**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 07**

**Network Risk Mitigation – Intrusion Detection**

**Intrusion Detection System**

Intrusion Detection System (IDS) adalah aplikasi perangkat lunak yang memonitor jaringan atau sistem untuk kegiatan yang berbahaya atau kegiatan intruder. Setiap kegiatan yang terdeteksi atau pelanggaran atas rule dilaporkan baik untuk administrator atau dikumpulkan secara terpusat menggunakan manajemen informasi keamanan atau security information and event management (SIEM). Sebuah sistem SIEM menggabungkan output dari berbagai sumber, dan menggunakan teknik alarm untuk melakukan penyaringan untuk membedakan aktivitas berbahaya dan false alarm.

Ada beberapa jenis IDS, yang paling umum adalah Network Intrusion detection system (NIDS) dan Host Intrusion Detection System (HIDS). Sebuah sistem yang memonitor file sistem operasi yang penting adalah contoh dari HIDS, sementara sistem yang menganalisa lalu lintas jaringan yang masuk adalah contoh dari NIDS. Ada dua cara untuk mengklasifikasikan IDS dengan pendekatan cara deteksinya, yaitu varian paling terkenal adalah berbasis signature deteksi (mengenali pola yang buruk, seperti malware) dan deteksi berbasis anomali (mendeteksi penyimpangan dari model lalu lintas "baik", yang sering bergantung pada pembelajaran mesin – machine learning). Beberapa IDS memiliki kemampuan untuk menanggapi gangguan yang terdeteksi. Sistem dengan kemampuan respon biasanya disebut sebagai sistem Intrusion Prevention System.

IDS berbeda dengan firewall, meskipun mereka berdua berhubungan dengan keamanan jaringan, Firewall berfungsi untuk menghentikan intrusi yang terjadi. Firewall membatasi akses antara jaringan untuk mencegah intrusi dan tidak menandakan serangan dari dalam jaringan. IDS mengevaluasi intrusi setelah terjadi dan mengenerate sinyal alarm. Sebuah IDS juga dapat menyampaikan alarm untuk serangan yang berasal dari dalam sistem. Teknik yang digunakan adalah memeriksa (scanning) komunikasi jaringan, mengidentifikasi heuristik dan pola (sering dikenal sebagai signature) dari serangan komputer yang sudah diketahui secara umum, dan mengambil tindakan untuk memperingatkan operator. Jika di kaji lebih dalam lagi, firewall dapat menscan atau memeriksa hanya bagian paket header nya saja, sementara itu IDS dapat memeriksa selain paket header juga dapat memeriksa payload. Sistem kerja IDS adalah menggunakan string matching artinya IDS mempunyai database yang berisi pattern atau signature dari semua mailware. Pada saat proses memeriksa payload, IDS akan mencari signature tersebut didalam payload. Apabila ditemukan signature dalam payload maka IDS akan memberikan alarm.

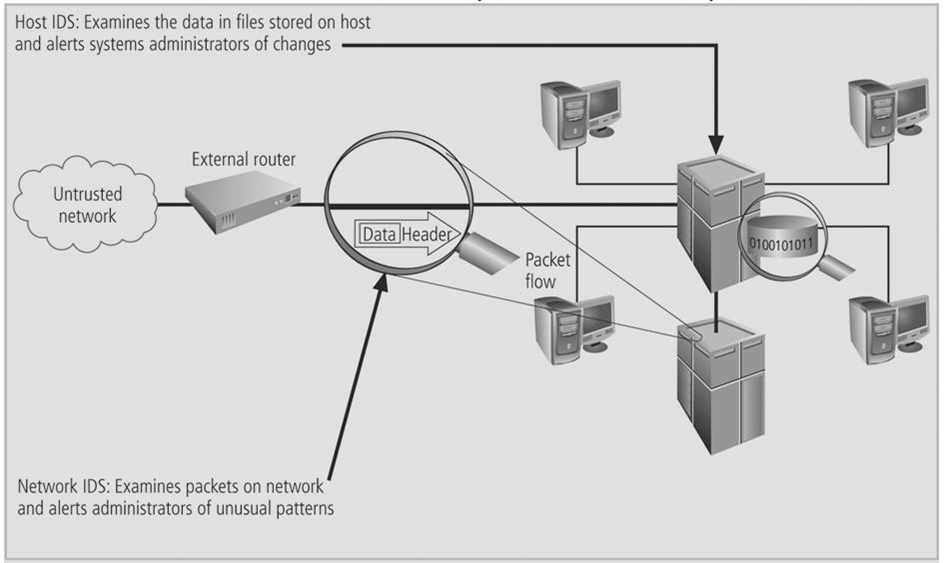
Ada berbagai macam type IDS yaitu:

• Network Intrusion Detection System (NIDS)

• Host Intrusion Detection System (HIDS)

• Application Based

• Physical IDS



Gambar 1. Network IDS dan Host IDS

Network Intrusion detection system (NIDS) ditempatkan pada titik strategis atau titik dalam jaringan untuk memonitor lalu lintas ke dan dari semua perangkat pada jaringan seperti terlihat pada gambar 1. NIDS melakukan analisis lalu lintas yang lewat di seluruh subnet. Semua trafik yang masuk ke subnet akan di periksa dan dicocokkan dengan pattern atau signature yang ada di database. Setelah serangan diidentifikasi, atau perilaku abnormal dirasakan, sebuah alert atau peringatan dikirim ke administrator. NIDS dapat di instal pada subnet dimana firewall berada. Idealnya NIDS memeriksa semua lalu lintas inbound dan outbound, namun hal itu dapat membuat bottleneck yang akan merusak kecepatan keseluruhan jaringan. Ketika kita mengklasifikasikan perancangan NIDS sesuai dengan properti sistem interaktivitas, ada dua jenis: on-line dan off-line NIDS. On-line NIDS berhubungan dengan jaringan secara real time. Ini analisis paket Ethernet dan menerapkan beberapa aturan, untuk memutuskan apakah itu adalah serangan atau tidak. Off-line NIDS berhubungan dengan data yang tersimpan dan dibagikan melalui beberapa proses untuk memutuskan apakah itu adalah serangan atau tidak.

Host Intrusion Detection System (HIDS) berjalan di individual host atau perangkat pada jaringan. Sebuah HIDS memonitor paket inbound dan outbound dari perangkat itu saja dan akan memberitahukan administrator jika aktivitas yang mencurigakan terdeteksi. Dibutuhkan snapshot dari file sistem yang ada, dan mencocokkannya dengan snapshot sebelumnya. Jika file sistem penting yang dimodifikasi atau dihapus, peringatan dikirim ke administrator untuk menyelidiki. Contoh penggunaan HIDS dapat dilihat pada mesin misi kritis, yang tidak diharapkan untuk mengubah konfigurasi mereka.

Aplikasi Based IDS adalah bagian khusus dari IDS Host-Based (HIDS) yang menganalisa peristiwa atau perubahan dalam aplikasi perangkat lunak. Sumber informasi umum untuk IDS Based Aplikasi adalah aplikasi file log transaksi. Aplikasi Based IDS memonitor interaksi antara pengguna dan aplikasi, yang merekam jejak aktivitas pengguna individu.

Physical intrusion detection adalah tindakan mengidentifikasi ancaman terhadap sistem fisik. Dalam banyak kasus Physical intrusion detection bertindak sebagai sistem pencegahan juga. Contoh deteksi intrusi fisik adalah: Penjaga keamanan, Kamera keamanan, Access Control Systems (Card, Biometric), Sensor gerak dan sebagainya.

Intrusion Prevention System (IPS) adalah teknologi pencegahan jaringan keamanan atau sebuah teknik untuk mencegah ancaman atau resiko. Hal ini dilakukan dengan meneliti traffic jaringan untuk mendeteksi dan mencegah eksploitasi kerentanan. Kerentanan eksploitasi biasanya datang dalam bentuk malicious software atau perangkat lunak yang berbahaya untuk sebuah aplikasi target atau layanan. Setelah sukses mengeksploitasi, penyerang dapat menonaktifkan aplikasi target (yang mengakibatkan keadaan denial-of-service), atau berpotensi dapat mengakses semua hak pada aplikasi tersebut. Fungsi utama dari IPS adalah untuk mengidentifikasi aktivitas berbahaya, dan mencatat informasi tentang kegiatan ini, melaporkannya dan mencoba untuk memblokir atau menghentikannya.

IPS adalah merupakan ekstensi dari IDS karena mereka berdua memantau lalu lintas jaringan dan sistem dari kegiatan atau aktivitas yang berbahaya. Perbedaan utama adalah IDS hanya menghasilkan alert atau pemberitahuan, IPS dapat melakukan tindakan selanjutnya. IPS ditempatkan in-line dan mampu secara aktif mencegah atau blok intrusi yang terdeteksi. IPS dapat mengambil tindakan seperti mengirim alarm , men-drop paket yang terdeteksi berbahaya, mengulang koneksi atau memblokir lalu lintas dari alamat IP tertentu.

**Honeypot**

Honeypot adalah sistem komputer di internet yang secara tegas diatur untuk menarik dan sebagai perangkap untuk orang-orang yang berusaha untuk menembus sistem komputer orang lain. Umumnya, honeypot terdiri dari data (misalnya, dalam sebuah situs jaringan) yang tampaknya menjadi bagian yang sah dari situs tetapi sebenarnya terisolasi dan dimonitor, dan yang tampaknya berisi informasi atau sumber daya yang berharga kepada penyerang. Hal ini mirip dengan polisi memancing penjahat dan kemudian melakukan pengawasan menyamar, dan akhirnya menghukum kriminal. Sebuah honeypot bekerja dengan membodohi penyerang menjadi percaya itu adalah sistem yang sah; mereka menyerang sistem tanpa mengetahui bahwa mereka sedang diamati secara terselubung. Ketika seorang penyerang mencoba untuk kompromi honeypot, informasi terkait serangan, seperti alamat IP dari penyerang, akan dikumpulkan. Kegiatan ini dilakukan oleh penyerang memberikan informasi berharga dan analisis teknik menyerang, memungkinkan administrator sistem untuk "melacak kembali" ke sumber serangan jika diperlukan.

Sebuah honeypot dapat digunakan untuk mitigasi risiko. Kebanyakan honeypots dapat mengemulasi sistem operasi tertentu atau service. Ini membantu untuk melindungi jaringan dan sistem terhadap serangan yang dilakukan oleh alat atau software otomatis yang bertujuan untuk secara acak mencari dan mengambil alih sistem yang rentan. Dengan menjalankan honeypot produksi, proses scanning dari alat serangan ini dapat diperlambat, sehingga membuang-buang waktu mereka. Beberapa honeypots produksi bahkan dapat mematikan serangan secara total, misalnya, denagn mengirim para penyerang paket acknowledgement dengan ukuran nol byte. Hal ini akan membuat penyerang menjadi menunggu di mana ia hanya bisa mengirim data bila ukuran jendela meningkat. Dengan cara ini, honeypots produksi sering digunakan sebagai pengintai atau sebagai alat pencegahan.

Honeypots juga dapat digunakan untuk penelitian, untuk mengetahui bagaimana cara attacker menyerang sebuah sistem. Honeypot dapat mengumpulkan informasi yang menyeluruh mengenai teknik serangan baru dan metodenya, dan karenanya memberikan gambaran yang lebih akurat dari jenis serangan yang dilakukan. Dengan ini maka dapat memberikan peningkatan informasi pencegahan serangan, deteksi dan reaksi, yang diambil dari file log dan informasi lainnya yang ditangkap selama proses penyerangan. Secara umum, lembaga penelitian honeypot seperti universitas dan departemen militer akan menjalankan honeypots penelitian untuk mengumpulkan data tentang metode serangan baru. Beberapa hasil penelitian ini dipublikasikan untuk kepentingan seluruh masyarakat.

**SIMPULAN**

1. Ada berbagai macam type IDS yaitu:

• Network Intrusion Detection System (NIDS)

• Host Intrusion Detection System (HIDS)

• Application Based

• Physical IDS

1. Honeypots dapat digunakan untuk penelitian, untuk mengetahui bagaimana cara attacker menyerang ke sebuah sistem.

**DAFTAR PUSTAKA**

1. Stallings, William. (2006). Cryptography and Network Security. 4th edition. Pearson Education.Whitman, M.E., Mattoro, H.J. (2013).
2. Scambray, Joel; Liu, Vincent; Sima, Caleb. (2011). Hacking Exposed Web Applications: Web Application Security Secrets and Solutions. 3rd Edition. McGraw-Hill. ISBN: 9780071740647.
3. Slay, Jill and Andy Koronios. (2006). Security and Risk Management. John Wiley & Sons, Inc.