Mohammad Cahyadi
09011381621065

WHITEPAPER

INTRUSION DETECTION AND PREVENTION SYSTEM

[1]Saat ini komponen keamanan jaringan yang tersedia seperti Firewall, program Anti-Virus, dan intrusion prevention system (IDS) tidak dapat mengatasi berbagai serangan berbahaya dan zero day exploits pada jaringan dan sistem komputer. Multi-exploit worm seperti Nimda, Trojan horse, dan virus polimorfik dapat menembus keamanan, menyebabkan downtime dan kerugian finansial yang sangat besar bagi bisnis. "Script kiddies" dapat membuat kode berbahaya dengan alat-alat seperti Fragrouter dan ADMutate. Pusat Koordinasi CERT (Computer Emergency Response) di Universitas Carnegie Mellon melaporkan bahwa jumlah insiden keamanan yang dilaporkan meningkat dua kali lipat setiap tahun (CERT / CC). IPS menggunakan pendekatan proaktif baru yang menghentikan peretas (black hat) sebelum mereka dapat melakukan kerusakan.

Komponen keamanan pada jaringan

1. **Intrusion detection system**

   Richard Kemmerer dan Giovanni Vigna menjelaskan, "... sistem deteksi intrusi tidak mendeteksi intrusi sama sekali - mereka hanya mengidentifikasi bukti intrusi, baik saat sedang berlangsung atau setelah fakta." IDS mengidentifikasi ancaman keamanan dengan mendeteksi pemindaian, penyelidikan, dan serangan tetapi tidak blokir pola-pola ini; alih-alih hanya melaporkan bahwa mereka terjadi. Namun data log IDS sangat berharga sebagai bukti forensik dan penanganan insiden. Ini mendeteksi serangan internal, yang tidak terlihat oleh firewall dan juga membantu dalam audit firewall.

   Tipe-tipe IDS;

   - Anomaly-based detection IDS melaporkan penyimpangan dari perilaku "normal" atau yang diharapkan. Perilaku selain "normal" dianggap sebagai serangan dan ditandai serta dicatat.
   - Misuse-based detection IDS memicu alarm ketika kecocokan ditemukan untuk "sidik jari" - signature yang terkandung dalam database signature. "Sidik jari" ini didasarkan pada seperangkat aturan yang cocok dengan pola khas eksploitasi yang digunakan oleh penyerang.
   - Network-based IDS (NIDS) berada di belakang firewall, di zona demiliterisasi (DMZ) atau jaringan pribadi dan mengendus paket dalam mode promiscuous yang tidak terlihat oleh penyerang. Ini memonitor dan menganalisis paket dan dapat menggunakan teknik deteksi anomali atau penyalahgunaan.
   - Perangkat lunak IDS (HIDS) berbasis host dijalankan pada setiap host. Perangkat lunak memonitor dan mendeteksi aktivitas dan log pengguna dan sistem operasi. Serangan pada host tertentu terdeteksi menggunakan deteksi penyalahgunaan. HIDS melihat lebih dekat dan lebih dalam pada aktivitas alat serangan pada host dan harus digunakan di Web, server DNS, dan host target.

2. **Intrusion prevention system**

   IDS dapat mengevaluasi lalu lintas yang melewati port terbuka ini tetapi tidak dapat menghentikannya. IPS dapat secara proaktif memblokir serangan. Pendekatan berbasis signature fokus pada bagaimana serangan bekerja, mencoba mendeteksi string tertentu. Jika penyerang membuat perubahan kecil dengan menggunakan teknik penghindaran

IDS yang dibahas di atas, signature yang ditulis sebelumnya tidak lagi mendeteksi serangan. IPS justru berfokus pada apa yang dilakukan serangan, yang tidak berubah.

Pendekatan IPS;

- Software based heuristic approach - This approach is similar to IDS anomaly detection using neural networks with the added ability to act against intrusions and block them.
- Kode ponsel seperti ActiveX, applet Java dan berbagai macam bahasa scripting dikarantina dalam kotak pasir - area dengan akses terbatas ke sumber daya sistem lainnya.
- Pendekatan hibrid - Pada IPS berbasis jaringan (NIPS), berbagai metode deteksi, beberapa hak milik termasuk anomali protokol, anomali lalu lintas, dan deteksi signature bekerja bersama untuk menentukan serangan yang akan terjadi dan memblokir lalu lintas yang datang dari router inline.
- Pendekatan perlindungan berbasis kernel - Digunakan pada IPS berbasis host (HIPS). Sebagian besar sistem operasi membatasi akses ke kernel oleh aplikasi pengguna. Kernel mengontrol akses ke sumber daya sistem seperti memori, perangkat I / O, dan CPU, mencegah akses pengguna langsung.

Tipe-tipe IPS;

- Host based Intrusion Prevention (HIP)

  StormENatch OKENA menggunakan pendekatan berbasis kernel dan bekerja pada server dan workstation. Kebijakan - kumpulan aturan kontrol akses yang didasarkan pada perilaku yang dapat diterima, tersedia di luar kotak untuk aplikasi umum seperti Microsoft SQL Server, Instant Messenger, dan IIS Server. Kebijakan mengontrol sumber daya apa yang digunakan, operasi apa yang diminta, dan aplikasi mana yang memintanya. StormWatch menghubungkan ke kernel dan memotong panggilan sistem (Okena).
  - File System interceptor
  - Network interceptor
  - Configuration interceptor
  - Execution space (Run-time environment) interceptor
- Network based Intrusion Prevention (NIP)
  - Deteksi Signature Stateful - Ini terlihat pada bagian lalu lintas yang relevan, di mana serangan dapat dilakukan. Ini dilakukan dengan melacak keadaan dan berdasarkan konteks yang ditentukan oleh pengguna mendeteksi serangan. Ini tidak sepenuhnya otomatis, karena pengguna perlu memiliki pengetahuan sebelumnya tentang serangan itu.
  - Deteksi anomali protokol - Semua vendor melakukan analisis paket terperinci dengan mesin decode protokol untuk memastikan paket memenuhi persyaratan protokol.

[2]Agar IPS dapat dipercaya, solusinya harus: komprehensif dalam mekanisme pemblokiran serangannya; dibuktikan di lapangan memverifikasi bahwa itu berfungsi, mudah dipasang dan digunakan; dan harus skala untuk penyebaran yang diperluas.

Pendekatan ini memberikan solusi berbasis signature terbuka yang didukung penuh yang dirancang dan dioptimalkan untuk perlindungan in-line. Sering kali, pendekatan dan arsitektur hak milik memerlukan validasi yang signifikan yang pada kenyataannya melakukan pekerjaan yang membutuhkan waktu dan usaha.

Terakhir, setiap IPS harus fleksibel dalam opsi penempatan jaringannya dan memenuhi kriteria fungsional tertentu agar efektif. Bagian berikutnya akan meninjau skenario penyebaran khas bersama dengan contoh kriteria pengujian umum yang harus ditinjau dan diverifikasi oleh evaluator sebelum berinvestasi ke dalam penawaran IPS tertentu.

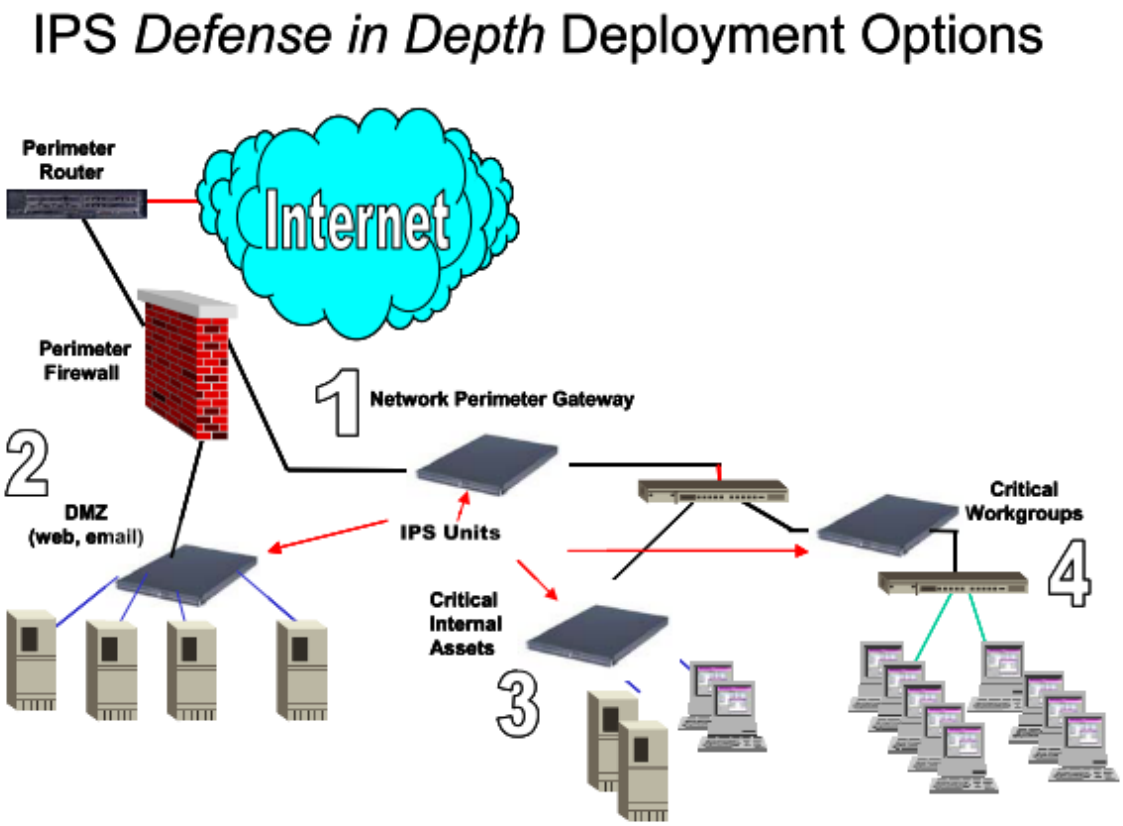

Illustration 1– Potential IPS Deployment Options

Ilustrasi 1 menunjukkan opsi penempatan IPS utama.

1. Di belakang firewall perimeter jaringan dan penghentian VPN apa pun.
2. Antara firewall perimeter jaringan dan server berbasis DMZ seperti Web dan server email
3. Di depan aset internal penting seperti server aplikasi
4. Di depan kelompok kerja departemen utama

Evaluation Criteria

IPS harus dapat melakukan fungsi-fungsi berikut:

- Menawarkan fleksibilitas dalam opsi penempatan
- Memiliki rangkaian lengkap mekanisme pemblokiran serangan yang terbukti di lapangan
- Lakukan dengan "kecepatan kawat" ketika diserang dan beban lalu lintas pengguna yang tinggi
- Opsi redundansi apa untuk ketersediaan sistem yang tinggi
- Mudah dikelola secara lokal atau jarak jauh

Deployment Options

- Penerapan In-Line dengan semua set aturan dinonaktifkan.

- Penerapan In-Line dengan semua set aturan diaktifkan untuk hanya mendeteksi secara pasif
- Penempatan In-Line dengan set aturan fitur yang diatur untuk memblokir serangan
- Port jaringan internal dan eksternal yang didedikasikan untuk isolasi lalu lintas
- Kemampuan untuk digunakan dalam berbagai topologi
- VLAN dukungan: berbasis standar (IEEE 802.1q) atau vendor khusus (Cisco ISL)

Attack Blocking Mechanisms

- Fungsi penyaringan bridge Layer 2
- Pemblokiran alamat Layer 3
- Pemblokiran berdasarkan nomor Port TCP / UDP atau kombinasi alamat IP dan Nomor Port TCP / UDP
- Memblokir serangan paket tunggal
- Memblokir serangan ICMP Flood Denial of Service
- Memblokir SYN Flood Denial of Service Serangan Service (DoS), Denial of Service (DDoS) Terdistribusi
- Memblokir komunikasi respons gema ICMP yang tidak diminta
- Memblokir paket TCP dengan format paket yang buruk, penggunaan flag
- Memblokir Fragmen IP Ilegal
- Kemampuan untuk menangani / memesan kembali segmen TCP; Fragmen IP
- Kemampuan untuk melindungi operasi internal dari penyalahgunaan yang disengaja
- Memblokir paket IP yang menggunakan pengaturan Opsi ilegal • Memblokir permintaan HTTP dengan cacat METODE
- Memblokir permintaan HTTP dengan eksploitasi buffer overflow
- Memblokir permintaan HTTP dengan eksploitasi buffer overflow ketika Eksploitasi didistribusikan di beberapa paket Eksploitasi dibuat dengan teknik penyandian yang dimodifikasi
- Memblokir lalu lintas peer to peer (P2P) yang tidak diinginkan
- Kemampuan untuk melakukan penyaringan konten keluar untuk melindungi terhadap distribusi ilegal kekayaan intelektual atau penyebaran worm / virus.
- Kemampuan untuk mendefinisikan signature khusus untuk digunakan dengan paket IP, TCP, atau UDP
- Performa
- Dampak throughput minimal pada pengaturan koneksi tinggi / tingkat teardown
- Pengaturan koneksi / tingkat teardown
- Latensi rendah di berbagai ukuran paket dan tingkat transmisi
- Memblokir serangan Denial of Service (mis. SYN Flood) seraya mempertahankan waktu respons aplikasi pengguna akhir yang dapat diterima

Mohammad Cahyadi
09011381621065

REFERENSI

[1] I. P. Systems-, “Information Security Reading Room Intrusion Prevention Systems-Security &# 39 ; s Silver Bullet ? tu ho ll r igh,” 2019.

[2] NitroGuard, “Intrusion Prevention : A White Paper Intrusion Prevention : The Business Case.”