Copyright © September 2023

PERTEMUAN 4
MELINDUNGI ORGANISASI

Bab ini mencakup beberapa teknologi dan proses yang digunakan oleh para profesional keamanan siber saat melindungi jaringan, peralatan, dan data organisasi. Pertama, secara singkat mencakup banyak jenis firewall, peralatan keamanan, dan perangkat lunak yang saat ini digunakan, termasuk praktik terbaik. Selanjutnya, bab ini menjelaskan botnet, rantai pemutusan, keamanan berbasis perilaku, dan penggunaan NetFlow untuk memantau jaringan. Bagian ketiga membahas pendekatan Cisco terhadap keamanan siber, termasuk tim CSIRT dan pedoman keamanan. Ini secara singkat mencakup alat yang digunakan oleh para profesional keamanan siber untuk mendeteksi dan mencegah serangan jaringan.

1.1. FIREWALL

1.1.1. Jenis Firewall

1. Jenis Firewall

Firewall adalah dinding atau partisi yang dirancang untuk mencegah api menyebar dari satu bagian bangunan ke bagian lain. Dalam jaringan komputer, firewall dirancang untuk mengontrol, atau menyaring, komunikasi mana yang diizinkan masuk dan mana yang diizinkan keluar dari perangkat atau jaringan, seperti yang ditunjukkan pada gambar. Firewall dapat dipasang pada satu komputer dengan tujuan untuk melindungi satu komputer tersebut (firewall berbasis host), atau dapat berupa perangkat jaringan yang berdiri sendiri yang melindungi seluruh jaringan komputer dan semua perangkat host di jaringan tersebut. (firewall berbasis jaringan). Selama bertahun-tahun, ketika serangan komputer dan jaringan menjadi lebih

Copyright © September 2023

canggih, jenis firewall baru telah dikembangkan yang melayani tujuan berbeda dalam melindungi jaringan. Berikut adalah daftar jenis firewall umum:

- Network Layer Firewall – memfilter berdasarkan alamat IP sumber dan tujuan
- Transport Layer Firewall – pemfilteran berdasarkan port data sumber dan tujuan, dan pemfilteran berdasarkan status koneksi
- Application Layer Firewall – pemfilteran berdasarkan aplikasi, program, atau layanan
- Context Aware Application Firewall – pemfilteran berdasarkan pengguna, perangkat, peran, jenis aplikasi, dan profil ancaman
- Server Proxy – memfilter permintaan konten web seperti URL, domain, media, dll.
- Reverse Proxy Server – ditempatkan di depan server web, server proxy terbalik melindungi, menyembunyikan, membongkar, dan mendistribusikan akses ke server web
- Network Address Translation (NAT) Firewall – menyembunyikan atau menyamarkan alamat pribadi host jaringan
- Firewall berbasis host – pemfilteran port dan panggilan layanan sistem pada satu sistem operasi computer.

2. Port Scanning

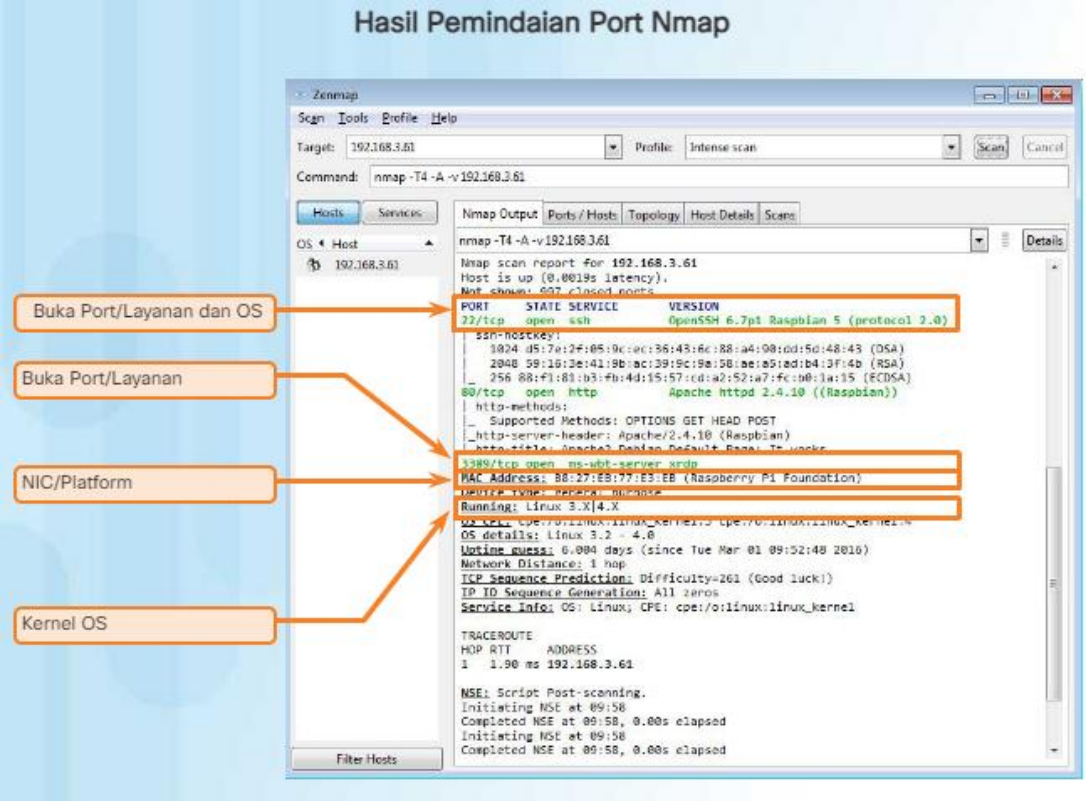
Pemindaian port adalah proses menyelidiki komputer, server, atau host jaringan lain untuk port terbuka. Dalam jaringan, setiap aplikasi yang berjalan pada perangkat diberi pengidentifikasi yang disebut nomor port. Nomor port ini digunakan di kedua ujung transmisi sehingga data yang benar diteruskan ke aplikasi yang benar. Pemindaian port dapat digunakan

secara jahat sebagai alat pengintai untuk mengidentifikasi sistem operasi dan layanan yang berjalan di komputer atau host, atau dapat digunakan secara tidak berbahaya oleh administrator jaringan untuk memverifikasi kebijakan keamanan jaringan di jaringan. Untuk tujuan mengevaluasi firewall dan keamanan port jaringan komputer Anda sendiri, Anda dapat menggunakan alat pemindai port seperti Nmap untuk menemukan semua port yang terbuka di jaringan Anda. Pemindaian port dapat dilihat sebagai awal dari serangan jaringan dan oleh karena itu tidak boleh dilakukan pada server publik di Internet, atau pada jaringan perusahaan tanpa izin. Untuk menjalankan pemindaian port Nmap komputer di jaringan rumah lokal Anda, unduh dan luncurkan program seperti Zenmap, berikan alamat IP target komputer yang ingin Anda pindai, pilih profil pemindaian default, dan tekan pindai. Pemindaian Nmap akan melaporkan semua layanan yang sedang berjalan (misalnya, layanan web, layanan email, dll.) dan nomor port. Pemindaian port umumnya menghasilkan salah satu dari tiga respons:

- Buka atau Diterima – Tuan rumah menjawab yang menunjukkan layanan mendengarkan di port.
- Ditutup, Ditolak, atau Tidak Mendengarkan – Tuan rumah menjawab yang menunjukkan bahwa koneksi akan ditolak ke port.
- Difilter, Dijatuhkan, atau Diblokir – Tidak ada balasan dari tuan rumah.

Untuk menjalankan pemindaian port jaringan Anda dari luar jaringan, Anda harus memulai pemindaian dari luar jaringan. Ini akan melibatkan menjalankan pemindaian port Nmap terhadap firewall atau alamat IP publik router Anda. Untuk menemukan alamat IP publik Anda, gunakan mesin pencari seperti Google dengan pertanyaan "apa alamat ip saya". Mesin pencari akan mengembalikan alamat IP publik Anda. Untuk menjalankan pemindaian port untuk enam port umum terhadap router rumah atau firewall Anda, buka Nmap Online Port Scanner di

https://hackertarget.com/nmap-online-port-scanner/ dan masukkan alamat IP publik Anda di input box : Alamat IP yang akan dipindai… dan tekan Quick Nmap Scan . Jika respons terbuka untuk salah satu port: 21, 22, 25, 80, 443, atau 3389 maka kemungkinan besar, penerusan port telah diaktifkan di router atau firewall Anda, dan Anda menjalankan server di jaringan pribadi Anda, seperti yang ditunjukkan dalam gambar.



Gambar 1. Port Scanner

1.1.2. Peralatan Keamanan

1. Peralatan Keamanan

Saat ini tidak ada alat keamanan tunggal atau bagian dari teknologi yang akan menyelesaikan semua kebutuhan keamanan jaringan. Karena ada berbagai peralatan dan alat keamanan yang perlu diimplementasikan, penting bagi mereka semua untuk bekerja sama.

Copyright © September 2023

Peralatan keamanan paling efektif ketika mereka adalah bagian dari suatu sistem. Peralatan keamanan dapat berupa perangkat yang berdiri sendiri, seperti router atau firewall, kartu yang dapat dipasang ke perangkat jaringan, atau modul dengan prosesor dan memori cache-nya sendiri. Peralatan keamanan juga dapat berupa perangkat lunak yang dijalankan pada perangkat jaringan. Peralatan keamanan termasuk dalam kategori umum ini:

a. Router

   router Cisco Integrated Services Router (ISR), yang ditunjukkan pada Gambar 1, memiliki banyak kemampuan firewall selain hanya fungsi perutean, termasuk penyaringan lalu lintas, kemampuan untuk menjalankan Intrusion Prevention System (IPS), enkripsi, dan kemampuan VPN untuk tunneling terenkripsi yang aman .

b. Firewall

   Cisco Next Generation Firewalls memiliki semua kemampuan router ISR, serta manajemen jaringan dan analitik yang canggih. Cisco Adaptive Security Appliance (ASA) dengan kemampuan firewall ditunjukkan pada Gambar 2.

c. IPS

   Perangkat IPS Cisco Next Generation, yang ditunjukkan pada Gambar 3, didedikasikan untuk pencegahan intrusi.

d. VPN

   Peralatan keamanan Cisco dilengkapi dengan server dan teknologi klien Virtual Private Network (VPN). Ini dirancang untuk tunneling terenkripsi yang aman.

e. Malware/Antivirus

Copyright © September 2023

Cisco Advanced Malware Protection (AMP) hadir di router Cisco generasi berikutnya, firewall, perangkat IPS, Peralatan Keamanan Web dan Email dan juga dapat diinstal sebagai perangkat lunak di komputer host.

f. Perangkat Keamanan Lainnya

Kategori ini mencakup peralatan keamanan web dan email, perangkat dekripsi, server kontrol akses klien, dan sistem manajemen keamanan.

1.1.3. Mendeteksi Serangan Secara Real Time

1. Mendeteksi Serangan Secara Real Time

Perangkat lunak tidak sempurna. Ketika seorang peretas mengeksploitasi cacat pada perangkat lunak sebelum pembuatnya dapat memperbaikinya, itu dikenal sebagai serangan zero-day. Karena kecanggihan dan besarnya serangan zero-day yang ditemukan saat ini, menjadi umum bahwa serangan jaringan akan berhasil dan bahwa pertahanan yang berhasil sekarang diukur dalam seberapa cepat jaringan dapat merespons serangan. Kemampuan untuk mendeteksi serangan saat terjadi secara real-time, serta menghentikan serangan dengan segera, atau dalam beberapa menit setelah terjadi, adalah tujuan yang ideal. Sayangnya, banyak perusahaan dan organisasi saat ini tidak dapat mendeteksi serangan hingga berhari-hari atau bahkan berbulan-bulan setelah serangan itu terjadi.

- Real Time Scanning from Edge to Endpoint- Mendeteksi serangan secara waktu nyata memerlukan pemindaian aktif terhadap serangan menggunakan firewall dan perangkat jaringan IDS/IPS. Deteksi malware klien/server generasi berikutnya dengan koneksi ke pusat ancaman global online juga harus digunakan. Saat ini, perangkat dan perangkat lunak pemindaian aktif harus mendeteksi anomali jaringan menggunakan analisis berbasis konteks dan deteksi perilaku.

Copyright © September 2023

- DDoS Attacks and Real Time Response- DDoS adalah salah satu ancaman serangan terbesar yang membutuhkan respons dan deteksi waktu nyata. Serangan DDoS sangat sulit untuk dipertahankan karena serangan berasal dari ratusan, atau ribuan host zombie, dan serangan tersebut muncul sebagai lalu lintas yang sah, seperti yang ditunjukkan pada gambar. Bagi banyak perusahaan dan organisasi, serangan DDoS yang terjadi secara teratur melumpuhkan server Internet dan ketersediaan jaringan. Kemampuan untuk mendeteksi dan merespons serangan DDoS secara real-time sangat penting.

1.1.4. Deteksi Malware

1. Melindungi terhadap Malware

Bagaimana Anda memberikan pertahanan terhadap kehadiran konstan serangan zero-day, serta ancaman persisten tingkat lanjut (APT) yang mencuri data dalam jangka waktu yang lama? Salah satu solusinya adalah dengan menggunakan solusi deteksi malware tingkat perusahaan yang menawarkan deteksi malware secara real-time. Administrator jaringan harus terus memantau jaringan untuk tanda-tanda malware atau perilaku yang mengungkapkan keberadaan APT. Cisco memiliki Advanced Malware Protection (AMP) Threat Grid yang menganalisis jutaan file dan menghubungkannya dengan ratusan juta artefak malware lainnya yang dianalisis. Ini memberikan pandangan global tentang serangan malware, kampanye, dan distribusinya. AMP adalah perangkat lunak klien/server yang digunakan pada titik akhir host, sebagai server mandiri, atau pada perangkat keamanan jaringan lainnya. Gambar tersebut menunjukkan manfaat dari AMP Threat Grid.

1.1.5. Praktik Keamanan Terbaik

Copyright © September 2023

Banyak organisasi nasional dan profesional telah menerbitkan daftar praktik terbaik keamanan. Berikut adalah daftar beberapa praktik terbaik keamanan:

- Lakukan Penilaian Risiko – Mengetahui nilai dari apa yang Anda lindungi akan membantu dalam membenarkan pengeluaran keamanan.
- Buat Kebijakan Keamanan – Buat kebijakan yang secara jelas menguraikan aturan perusahaan, tugas pekerjaan, dan harapan.
- Tindakan Keamanan Fisik – Batasi akses ke lemari jaringan, lokasi server, serta pemadaman kebakaran.
- Tindakan Keamanan Sumber Daya Manusia – Karyawan harus diteliti dengan baik dengan pemeriksaan latar belakang.
- Lakukan dan Uji Cadangan – Lakukan pencadangan rutin dan uji pemulihan data dari pencadangan.
- Pertahankan Patch dan Pembaruan Keamanan – Perbarui sistem dan program operasi perangkat server, klien, dan jaringan secara teratur.
- Gunakan Kontrol Akses – Konfigurasikan peran pengguna dan tingkat hak istimewa serta otentikasi pengguna yang kuat.
- Uji Respons Insiden Secara Teratur – Mempekerjakan tim respons insiden dan menguji skenario tanggap darurat.
- Menerapkan Alat Pemantauan, Analisis, dan Manajemen Jaringan - Pilih solusi pemantauan keamanan yang terintegrasi dengan teknologi lain.
- Implementasikan Perangkat Keamanan Jaringan – Gunakan router generasi berikutnya, firewall, dan peralatan keamanan lainnya.

Copyright © September 2023

- Menerapkan Solusi Keamanan Titik Akhir yang Komprehensif – Gunakan perangkat lunak antimalware dan antivirus tingkat perusahaan.
- Mendidik Pengguna – Mendidik pengguna dan karyawan dalam prosedur yang aman.
- Enkripsi data – Enkripsi semua data sensitif perusahaan termasuk email.

Beberapa panduan yang paling membantu dapat ditemukan di repositori organisasi seperti Pusat Sumber Daya Keamanan Komputer Institut Nasional Standar dan Teknologi (NIST), seperti yang ditunjukkan pada gambar. Salah satu organisasi yang paling dikenal dan dihormati untuk pelatihan keamanan siber adalah SANS Institute.

1.2. Pendekatan Prilaku Untuk Keamana Cyber

1.2.1. Botnet

Botnet adalah sekelompok bot, terhubung melalui Internet, dengan kemampuan untuk dikendalikan oleh individu atau kelompok jahat. Komputer bot biasanya terinfeksi dengan mengunjungi situs web, membuka lampiran email, atau membuka file media yang terinfeksi. Sebuah botnet dapat memiliki puluhan ribu, atau bahkan ratusan ribu bot. Bot ini dapat diaktifkan untuk mendistribusikan malware, meluncurkan serangan DDoS, mendistribusikan email spam, atau melakukan serangan brute force password. Botnet biasanya dikendalikan melalui server perintah dan kontrol. Penjahat dunia maya akan sering menyewakan Botnet, dengan biaya tertentu, kepada pihak ketiga untuk tujuan jahat. Gambar tersebut menunjukkan bagaimana filter lalu lintas botnet digunakan untuk memberi tahu komunitas keamanan di seluruh dunia tentang lokasi botnet.

1.2.2. Kill Chain

1. **The Kill Chain Pada Cyberdefense**

Copyright © September 2023

Dalam keamanan siber, Kill Chain adalah tahapan serangan sistem informasi. Dikembangkan oleh Lockheed Martin sebagai kerangka kerja keamanan untuk deteksi dan respons insiden, Cyber Kill Chain terdiri dari tahapan berikut:

- Tahap 1. Pengintaian - Penyerang mengumpulkan informasi tentang target.
- Tahap 2. Persenjataan - Penyerang membuat eksploitasi dan muatan berbahaya untuk dikirim ke target.
- Tahap 3. Pengiriman - Penyerang mengirimkan eksploitasi dan muatan berbahaya ke target melalui email atau metode lain.
- Tahap 4. Eksploitasi - Eksploitasi dijalankan.
- Tahap 5 Instalasi - Malware dan backdoors dipasang pada target.
- Tahap 6. Komando dan Kontrol - Kontrol jarak jauh dari target diperoleh melalui saluran atau server perintah dan kontrol.
- Tahap 7. Tindakan - Penyerang melakukan tindakan jahat seperti pencurian informasi, atau melakukan serangan tambahan pada perangkat lain dari dalam jaringan dengan bekerja melalui tahapan Rantai Pembunuhan lagi.

Untuk bertahan melawan Kill Chain, pertahanan keamanan jaringan dirancang di sekitar tahapan Kill Chain. Berikut adalah beberapa pertanyaan tentang pertahanan keamanan perusahaan, berdasarkan Cyber Kill Chain:

- Apa saja indikator serangan di setiap tahap Kill Chain?
- Alat keamanan apa yang diperlukan untuk mendeteksi indikator serangan di setiap tahapan?
- Apakah ada celah dalam kemampuan perusahaan untuk mendeteksi serangan?

Menurut Lockheed Martin, memahami tahapan Kill Chain memungkinkan mereka memasang rintangan defensif, memperlambat serangan, dan pada akhirnya mencegah hilangnya data. Gambar tersebut menunjukkan bagaimana setiap tahap dari Rantai Pembunuhan setara dengan peningkatan jumlah upaya dan biaya untuk menghambat dan memulihkan serangan.

1.1.3. Behavior – Based Security

Behavior – Based Security atau Keamanan berbasis perilaku adalah bentuk deteksi ancaman yang tidak bergantung pada tanda tangan berbahaya yang diketahui, tetapi menggunakan konteks informasi untuk mendeteksi anomali dalam jaringan. Deteksi berbasis perilaku melibatkan menangkap dan menganalisis aliran komunikasi antara pengguna di jaringan lokal dan lokal, atau tujuan jarak jauh. Komunikasi ini, ketika ditangkap dan dianalisis, mengungkapkan konteks dan pola perilaku yang dapat digunakan untuk mendeteksi anomali. Deteksi berbasis perilaku dapat menemukan adanya serangan dengan perubahan dari perilaku normal.

- Honeypots - Honeypot adalah alat deteksi berbasis perilaku yang pertama-tama memikat penyerang dengan menarik pola perilaku jahat yang diprediksi penyerang, dan kemudian, ketika berada di dalam honeypot, administrator jaringan dapat menangkap, mencatat, dan menganalisis perilaku penyerang. Hal ini memungkinkan administrator untuk mendapatkan lebih banyak pengetahuan dan membangun pertahanan yang lebih baik.
- Cisco’s Cyber Threat Defense Solution Architecture – Ini adalah arsitektur keamanan yang menggunakan deteksi dan 11ontrol11r berbasis perilaku, untuk memberikan visibilitas, konteks, dan 11ontrol yang lebih besar. Tujuannya adalah untuk mengetahui

Copyright © September 2023

siapa, apa, di mana, kapan, dan bagaimana serangan terjadi. Arsitektur keamanan ini menggunakan banyak teknologi keamanan untuk mencapai tujuan ini.

1.1.4. Netflow dan Serangan Cyber

1. Netflow

Teknologi NetFlow digunakan untuk mengumpulkan informasi tentang data yang mengalir melalui jaringan. Informasi NetFlow dapat disamakan dengan tagihan telepon untuk lalu lintas jaringan Anda. Ini menunjukkan kepada Anda siapa dan perangkat apa yang ada di jaringan Anda, serta kapan dan bagaimana pengguna dan perangkat mengakses jaringan Anda. NetFlow adalah komponen penting dalam deteksi dan analisis berbasis perilaku. Switch, router, dan firewall yang dilengkapi dengan NetFlow dapat melaporkan informasi tentang data yang masuk, keluar, dan berjalan melalui jaringan. Informasi dikirim ke Kolektor NetFlow yang mengumpulkan, menyimpan, dan menganalisis catatan NetFlow. NetFlow mampu mengumpulkan informasi tentang penggunaan melalui banyak karakteristik berbeda tentang bagaimana data dipindahkan melalui jaringan, seperti yang ditunjukkan pada gambar. Dengan mengumpulkan informasi tentang aliran data jaringan, NetFlow mampu membangun perilaku dasar pada lebih dari 90 atribut yang berbeda.

1.3.Pendekatan Cisco Untuk keamanan Cyber

Copyright © September 2023

1.3.1. CSIRT

Banyak organisasi besar memiliki Computer Security Incident Response Team (CSIRT) untuk menerima, meninjau, dan menanggapi laporan insiden keamanan komputer, seperti yang ditunjukkan pada Gambar 1. Misi utama CSIRT adalah membantu memastikan perusahaan, sistem, dan pelestarian data dengan melakukan investigasi komprehensif terhadap insiden keamanan komputer. Untuk mencegah insiden keamanan, Cisco CSIRT menyediakan penilaian ancaman proaktif, perencanaan mitigasi, analisis tren insiden, dan tinjauan arsitektur keamanan, seperti yang ditunjukkan pada Gambar 2. CSIRT Cisco bekerja sama dengan Forum of Incident Response and Security Teams (FIRST), National Safety Information Exchange (NSIE), Defense Security Information Exchange (DSIE), dan DNS Operations Analysis and Research Center (DNS-OARC). Ada organisasi CSIRT nasional dan publik seperti Divisi CERT dari Institut Rekayasa Perangkat Lunak di Universitas Carnegie Mellon, yang tersedia untuk membantu organisasi, dan CSIRT nasional, mengembangkan, mengoperasikan, dan meningkatkan kemampuan manajemen insiden mereka.

1.3.2. Buku Panduan Keamanan

Teknologi terus berubah. Itu berarti serangan siber juga berkembang. Kerentanan baru dan metode serangan ditemukan terus menerus. Keamanan menjadi perhatian bisnis yang signifikan karena reputasi yang dihasilkan dan dampak keuangan dari pelanggaran keamanan. Serangan menargetkan jaringan penting dan data sensitif. Organisasi harus memiliki rencana untuk mempersiapkan, menangani, dan memulihkan dari pelanggaran. Salah satu cara terbaik untuk mempersiapkan pelanggaran keamanan adalah dengan mencegahnya. Harus ada panduan untuk mengidentifikasi risiko keamanan siber terhadap sistem, aset, data, dan kemampuan,

Copyright © September 2023

melindungi sistem dengan penerapan perlindungan dan pelatihan personel, dan mendeteksi kejadian keamanan siber sesegera mungkin. Ketika pelanggaran keamanan terdeteksi, tindakan yang tepat harus diambil untuk meminimalkan dampak dan kerusakannya. Rencana respons harus fleksibel dengan beberapa opsi tindakan selama pelanggaran. Setelah pelanggaran tersebut diatasi dan sistem dan layanan yang dikompromikan dipulihkan, langkah-langkah dan proses keamanan harus diperbarui untuk memasukkan pelajaran yang didapat selama pelanggaran. Semua informasi ini harus dikompilasi ke dalam buku pedoman keamanan. Buku pedoman keamanan adalah kumpulan kueri (laporan) berulang terhadap sumber data peristiwa keamanan yang mengarah pada deteksi dan respons insiden. Idealnya buku pedoman keamanan harus melakukan tindakan berikut:

- Mendeteksi mesin yang terinfeksi malware.
- Mendeteksi aktivitas jaringan yang mencurigakan.
- Deteksi upaya otentikasi yang tidak teratur.
- Menjelaskan dan memahami lalu lintas masuk dan keluar.
- Memberikan informasi ringkasan termasuk tren, statistik, dan hitungan.
- Menyediakan akses yang dapat digunakan dan cepat ke statistik dan metrik. Menghubungkan peristiwa di semua sumber data yang relevan.

1.3.3. Alat Untuk Pencegahan dan Deteksi Insiden

Ini adalah beberapa alat yang digunakan untuk mendeteksi dan mencegah insiden keamanan:

- SIEM – Sistem Informasi Keamanan dan Manajemen Peristiwa (SIEM) adalah perangkat lunak yang mengumpulkan dan menganalisis peringatan keamanan, log, dan data real time dan historis lainnya dari perangkat keamanan di jaringan.

Copyright © September 2023

- DLP – Data Loss Prevention Software (DLP) adalah perangkat lunak atau sistem perangkat keras yang dirancang untuk menghentikan data sensitif dicuri dari atau keluar dari jaringan. Sistem DLP dapat fokus pada otorisasi akses file, pertukaran data, penyalinan data, pemantauan aktivitas pengguna, dan banyak lagi. Sistem DLP dirancang untuk memantau dan melindungi data dalam tiga status berbeda: data sedang digunakan, data bergerak, dan data tidak aktif. Data yang digunakan difokuskan pada klien, data yang bergerak mengacu pada data saat berjalan melalui jaringan, dan data saat istirahat mengacu pada penyimpanan data.
- Cisco ISE dan TrustSec – Cisco Identity Services Engine (Cisco ISE) dan Cisco TrustSec memberlakukan akses ke sumber daya jaringan dengan membuat kebijakan kontrol akses berbasis peran yang membagi akses ke jaringan (tamu, pengguna ponsel, karyawan) tanpa kerumitan tambahan. Klasifikasi lalu lintas didasarkan pada identitas pengguna atau perangkat..

1.3.4. IDS dan IPS

An Intrusion Detection System (IDS), yang ditunjukkan pada gambar, adalah perangkat jaringan khusus, atau salah satu dari beberapa alat di server atau firewall yang memindai data terhadap database aturan atau tanda tangan serangan, mencari lalu lintas berbahaya. Jika kecocokan terdeteksi, IDS akan mencatat deteksi, dan membuat peringatan untuk administrator jaringan. Intrusion Detection System tidak mengambil tindakan saat kecocokan terdeteksi sehingga tidak mencegah terjadinya serangan. Tugas IDS hanyalah mendeteksi, mencatat, dan melaporkan. Pemindaian yang dilakukan oleh IDS memperlambat jaringan (dikenal sebagai latensi). Untuk mencegah penundaan jaringan, IDS biasanya ditempatkan offline, terpisah dari lalu lintas jaringan biasa. Data disalin atau dicerminkan oleh sakelar dan kemudian diteruskan

Copyright © September 2023

ke IDS untuk deteksi offline. Ada juga alat IDS yang dapat diinstal di atas sistem operasi komputer host, seperti Linux atau Windows. An Intrusion Prevention System (IPS) memiliki kemampuan untuk memblokir atau menolak lalu lintas berdasarkan aturan positif atau kecocokan tanda tangan. Salah satu sistem IPS/IDS yang paling terkenal adalah Snort. Versi komersial dari Snort adalah Cisco's Sourcefire. Sourcefire memiliki kemampuan untuk melakukan analisis port dan lalu lintas real-time, logging, pencarian dan pencocokan konten, dan dapat mendeteksi probe, serangan, dan pemindaian port. Ini juga terintegrasi dengan alat pihak ketiga lainnya untuk pelaporan, kinerja, dan analisis log.