Jaringan Terapan

Catatan Kuliah #11

Alauddin Maulana Hirzan, M. Kom
0607069401

Intrusion Detection System (IDS)

Intrusion Detection System (IDS)

Apa itu **Intrusion**? #1

Intrusi jaringan adalah penetrasi komputer yang tidak sah di perusahaan pengguna atau alamat di domain yang ditetapkan pengguna. Intrusi dapat bersifat pasif (di mana penetrasi diperoleh secara diam-diam dan tanpa deteksi) atau aktif (di mana perubahan pada sumber daya jaringan dilakukan).

Beberapa intrusi hanya dimaksudkan untuk memberi tahu pengguna bahwa penyusup ada di sana, mengotori situs Web pengguna dengan berbagai jenis pesan atau gambar kasar. Lainnya lebih berbahaya, berusaha untuk mengekstrak informasi penting baik satu kali atau sebagai hubungan parasit yang sedang berlangsung yang akan terus menyedot data sampai ditemukan.

Intrusion Detection System (IDS)

Apa itu **Intrusion**? #2

"Apa itu intrusi" biasanya merujuk ke penyerang mendapatkan akses tidak sah ke perangkat, jaringan, atau sistem.

- Address spoofing: Sumber serangan disembunyikan menggunakan server proxy yang dipalsukan.
- Fragmentation: Paket terfragmentasi memungkinkan penyerang melewati sistem deteksi organisasi.
- Pattern Evasion: Peretas menyesuaikan arsitektur serangan mereka untuk menghindari pola yang digunakan solusi IDS untuk menemukan ancaman.
- Coordinated Attack: Ancaman pemindaian jaringan mengalokasikan banyak host atau port ke penyerang yang berbeda.

Intrusion Detection System (IDS)

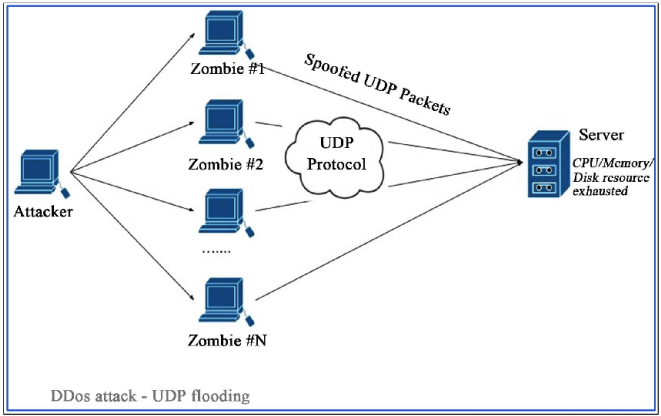
Apa itu **Intrusion**? #3

Selain itu terdapat teknik-teknik laini yang dapat dilakukan untuk melakukan Intrusion seperti:

- Multi-Routing
- Buffer Overflow Attacks
- Furtive Common Gateway Interface Scripts
- Protocol-Specific Attacks
- Traffic Flooding

Intrusion Detection System (IDS)

Apa itu **Intrusion**? #4



Intrusion Detection System (IDS)

Resiko **Intrusion** #1

Intrusi yang terjadi di jaringan dapat mengakibatkan berbagai macam hal mulai dari tingkat ringan hingga berat.

Berikut ini merupakan tingkat kerusakan yang bisa terjadi

- Perusakan Antarmuka
- Perusakan Data
- Malware
- Virus
- Worm

Intrusion Detection System (IDS)

Pencegahan Intrusion

Intrusi dapat dideteksi dan dicegah dengan menggunakan:

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

Masing-masing memiliki cara kerja dan tujuan yang berbeda. Sehingga dalam implementasinya di lingkungan server harus ditentukan terlebih dahulu.

Intrusion Detection System (IDS)

Apa itu **Intrusion Detection System**? #1

Menurut **Fortinet**:

> *Sistem deteksi intrusi (IDS) adalah aplikasi yang memantau lalu lintas jaringan dan mencari ancaman yang diketahui dan aktivitas mencurigakan atau berbahaya. IDS mengirimkan peringatan ke tim TI dan keamanan saat mendeteksi risiko dan ancaman keamanan apa pun.*

Sebagian besar solusi IDS hanya memantau dan melaporkan aktivitas dan lalu lintas yang mencurigakan saat mendeteksi anomali. Namun, beberapa dapat melangkah lebih jauh dengan mengambil tindakan saat mendeteksi aktivitas anomali, seperti memblokir lalu lintas berbahaya atau mencurigakan.

Intrusion Detection System (IDS)

Apa itu **Intrusion Detection System**? #2

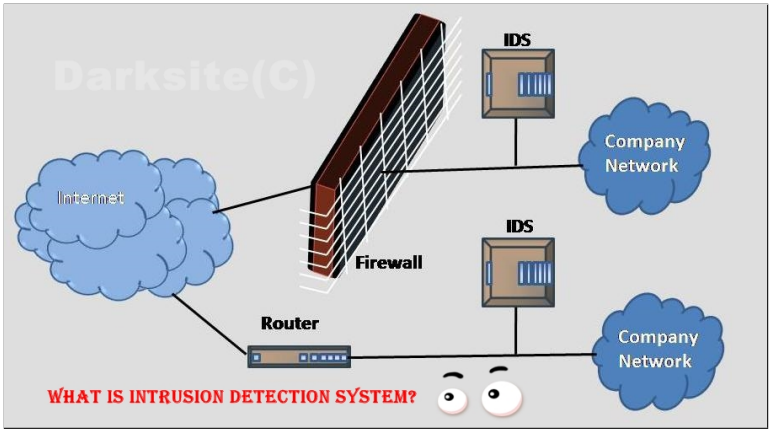
Menurut **NIST**:

> *Sistem deteksi intrusi (IDS) adalah sistem perangkat lunak atau perangkat keras yang mengotomatiskan proses pemantauan peristiwa yang terjadi dalam sistem komputer atau jaringan, menganalisis tanda-tanda masalah keamanan.*

Karena serangan jaringan telah meningkat dalam jumlah dan tingkat keparahan selama beberapa tahun terakhir, sistem deteksi intrusi telah menjadi tambahan yang diperlukan untuk infrastruktur keamanan sebagian besar organisasi.

Intrusion Detection System (IDS)

Apa itu **Intrusion Detection System**? #3



Intrusion Detection System (IDS)

Apa itu **Intrusion Detection System**? #4

IDS memiliki dua jenis, yaitu **Network Intrusion Detection System (NIDS)** dan **Host Intrusion Detection System (HIDS)**. Kedua IDS ini dipisahkan berdasarkan letak instalasi dari perangkat.

- NIDS
  - Sistem deteksi intrusi jaringan ditempatkan pada titik strategis dalam jaringan untuk memeriksa lalu lintas dari semua perangkat di jaringan.
- HIDS
  - Sistem deteksi intrusi host berjalan pada host atau perangkat yang berdiri sendiri di jaringan.

Intrusion Detection System (IDS)

Network Intrusion Detection System (NIDS) #1

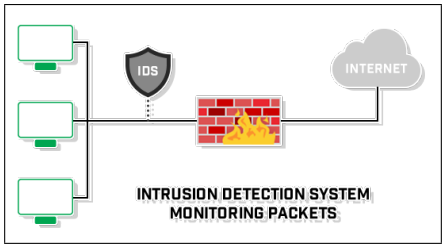
Terutama, sistem ini melakukan analisis lalu lintas yang lewat di seluruh subnet dan mencocokkan lalu lintas yang diteruskan di subnet dengan kumpulan serangan yang diketahui. Setelah mengidentifikasi serangan atau merasakan perilaku abnormal, sistem ini mengirimkan peringatan ke administrator.

Solusi NIDS diterapkan pada titik-titik strategis dalam jaringan organisasi untuk memantau lalu lintas masuk dan keluar. Pendekatan IDS ini memantau dan mendeteksi lalu lintas berbahaya dan mencurigakan yang datang dan pergi dari semua perangkat yang terhubung ke jaringan.

Intrusion Detection System (IDS)

Network Intrusion Detection System (NIDS) #2

Sistem Deteksi Intrusi Berbasis Jaringan (NIDS) memantau pola lalu lintas jaringan untuk mendeteksi aktivitas yang mencurigakan. Sensor ditempatkan di titik pemeriksaan strategis



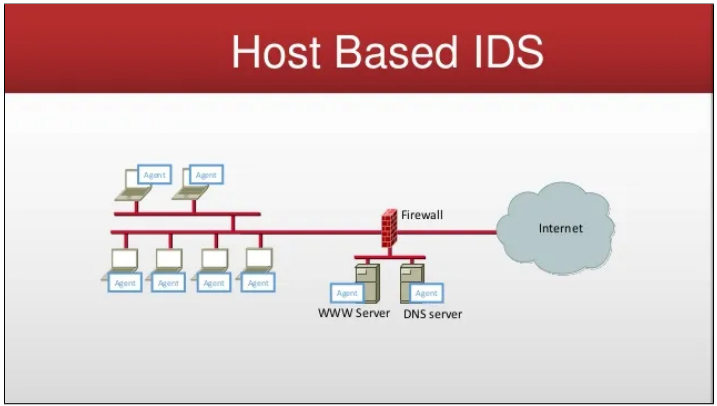
Intrusion Detection System (IDS)

Host Intrusion Detection System (HIDS) #1

Sistem HIDS diinstal pada perangkat individual yang terhubung ke internet dan jaringan internal organisasi. Solusi ini dapat mendeteksi paket yang berasal dari dalam bisnis dan lalu lintas berbahaya tambahan yang tidak dapat dilakukan oleh solusi NIDS. Itu juga dapat menemukan ancaman jahat yang datang dari host, seperti host yang terinfeksi malware yang mencoba menyebarkannya ke seluruh sistem organisasi.

Intrusion Detection System (IDS)

Host Intrusion Detection System (HIDS) #2



Intrusion Detection System (IDS)

Pro dan Kontra #1

Pro

- NIDS dapat dengan mudah digunakan ke dalam jaringan yang ada dengan sedikit gang-guan.
- NIDS dapat mendeteksi peristiwa waktu nyata, memungkinkan mereka mencatat bukti serangan yang mungkin coba dihapus oleh pelaku jahat.
- Sistem intrusi jaringan dapat menganalisis berbagai jenis dan jumlah serangan. Data yang dikumpulkan kemudian dapat digunakan untuk menerapkan kontrol keamanan yang lebih efektif dan mengidentifikasi masalah konfigurasi perangkat jaringan.
- Peningkatan visibilitas jaringan memudahkan untuk memenuhi persyaratan kepatuhan khusus untuk keamanan TI.

Intrusion Detection System (IDS)

Pro dan Kontra #2

Kontra

- Sistem deteksi intrusi jaringan hanya membantu mengungkap serangan, bukan mencegah atau menghentikannya.
- NIDS tidak dapat menganalisis paket terenkripsi.
- Sistem deteksi Intrusi Jaringan tidak dapat dengan mudah mengenali jenis serangan tertentu, misalnya, jika menggunakan paket yang terfragmentasi.
- NIDS membutuhkan administrator sistem yang berpengalaman untuk mengawasi dan memantau

Intrusion Detection System (IDS)

Bagaimana Sistem Deteksi Intrusi Bekerja #1

IDS dapat mendeteksi serangan dengan menggunakan dua cara, yaitu:

- Signature-based Detection
- Anomaly-based Detection

Masing-masing metode memiliki kelebihan serta kekurangan tersendiri dalam melindungi sistem jaringan.

Intrusion Detection System (IDS)

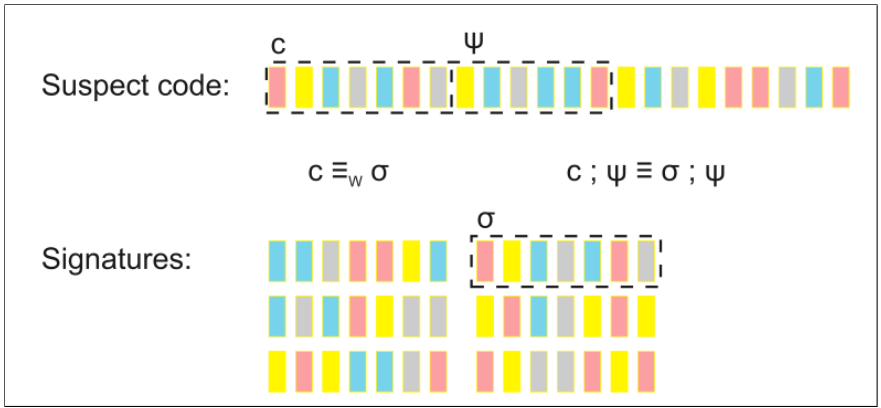
Bagaimana Sistem Deteksi Intrusi Bekerja #2

Signature-based Detection

- IDS berbasis tanda tangan mengacu pada deteksi serangan berdasarkan kriteria yang telah ditentukan sebelumnya seperti lalu lintas jaringan atau urutan instruksi berba-haya yang teridentifikasi yang umum untuk malware.
- Pola yang terdeteksi dikenal sebagai tanda tangan. IDS berbasis tanda tangan dapat dengan mudah mendeteksi pola serangan yang sudah ada atau diketahui sementara sulit untuk mendeteksi serangan baru tanpa pola yang ada.

Intrusion Detection System (IDS)

Bagaimana Sistem Deteksi Intrusi Bekerja #3



Intrusion Detection System (IDS)

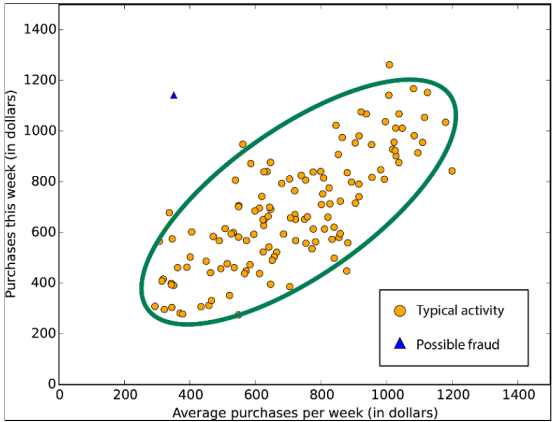
Bagaimana Sistem Deteksi Intrusi Bekerja #4

Anomaly-based Detection

- IDS berbasis anomali terutama diperkenalkan untuk mendeteksi serangan malware yang tidak diketahui, yang sebagian disebabkan oleh perkembangan pesat malware baru. Seluruh idenya adalah penggunaan pembelajaran mesin untuk membuat model aktivitas yang dapat dipercaya dan membandingkan perilaku baru dengan model tersebut.

Intrusion Detection System (IDS)

Bagaimana Sistem Deteksi Intrusi Bekerja #5



Intrusion Detection System (IDS)

Software IDS Di Pasaran

Terdapat banyak sekali NIDS yang dapat dipasang secara gratis seperti

1. Snort `https://www.snort.org` (NIDS dan HIDS)
2. Samhain `https://la-samhna.de/samhain/s_download.html` (HIDS)
3. OSSEC `https://www.ossec.net/` (HIDS)
4. Comodo Internet Security `https://www.comodo.com` (HIDS)


THANK YOU