDS. Contoh tools: OSSEC (Host-based IDS) Tripwire AIDE (Advanced Intrusion Detection Environment)

Gemma Cahya H. S

## Pendekatan IDS

Aspek	Preemptory IDS	Reactionary IDS
Sumber Data	Traffic jaringan secara langsung	Log sistem/aplikasi
Waktu Deteksi	Real-time	Setelah kejadian
Respons	Bisa langsung (otomatis/manual)	Tertunda (manual/terjadwal)
Contoh Tools	Snort, Suricata, Zeek	OSSEC, Tripwire, AIDE
Cocok untuk	Network-based IDS	Host-based IDS
Aspek	Preemptory IDS	Reactionary IDS

# Klasifikasi IDS Berdasarkan Penempatan

## Network-Based IDS (NIDS)

- Memonitor lalu lintas jaringan dan menganalisis paket data untuk mendeteksi serangan atau aktivitas yang mencurigakan. Misal: melihat adanya network scanning.
- Ditempatkan di titik strategis jaringan di luar firewall, seperti dekat gateway atau di belakang firewall. Contoh: Snort, Suricata, Zeek.
- Menyediakan real-time monitoring activity jaringan:
  - Meng-capture, menguji header dan isi paket.
  - Membandingkan dengan pattern dan threat yang ada di database
  - Memberikan respon jika dianggap pengganggu.
- Respons berupa: notifying a console, sending an e-mail message, terminating the session.
  - Meng-capture, menguji header dan isi paket.

# Klasifikasi IDS Berdasarkan Penempatan

## Network-Based IDS (NIDS)

- Kelebihan:
  - Dapat mendeteksi serangan yang menargetkan banyak perangkat dalam jaringan.
  - Tidak memerlukan instalasi di setiap host.
- Kekurangan:
  - Tidak dapat mendeteksi serangan yang dilakukan secara terenkripsi (misal: dalam koneksi HTTPS).
  - Dapat mengalami Bottleneck jika ditempatkan di jaringan dengan lalu lintas tinggi.

# Klasifikasi IDS

## Host-Based IDS (NIDS)

- Berfokus pada aktivitas yang terjadi di level host atau sistem individu.
- Dipasang langsung di perangkat (host) untuk menganalisis aktivitas sistem operasi, log file, dan perubahan konfigurasi.
- Memantau aktivitas pengguna, perubahan file sistem, dan log keamanan.
- Kelebihan:
  - Dapat mendeteksi serangan berbasis malware atau aktivitas tidak sah yang terjadi di dalam sistem.
  - Memberikan informasi lebih rinci dibandingkan NIDS.
- Kekurangan:
  - Harus diinstal di setiap perangkat yang ingin dilindungi.
  - Dapat membebani performa sistem karena terus melakukan pemantauan.

## Klasifikasi IDS

### Signature-Based IDS

- Mendeteksi serangan dengan membandingkan aktivitas jaringan atau sistem dengan database pola serangan yang telah dikenal (signature).
- Kelebihan:
  - Tingkat false positive yang rendah untuk serangan yang telah dikenal.
  - Cepat dalam mendeteksi serangan yang telah memiliki signature.
- Kekurangan:
  - Tidak efektif untuk mendeteksi serangan baru. Misal: Zero-day attacks.
  - Memerlukan pembaruan database signature secara berkala.

## Klasifikasi IDS

Jenis IDS	Fokus Pemantauan	Kelebihan	Kekurangan
Network-Based	Lalu lintas jaringan	Deteksi serangan dari luar jaringan.	Kurang efektif untuk serangan internal.
Host-Based	Aktivitas pada host	Deteksi serangan dari dalam sistem.	Tidak memantau lalu lintas jaringan dari luar.
Signature-Based	Pola serangan yang dikenal	Akurat untuk serangan yang dikenal.	Tidak efektif untuk serangan baru.
Anomaly-Based	Penyimpangan dari keadaan normal sistem	Deteksi serangan baru atau tidak dikenal.	Tingkat false positive yang tinggi.

# Metode Pendektsian Serangan

## Rule Based / Signature Analysis

- Mendeksi dengan melakukan monitoring trafik jaringan dan mencocokkan pola penyerangan (signature) yang serupa.
- Lebih sulit dan membutuhkan waktu untuk memodelkan pattern (pola) berbagai macam intrusi baru.
- Tools: Snort

## Anomaly Detection

- Sistem mendefinisikan pola atau behavior jaringan sebelumnya. Semua deviasi dari pola normal akan dilaporkan sebagai serangan.
- Bisa mendeksi serangan dengan cara melihat deviasi dari pola normal.

# **Metode Pendekripsi Anomali**

## **Analisa Header**

- Berusaha menganalisa suatu serangan berdasarkan analisa nilai field yang dimiliki oleh header layer datalink, network, dan transport. Analisa paket header tidak menganalisa layer aplikasi atau isi paket. Biasa digunakan untuk menganalisa serangan dari lalu lintas jaringan yang tidak memiliki koneksi penuh ke network.

## **Analisa Payload (Contents Paket)**

- Didapatkan dari ekstraksi sesimpunan atribut dari setiap kejadian, baik koneksi TCP maupun UDP termasuk di dalamnya isi dari paket. Digunakan untuk menganalisa perilaku serangan yang sudah masuk ke sistem, misal U2R

## **Metode Pendeksi Anomali**

- Pertama: data trafik jaringan ditangkap dengan perangkat lunak tcpdump.
- Setelah melalui tahap preprocessing data dibagi menjadi dua bagian, yaitu data training dan data testing.
- Dengan menggunakan metode tertentu data training diklasifikasi menjadi dua kelas intrusi dan non intrusi.
- Hasil training digunakan untuk melakukan testing.

## Prinsip Kerja Pendekripsi Anomali

- Menganalisa paket normal saja, deviasi normal dianggap anomali/serangan.
- Sebagian besar IDS untuk anomali dilakukan dengan cara mengobservasi port dan ip yang tidak umum.
- Memiliki nilai yang tidak ada pada data normal yang di training
- Serangan memanfaatkan bug software untuk masuk ke sistem
- Teknik attack biasanya menggunakan bad checksum, unusual TCP flags, duplicate TCP packet, dll.
- Biasanya target program yang diserang memiliki perilaku yang tidak normal sehingga menghasilkan sistem yang tidak normal dan output yang tidak normal juga.

# Introduction

## Intrusion Prevention System

- Sebuah sistem yang tidak hanya mendeteksi serangan, namun juga dapat mencegah secara otomatis, seperti dengan memblokir lalu lintas yang mencurigakan.
- Fungsi Utama IPS:
  - Menganalisis lalu lintas secara real-time.
  - Menghentikan koneksi yang mencurigakan.
  - Mengupdate database signatur secara berkala untuk mencegah serangan baru.
  - Dapat diintegrasikan dengan firewall untuk perlindungan yang lebih komprehensif.



# Perbedaan Utama IDS vs IPS

Aspek	IDS	IPS
Fungsi utama	Mendeteksi serangan.	Mendeteksi dan mencegah serangan.
Respon terhadap serangan	Memberi peringatan (alert ke admin)	Secara otomatis mengambil tindakan (Blokir, isolasi, dll) untuk menghentikan serangan.
Mode Kerja	Pasif	Aktif
Letak dalam jaringan	Passive mode, biasanya setelah firewall.	Inline mode, berada di antara jaringan, sebelum atau sejajar dengan firewall.
Contoh tindakan	Kirim notifikasi atau log serangan.	Blokir IP, reset koneksi drop paket data.
Kontrol terhadap trafik	Tidak dapat menghentikan trafik secara langsung.	Dapat menghentikan / mengubah trafik berbahaya.

## PortSentry

01

### Metode IDS

Alat deteksi intrusi yang berfungsi untuk mendeteksi dan merespons pemindaian port yang dilakukan oleh penyerang.

- Cara Kerja PortSentry

- Port Scanning

- Memonitor port jaringan secara terus-menerus untuk mendeteksi adanya aktivitas pemindaian yang tidak sah.
    - Dapat dikonfigurasi untuk bekerja dalam metode stealth, yang membuatnya sulit dideteksi oleh penyerang.

- Deteksi Pemindaian Port

- Jika ada permintaan koneksi yang mencurigakan ke beberapa port dalam waktu singkat.

- Blokir IP Penyerang

- Integrasi dengan Sistem Keamanan

Gemma Cahya H. S

## PortSentry

01

### Metode IDS

- **Kelebihan**

- Mendeteksi serangan lebih awal sebelum peretas mencoba mengeskloitasi sistem.
- Dapat dikonfigurasi untuk memblokir IP Penyerang secara otomatis dengan iptables atau TCP Wrappers.
- Ringan dan mudah diimplementasikan di berbagai sistem operasi berbasis Linux.

- **Kelemahan**

- Dapat menyebabkan false positive, di mana koneksi yang sah dapat terdeteksi sebagai ancaman.
- Kurang efektif untuk serangan yang lebih kompleks, seperti serangan berbasis exploit yang tidak diawali dengan port scanning.

Gemma Cahya H. S

## HoneyPot

02

## Metode IDS

Sistem yang sengaja dirancang untuk menjadi umpan bagi penyerang dengan berpura-pura menjadi sistem yang rentan.

### Tujuan Utama Honeypot:

- Menjebak dan memantau aktivitas penyerang agar dapat memahami teknik yang mereka gunakan.
- Mengalihkan perhatian penyerang dari sistem utama ke sistem yang terkontrol.
- Mengumpulkan data dan log serangan untuk analisis keamanan dan perbaikan sistem.

## HoneyPot

02

# Metode IDS

## Cara Kerja Honeypot:

- **Membuat Sistem Palsu**

- Honeypot disiapkan agar terlihat seperti sistem nyata dengan layanan yang menarik bagi peretas (misal: SSH, FTP, atau database).
- Sistem ini dapat berupa low-interaction honeypot (hanya meniru layanan sederhana) atau high-interaction honeypot (menjalankan sistem operasional penuh).

- **Menarik Perhatian Penyerang**

- Dikonfigurasi untuk meniru celah keamanan yang umum ditemukan, sehingga menarik lebih banyak serangan.

- **Memonitor dan Menganalisis Serangan**

- Semua aktivitas penyerang direkam secara detail.

Gemma Cahya H. S

# HoneyPot

02

## Jenis-Jenis Honeypot

- **Low-Interaction Honeypot**

- Meniru layanan jaringan dengan cara yang terbatas. Contoh: Honeyd, Kippo (untuk SSH).
- Kelebihan: aman dan mudah dikonfigurasi.
- Kelemahan: Terbatas dalam menangkap informasi detail dari serangan.

- **High-Interaction Honeypot**

- Menjalankan sistem operasional penuh untuk menarik serangan yang sebenarnya. Contoh: Cowrie.
- Kelebihan: Mampu menangkap serangan yang lebih kompleks dan memberikan wawasan lebih dalam.
- Kekurangan: Memerlukan sumber daya lebih besar dan sulit dikonfigurasi.

## Metode IDS

Gemma Cahya H. S

## HoneyPot

02

### Kelebihan Honeypot

- Dapat mendeteksi serangan baru dan teknik eksploitasi terbaru.
- Mengalihkan perhatian penyerang dari sistem utama.
- Membantu dalam pengembangan strategi pertahanan jaringan berdasarkan data yang dikumpulkan.

### Kelemahan Honeypot

- Harus dikonfigurasi dengan hati-hati agar tidak menjadi titik lemah yang dapat dieksloitasi oleh peretas.
- Memerlukan sumber daya tambahan untuk pengelolaan dan pemantauan.
- Tidak dapat menggantikan sistem pertahanan jaringan lainnya seperti Firewall dan IDS, tetapi hanya sebagai alat pelengkap.

## Metode IDS