Tugas 4 Makassar, 4 Juni 2023

# KEAMANAN JARINGAN



Nama : Arif Rahman

Nim : 13020200034

Kelas : C2

Dosen Pengampu : Ramdan Satra, S.Kom., M.Kom., MTA

# PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS ILMU KOMPUTER UNIVERSITAS MUSLIM INDONESIA MAKASSAR

**2023**

B I

## Pertemuan 8

Rangkuman:

SSL (Secure Socket Layer) adalah protokol yang digunakan untuk membangun koneksi aman antara web server dan client atau antara mail server dan mail client. SSL menggunakan enkripsi untuk melindungi informasi sensitif yang ditransmisikan, seperti data kartu kredit, username, dan password. Setiap kali pengunjung mengakses situs dengan SSL, tercipta koneksi terenkripsi antara browser dan server.

Terdapat dua jenis sertifikat SSL, yaitu Self Signed Certificate dan Trusted Certificate Authority. Self Signed Certificate dapat dibuat secara gratis oleh pengguna, tetapi sertifikat ini tidak diakui secara resmi oleh otoritas terpercaya. Jika sebuah website menggunakan Self Signed Certificate, biasanya akan muncul peringatan pada browser. Trusted Certificate Authority adalah sertifikat yang diterbitkan oleh lembaga otoritas terpercaya setelah proses verifikasi. Sertifikat ini harus dibeli dan dipasang di web server untuk membangun kepercayaan dari browser.

Proses pembangunan koneksi SSL melibatkan pertukaran kunci kriptografi antara server dan browser. Server menyediakan SSL Certificate yang berisi Public Key, sedangkan browser memvalidasi keabsahan sertifikat tersebut. Browser kemudian membuat Symmetric Encryption key (session key) dan mengenkripsi session key dengan Public Key yang ada di dalam sertifikat. Server mendekripsi data yang dikirim oleh browser menggunakan Private Key dan menggunakan session key untuk mengirim data terenkripsi ke browser. Dengan demikian, koneksi SSL terbentuk dan data dapat dikirim secara aman antara server dan browser.

# BAB II

## Pertemuan 9

Rangkuman:

Intrusion Detection System (IDS) adalah perangkat atau aplikasi yang memonitor jaringan dan sistem untuk mendeteksi kegiatan berbahaya atau pelanggaran kebijakan. IDS melakukan pencarian, penelitian, dan pelaporan terhadap tindakan yang tidak sah atau berpotensi membahayakan aktivitas jaringan atau komputer.

Intrusion Prevention Systems (IPS) adalah sistem keamanan jaringan yang memantau aktivitas jaringan dan sistem untuk mengidentifikasi aktivitas berbahaya. IPS berfungsi mengidentifikasi aktivitas yang berpotensi berbahaya, mencatat informasinya, mencoba untuk mencegah atau menghentikannya, dan melaporkannya.

Ada dua jenis utama IDS, yaitu Network-based IDS (NIDS) dan Host-based IDS (HIDS). NIDS ditempatkan pada titik pintu gerbang jaringan dan menganalisis lalu lintas jaringan, sedangkan HIDS menggunakan perangkat lunak agen yang dipasang pada host untuk memonitor aktivitas di dalamnya. IDS dapat bersifat pasif, hanya memberikan laporan, atau reaktif (IPS), yang merespons dan mencoba menghentikan aktivitas yang mencurigakan. IDS penting sebagai pelengkap sistem keamanan lainnya untuk mendeteksi ancaman yang tidak dapat diatasi oleh firewall dan ancaman internal dalam jaringan.

# BAB III

## Pertemuan 10

Rangkuman:

Jenis-jenis serangan jaringan komputer meliputi spoofing, denial-of-service attacks (DoS), ping of death, sniffer, DNS poisoning, Trojan horse, SQL injection, PHP injection, dan script kiddies. Spoofing merupakan teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi dengan memalsukan identitas yang dapat dipercaya. Beberapa jenis spoofing meliputi IP spoofing, DNS spoofing, dan identity spoofing. DoS adalah serangan yang bertujuan menghabiskan sumber daya komputer atau server sehingga tidak dapat berfungsi dengan benar, sehingga menghentikan akses layanan bagi pengguna lain. Serangan ini dapat dilakukan dengan flooding traffic, flooding request, atau mengganggu komunikasi antara host dan klien. Serangan DoS yang lebih canggih disebut sebagai distributed denial-of-service (DDoS), yang melibatkan banyak host penyerang untuk menyerang satu host target.

Ping of death adalah serangan yang melibatkan pengiriman ping yang berbahaya atau berukuran besar ke komputer target, yang dapat menyebabkan kerusakan atau crash pada komputer tersebut. Sniffer atau packet sniffer adalah aplikasi yang digunakan untuk melihat lalu lintas data dalam jaringan komputer. Sniffer dapat digunakan untuk tujuan troubleshooting jaringan, mendeteksi penyelundup dalam jaringan, memantau penggunaan jaringan, serta memata-matai pengguna jaringan lain. DNS poisoning merupakan teknik yang memanipulasi server DNS agar mengarahkan lalu lintas paket data ke server palsu yang dibuat menyerupai server asli, dengan tujuan mengumpulkan informasi pribadi pengguna atau melakukan serangan phishing.

Trojan horse atau kuda Troya adalah bentuk perangkat lunak jahat yang dapat merusak sistem atau jaringan. Trojan bertujuan untuk memperoleh informasi dari target dan mengendalikan target dengan mendapatkan hak akses ke sistem. Trojan berbeda dengan virus komputer atau worm karena bersifat stealth (siluman) dalam operasinya dan sering kali menyamar sebagai program yang baik-baik. Trojan dapat disebarkan melalui berkas yang dieksekusi, seringkali dengan nama yang menarik untuk menarik pengguna untuk menjalankannya. Trojan dapat digunakan untuk mencuri data penting pengguna seperti password atau melakukan pengacakan sistem yang terinfeksi.

# BAB IV

## Pertemuan 11

Rangkuman:

VPN (Virtual Private Network) adalah teknologi komunikasi yang memungkinkan pengguna terhubung ke jaringan publik dan bergabung dengan jaringan lokal dengan hak dan pengaturan yang sama seperti berada dalam jaringan lokal (LAN) sendiri. Hal ini memungkinkan pengguna untuk mengakses jaringan perusahaan atau sumber daya yang terbatas dengan aman melalui koneksi internet. VPN memiliki beberapa fungsi utama, termasuk kerahasiaan data dengan mengenkripsi semua data yang lewat melalui jaringan, menjaga keutuhan data selama perjalanan melalui internet, dan melakukan autentikasi terhadap sumber data yang dikirim untuk memastikan asal dan keaslian data.

Penerapan VPN umumnya dilakukan karena beberapa alasan. Dari perspektif jaringan, VPN membantu mengatasi masalah keamanan yang tidak memadai dalam jaringan internet publik, sementara dari perspektif perusahaan, VPN menjadi kebutuhan dasar untuk pertukaran data antara kantor cabang atau rekanan perusahaan. Dengan menggunakan VPN, perusahaan dapat membangun jaringan yang aman dengan pengamanan transmisi data di atas infrastruktur IP yang ada, menjaga kerahasiaan, keutuhan, dan autentikasi data yang dikirim melalui jaringan.

Keuntungan menggunakan VPN termasuk kemampuan akses jarak jauh (remote access) yang memungkinkan pengguna mengakses komputer atau jaringan kantor dari mana saja selama terhubung ke internet, meningkatkan keamanan saat mengakses internet publik atau hotspot, serta menghemat biaya setup jaringan dengan memanfaatkan infrastruktur jaringan internet atau publik yang sudah ada. Namun, penting juga untuk memperhatikan aspek keamanan dalam penggunaan VPN dan menjaga sistem keamanan yang tepat.

Dalam keamanan jaringan, VPN memiliki peran penting. VPN membantu mengidentifikasi pengguna yang memiliki akses ke jaringan, meningkatkan keamanan melalui enkripsi data, dan tidak terlihat pada jaringan yang lebih besar. Selain itu, VPN juga mendukung mobilitas dengan menyediakan koneksi ke jaringan Wi-Fi dan nirkabel pribadi. Meskipun VPN memiliki kelebihan seperti solusi biaya efektif untuk organisasi besar dan meningkatkan mobilitas, juga ada kekurangan yang perlu diperhatikan, seperti risiko keamanan global dengan akses karyawan, dan perlunya perhatian ekstra terhadap sistem keamanan yang jelas.

# BAB V

## Pertemuan 12

Rangkuman:

Audit keamanan jaringan melibatkan penentuan ruang lingkup audit, seperti perangkat keras, perangkat lunak, dan aspek manusia. Selanjutnya, menentukan ancaman seperti tren keamanan cyber dan kepatuhan hukum. Evaluasi sikap keamanan dilakukan melalui pemantauan jaringan, pembaruan perangkat lunak, dan kesadaran karyawan. Respons otomatis dan tindakan remediasi, seperti pembaruan perangkat lunak, backup data, dan pendidikan karyawan, penting dalam menjaga keamanan jaringan.

Audit keamanan jaringan melibatkan penentuan ruang lingkup audit, ancaman seperti tren keamanan cyber dan kepatuhan hukum, serta evaluasi sikap keamanan melalui pemantauan jaringan, pembaruan perangkat lunak, dan kesadaran karyawan. Respons otomatis dan tindakan remediasi, seperti pembaruan perangkat lunak, backup data, dan pendidikan karyawan, penting dalam menjaga keamanan jaringan.

Audit keamanan jaringan melibatkan penentuan ruang lingkup audit (perangkat keras, perangkat lunak, dan aspek manusia), identifikasi ancaman (tren keamanan cyber, kepatuhan hukum, dan riwayat serangan), serta evaluasi sikap keamanan melalui pemantauan jaringan, pembaruan perangkat lunak, dan kesadaran karyawan. Respons otomatis dan tindakan remediasi (pembaruan perangkat lunak, backup data, dan pendidikan karyawan) menjadi penting dalam menjaga keamanan jaringan.

# BAB VI

## Pertemuan 13

Rangkuman:

Standar keamanan jaringan merupakan panduan penting untuk menjaga keamanan infrastruktur jaringan suatu organisasi. Dalam standar ini, terdapat beberapa poin kunci yang harus diperhatikan. Pertama, penggunaan konfigurasi yang aman dan hanya mengaktifkan layanan yang penting. Hal ini membantu mengurangi potensi serangan dan meminimalkan celah keamanan. Kedua, proses kontrol perubahan harus diimplementasikan secara ketat untuk menghindari perubahan konfigurasi yang tidak diotorisasi dan berpotensi membuka celah keamanan. Terakhir, pemantauan dan pencatatan harus dilakukan secara rutin untuk mendeteksi kejadian kebobolan keamanan dan melacak perubahan konfigurasi yang dilakukan.

Selanjutnya, dalam standar keamanan jaringan juga ditekankan pentingnya perbaikan perangkat lunak yang bermasalah. Identifikasi dan perbaikan kerentanan perangkat lunak yang dilakukan dengan menggunakan patch keamanan yang disediakan oleh vendor menjadi langkah penting dalam menjaga keamanan jaringan. Selain itu, penggunaan perangkat lunak dan firmware yang masih didukung oleh vendor juga merupakan aspek penting dalam standar ini. Hal ini membantu memastikan bahwa perangkat jaringan tetap diperbarui dan mendapatkan dukungan keamanan yang diperlukan.

Terakhir, standar keamanan jaringan juga menekankan pada pentingnya deteksi akses yang tidak sah dan pengamanan jaringan nirkabel. Melalui pemantauan jaringan, organisasi dapat mendeteksi dan merespons akses atau eksploitasi yang tidak sah dengan cepat. Selain itu, perlindungan terhadap akses nirkabel 802.11 juga menjadi fokus utama. Penggunaan otentikasi dan enkripsi yang aman, serta perlindungan fisik atau penghalang dari gangguan, membantu melindungi akses nirkabel dan mencegah serangan yang berpotensi terjadi melalui jalur ini.

Dengan mengikuti standar keamanan jaringan ini, organisasi dapat memperkuat keamanan jaringan mereka secara keseluruhan. Dengan mengimplementasikan konfigurasi yang aman, menjalankan proses kontrol perubahan yang ketat, dan melindungi perangkat lunak serta akses nirkabel, organisasi dapat mengurangi risiko serangan dan menjaga kerahasiaan, integritas, dan ketersediaan sistem dan data mereka.

# PENUTUP

Dalam rangkuman ini, kami telah menjelajahi pentingnya keamanan jaringan dalam era digital yang terus berkembang. Keamanan jaringan tidak hanya menjadi kebutuhan yang mendesak, tetapi juga merupakan fondasi yang kokoh untuk memastikan integritas, kerahasiaan, dan ketersediaan data yang kita kelola.

Melalui peninjauan ini, kami telah menyoroti ancaman yang ada, seperti serangan malware, peretasan, dan serangan DDoS, serta strategi yang dapat diadopsi untuk melindungi jaringan kita. Dari penggunaan kebijakan keamanan yang kuat dan pemantauan yang cermat hingga implementasi teknologi keamanan canggih, ada banyak langkah yang dapat kita ambil untuk menjaga jaringan kita tetap aman.