PERTEMUAN 9
NETWORK SECURITY

A. TUJUAN PEMBELAJARAN

Pada pertemuan ini akan dijelaskan mengenai keamanan jaringan. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Mendefinisikan Network Security.
2. Mengklasifikasikan Network Security
3. Mengidentifikasi Jenis Serangan pada Network Security

B. URAIAN MATERI

1. Mendefinisikan Network Securty

Jaringan komputer (*computer network*) atau sederhananya jaringan (*network*) adalah penyatuan komputer yang memungkinkan mereka untuk berinteraksi dan berkomunikasi satu sama lain. Namun, kita dapat mengatakan bahwa, dalam istilah yang lebih paham komputer, jaringan komputer mengacu pada grup/kumpulan komputer mana pun yang terhubung satu sama lain, memungkinkan komunikasi antara satu dan lainnya. Jaringan juga memungkinkan komputer anggota untuk berbagi aplikasi, data, dan sumber daya jaringan lainnya (server file, printer, dll.)

Keamanan jaringan (network security) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer.

Network security melibatkan otorisasi akses ke data di dalam jaringan, yang dikendalikan oleh administrator jaringan. Pengguna (users) memilih atau diberi ID dan password atau informasi otentikasi lain yang memungkinkan mereka untuk mengakses informasi dan program dalam wewenang mereka sendiri.

Network security mencakup berbagai jaringan komputer, baik publik maupun pribadi, yang digunakan dalam pekerjaan sehari-hari; melakukan transaksi dan komunikasi di antara bisnis, instansi pemerintah dan individu.

Jaringan tersebut dapat bersifat pribadi, seperti di dalam perusahaan, dan lainnya yang mungkin terbuka bagi akses publik.

Network security terlibat dalam organisasi, perusahaan, dan jenis lembaga lainnya. Seperti bagaimana mengamankan jaringan, serta melindungi dan mengawasi operasi yang dilakukan. Dimana cara paling umum dan sederhana untuk melindungi sumber daya jaringan (network resource) adalah dengan menetapkan nama yang unik dan password yang sesuai.

a. Konsep Network Security

Sistem keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja untuk mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang.

b. Jenis Gangguan Keamanan Jaringan

Ada beberapa jenis gangguan keamanan jaringan yang perlu Anda ketahui. Berikut daftarnya:

1) Hacking: perusakan pada infrastruktur jaringan komputer yang sudah ada.
2) Carding: pencurian data terhadap identitas perbankan seseorang. Misalnya pencurian nomor kartu kredit yang dimanfaatkan untuk berbelanja online.
3) Deface: perubahan terhadap bentuk atau tampilan website.
4) Physing: pemalsuan data resmi.

Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan *Confidentiality* (kerahasiaan), *Integrity* (integritas), *Availability* (ketersediaan).

Confidentiality adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

a. *Confidentiality* (kerahasiaan)

Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

b. *Integrity* (integritas)

Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

c. *Availability* (ketersediaan)

Ketersediaan (*availability*) adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

Dengan konsep yang ada di dalam *availability*, informasi dapat selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang. Hingga ketika user membutuhkan informasi tersebut, informasi dapat diakses dan digunakan dengan cepat.

2. Mengklasifikasikan Network Security

Serangan terhadap keamanan sistem informasi (security attack) dewasa ini seringkali terjadi. Kejahatan computer (cyber crime) pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan. Ada beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang yaitu :

a. Interception yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi

b. Interruption yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login.
c. Fabrication yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target
d. Modification yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

Menurut David Icove, dilihat dari lubang keamanan yang ada pada suatu sistem, keamanan dapat diklasifikasikan menjadi empat macam:

a. Keamanan Fisik (Physical Security)

Suatu keamanan yang meliputi seluruh sistem beserta peralatan, peripheral, dan media yang digunakan. Biasanya seorang penyerang akan melakukan wiretapping (proses pengawasan dan penyadapan untuk mendapatkan password agar bisa memiliki hak akses). Dan jika gagal, maka DOS (Denial Of Service) akan menjadi pilihan sehingga semua service yang digunakan oleh komputer tidak dapat bekerja. Sedangkan cara kerja DOS biasanya mematikan service apa saja yang sedang aktif atau membanjiri jaringan tersebut dengan pesan-pesan yang sangat banyak jumlahnya. Secara sederhana, DOS memanfaatkan celah lubang keamanan pada protokol TCP/IP yang dikenal dengan Syn Flood, yaitu sistem target yang dituju akan dibanjiri oleh permintaan yang sangat banyak jumlahnya (flooding), sehingga akses menjadi sangat sibuk.

b. Keamanan Data dan Media

Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengolah data. Biasanya penyerang akan menyisipkan virus pada komputer target melalui attachment pada e-mail. Cara lainnya adalah dengan memasang backdoor atau trojan horse pada sistem target. Tujuannya untuk mendapatkan dan mengumpulkan informasi berupa password administrator. Password tersebut nantinya digunakan untuk masuk pada account administrator.

c. Keamanan Dari Pihak Luar

Memanfaatkan faktor kelemahan atau kecerobohan dari orang yang berpengaruh (memiliki hak akses) merupakan salah satu tindakan yang diambli oleh seorang hacker maupun cracker untuk dapat masuk pada sistem yang

menjadi targetnya. Hal ini biasa disebut social engineering. Social engineering merupakan tingkatan tertinggi dalam dunia hacking maupun cracking. Biasanya orang yang melakukan social engineering akan menyamar sebagai orang yang memakai sistem dan lupa password, sehingga akan meminta kepada orang yang memiliki hak akses pada sistem untuk mengubah atau mengganti password yang akan digunakan untuk memasuki sistem tersebut.

d. Keamanan dalam Operasi

Merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Dengan demikian, sistem tersebut dapat berjalan baik atau menjadi normal kembali. Biasanya para penyerang akan menghapus seluruh log-log yang tertinggal pada sistem target (log cleaning) setelah melakukan serangan.

3. Mengidentifikasi Jenis Serangan pada Network Security

a. Denial-of-Service/ Distributed Denial-of-Service (DoS/DDoS)

Tujuan dari serangan denial-of-service adalah membanjiri jaringan yang diserang dengan jumlah *traffic* yang sangat banyak, mematikan infrastruktur jaringan seperti router atau firewall. Karena penyerang tidak tertarik untuk menerima tanggapan atas paket serangannya, serangan DoS adalah peluang yang ideal untuk menggunakan alamat palsu. Alamat palsu lebih sulit untuk difilter, karena setiap paket palsu tampaknya berasal dari alamat yang berbeda, dan mereka menyembunyikan sumber serangan yang sebenarnya. Hal ini membuat *backtracking* menjadi sangat sulit. Kekusutan baru pada DoS adalah DoS terdistribusi, yang memanfaatkan botnet untuk menghasilkan serangan DoS dari berbagai sumber. Hal ini tidak hanya membuat serangan lebih sulit untuk dipertahankan, karena banyak komputer dapat menghasilkan lebih banyak *traffic* secara signifikan daripada satu komputer, tetapi juga membuatnya jauh lebih sulit untuk melacak sumber serangan.

Ketika serangan DoS terjadi, gejala yang biasa terjadi meliputi:

1) Kinerja jaringan sangat lambat, termasuk saat membuka file atau mengakses situs web.
2) Tidak tersedianya salah satu atau semua situs web.
3) Peningkatan dramatis dalam jumlah email spam yang diterima.

Ada tiga jenis serangan DDoS yang umum:

1) Volume-based attacks. Menjenuhkan bandwidth situs atau sistem serangan dengan membanjiri situs atau sistem dengan paket UPP, paket ICMP, atau paket palsu lainnya.
2) Protocol attacks. Menggunakan sumber daya server atau perangkat komunikasi, seperti firewall dan *load balancers*. Termasuk SYN *floods*, serangan paket terfragmentasi, serangan *ping of death*, dan Smurf DDoS.
3) Application-layer attacks. Menggunakan kerentanan sistem atau perangkat untuk merusak server atau perangkat komunikasi. Ini termasuk serangan *low-and-slow* dan GET/POST *floods*.

Beberapa jenis serangan DDoS yang populer dan berbahaya meliputi:

1) UDP floods. Menggunakan *User Datagram Protocol* (UDP), yang merupakan protokol jaringan tanpa koneksi, untuk membanjiri port acak pada host jarak jauh dengan banyak paket UDP. Ketika server berulang kali memeriksa aplikasi yang merespon di port itu ke titik di mana sistem menggunakan semua sumber dayanya untuk meresponsnya sistem menjadi tidak dapat diakses.
2) ICMP (ping) flood. Menggunakan paket ICMP untuk menbanjiri sistem. Jenis serangan ini dapat menghabiskan bandwidth keluar dan masuk karena server korban sering mencoba merespons dengan paket ICMP Echo Reply.
3) SYN flood. Banyak protokol TCP menggunakan three-way handshake di mana SYN Request digunakan untuk memulai koneksi TCP. Host menanggapi dengan tanggapan SYN-ACK, yang dikonfirmasi dengan tanggapan ACK dari requester. Dalam SYN flood, penyerang mengirimkan beberapa permintaan SYN tetapi tidak menanggapi tanggapan SYN-ACK, atau penyerang mengirimkan permintaan SYN dari alamat IP palsu. Terlalu banyak permintaan SYN menyebabkan sistem tidak menerima koneksi baru.
4) Ping of death. Serangan yang mengirimkan beberapa ping dalam format yang salah atau berbahaya ke komputer. Paket IP, termasuk header, memiliki panjang 65.535 byte, dan banyak sistem komputer tidak pernah dirancang untuk menangani paket ping yang lebih besar dari ini, karena melanggar Protokol Internet. Dengan mengirimkan fragmen IP dengan

Fragment Offset yang terlalu besar, penyerang dapat menyebabkan paket IP, yang dipecah menjadi ukuran yang lebih kecil untuk melintas, kemudian untuk membentuk paket yang lebih besar dari 65.535 byte setelah dipasang kembali pada penerima, sehingga buffer memori meluap. Dengan demikian, area memori penting ditimpa, menyebabkan *denial-of-service* untuk paket yang sah.

5) HTTP flood. Menggunakan banyak permintaan HTTP GET atau POST untuk menyerang server web atau aplikasi. Serangan ini paling efektif jika memaksa server atau aplikasi untuk mengalokasikan sumber daya semaksimal mungkin dalam menanggapi setiap permintaan.
6) Email bomb. Mengirim begitu banyak email ke pengguna atau domain, server menjadi kewalahan.
7) Zero-day attacks. Serangan ini didasarkan pada penggunaan kerentanan yang tidak diketahui atau baru saja diumumkan.

Untuk melindungi dari serangan DoS, gunakan kombinasi deteksi serangan, klasifikasi lalu lintas, dan alat respons yang dapat mengidentifikasi dan memblokir *traffic* yang tidak sah. Ini termasuk *intruder prevention systems* (IPS) dan opsi keamanan yang tersedia di firewall, router, dan sakelar yang mengurangi dampak luapan. Selain itu, periksa dokumentasi untuk mengetahui praktik terbaik dalam memperkuat server dan peralatan jaringan. Pastikan server dan peralatan jaringan dilengkapi dengan patch keamanan terbaru.

b. IP Spoofing

IP spoofing adalah modifikasi paket data sehingga paket data dari komputer yang menyerang tampak seperti berasal dari komputer tepercaya. Dengan tampil sebagai komputer tepercaya, penyerang dapat melewati langkah-langkah keamanan jaringan, seperti filter paket, atau solusi lain yang mengandalkan alamat IP untuk otentikasi. Metode serangan pada sistem jarak jauh ini bisa sangat sulit karena penyerang harus memodifikasi ribuan paket agar berhasil menyelesaikan serangan. Jenis serangan ini umumnya bekerja paling baik bila ada hubungan kepercayaan antar mesin. Misalnya, tidak jarang di beberapa lingkungan memiliki host UNIX di jaringan perusahaan yang saling percaya. etelah pengguna berhasil mengautentikasi ke satu host, mereka secara otomatis dipercaya pada host lain dan tidak memerlukan ID

pengguna atau kata sandi untuk masuk ke sistem. Jika penyerang berhasil memalsukan koneksi dari mesin tepercaya, dia mungkin dapat mengakses mesin target tanpa otentikasi. Mengidentifikasi mesin tepercaya sering kali dilakukan dengan menggunakan sniffing jaringan.

c. DNS Poisoning

Serangan DNS *poisoning* adalah serangan terhadap informasi yang disimpan dalam cache di server DNS. Saat permintaan DNS dibuat, hasil permintaan disimpan dalam cache di server DNS sehingga permintaan DNS berikutnya yang dibuat untuk server yang sama dapat dikembalikan lebih cepat, tanpa memerlukan pencarian oleh server DNS eksternal. Sayangnya, file cache ini tidak terlalu aman, dan penyerang menargetkan file ini untuk memasukkan alamat IP palsu untuk entri server tertentu ke dalam cache. Jika ini terjadi, semua host yang membuat permintaan untuk situs tersebut dari server DNS yang diracuni akan diarahkan ke situs yang salah. Entri palsu dalam cache akan tetap ada sampai cache kedaluwarsa dan di-*refresh*.

d. Man-in-the-middle

Serangan man-in-the-middle adalah jenis serangan di mana penyerang menerobos komunikasi antara titik akhir koneksi jaringan. Setelah penyerang masuk ke aliran komunikasi, mereka dapat mencegat data yang sedang ditransfer, atau bahkan memasukkan informasi palsu ke aliran data. Jenis serangan ini sering digunakan untuk mencegat koneksi HTTP dan HTTPS. Sistem yang terhubung ke jaringan nirkabel sangat rentan terhadap bentuk serangan ini.

e. Back door

Serangan *back door* adalah serangan terhadap celah yang tersisa di bagian fungsional perangkat lunak yang memungkinkan akses ke sistem atau aplikasi perangkat lunak tanpa sepengetahuan pemiliknya. Sering kali, *back door* ini ditinggalkan oleh pengembang aplikasi, tetapi pengujian kode saat ini telah secara dramatis mengurangi jumlah ini yang ditemukan dalam perangkat lunak komersial. Versi yang lebih umum dari serangan ini terjadi ketika administrator sistem membuat akun sistem yang dapat mereka gunakan jika mereka diminta untuk meninggalkan perusahaan. Sebagai seorang

profesional keamanan informasi, salah satu tujuannya harus memvalidasi akun sistem milik karyawan setidaknya setahun sekali.

f. Replay attack

Serangan replay terjadi ketika penyerang dapat menangkap aliran data utuh dari jaringan menggunakan sniffer jaringan, memodifikasi komponen tertentu dari aliran data, dan kemudian memutar ulang *traffic* kembali ke jaringan untuk menyelesaikan serangan mereka.

g. Weak encryption keys

Serangan terhadap kunci enkripsi yang lemah berhasil terjadi ketika kunci memiliki nilai yang memungkinkan terjadi pemecahan enkripsi. Setelah enkripsi rusak, penyerang dapat mengakses data yang seharusnya dienkripsi. Contoh dari serangan ini adalah kelemahan yang dieksploitasi dalam standar keamanan *Wired Equivalent Privacy* (WEP) yang digunakan dalam hubungannya dengan jaringan nirkabel. Dimaksudkan untuk digunakan mengamankan jaringan nirkabel, alih-alih kunci WEP ditemukan lemah dan dapat dipecahkan jika *traffic* nirkabel 5 hingga 10 MB dapat ditangkap. *Traffic* ini kemudian dapat dijalankan melalui salah satu dari banyak alat yang diterbitkan oleh komunitas peretas, dan hasilnya adalah kunci WEP, yang memungkinkan penyerang untuk membaca informasi yang dilindungi dengan WEP. Serangan ini adalah contoh lain dari serangan yang mengandalkan sniffer jaringan agar berhasil melakukan serangan.

h. Password cracking

Peretasan kata sandi adalah serangan yang mencoba mendekripsi kata sandi yang disimpan. Serangan peretasan kata sandi yang berhasil membutuhkan akses ke basis data kata sandi terenkripsi, dan alat yang dirancang untuk mendekripsi basis data.

i. Dictionary attack

Serangan kamus mirip dengan serangan peretasan kata sandi, kecuali dibandingkan menggunakan alat untuk mencoba mendekripsi kata sandi, serangan kamus menggunakan kamus kata sandi umum dan upaya masuk berulang kali dengan kata sandi tersebut untuk mencoba menemukan logon, dan kombinasi kata sandi yang berhasil. ariasi serangan ini adalah serangan menebak kata sandi, di mana penyerang akan mengumpulkan informasi

tentang korban dalam upaya menebak kata sandinya. Inilah sebabnya mengapa kebijakan kata sandi biasanya melarang penggunaan nama kerabat, hewan peliharaan, dan sebagainya untuk kata sandi.

j. Brute force attack

Serangan brute force sangat mirip dengan serangan kamus, kecuali dibandingkan menggunakan kamus kata sandi umum, serangan brute force mencoba setiap kombinasi tombol yang diketahui untuk memecahkan kata sandi. Semakin panjang dan kompleks kata sandi, semakin sulit serangan jenis kata sandi ini berhasil.

k. SQL injection attack

Serangan injeksi SQL adalah salah satu serangan terlama terhadap aplikasi web yang menggunakan aplikasi database SQL Server. Dalam serangan ini, karakter kontrol dimasukkan ke dalam aplikasi web dan bergantung pada konfigurasi server basis data, serangan dapat berkisar dari pengambilan informasi dari basis data server web hingga memungkinkan eksekusi kode atau bahkan akses penuh ke server. Serangan ini mengandalkan kelemahan database serta kelemahan pengkodean.

l. Buffer overflow attack

Serangan buffer overflow mengeksploitasi kode yang ditulis dengan buruk dengan memasukkan data ke dalam kolom variabel dan memanfaatkan respons untuk mengakses informasi dalam aplikasi. Serangan ini terjadi jika pengembang aplikasi tidak membatasi atau memeriksa ukuran data yang dimasukkan ke dalam kolom aplikasi. Ketika data yang terlalu panjang untuk dimasukkan ke kolom, itu menciptakan kesalahan yang dapat dimanfaatkan oleh penyerang untuk melakukan tindakan jahat terhadap aplikasi.

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi keamanan komputer yang Anda ketahui!
2. Sebutkan dan jelaskan lapisan data link yang anda ketahui!
3. Sebutkan dan jelaskan jenis-jenis serangan network security!
4. Berikan kesimpulan yang anda ketahui dalam network security!
5. Apa yang dimaksud dengan buffer overflow attack!

D. REFERENSI

Stallings, W., & Brown, L. (2018). *Computer Security Principles and Practices*. 4th Edition. New York: Pearson Education Limited.

Gollmann, D. (2011). Computer Security. 3rd Edition. India: John Wiley & Sons, Ltd.

Goodrich, M., & Tamassia, R. (2014). Introduction to Computer Security. Harlow: Pearson Education Ltd.

Panek, C. (2020). Security Fundamental. Canada: Sybex A Wiley Brand.

Scott, R. (2019). Computer Networking Beginner Guide.

Peterson, L. L., & Davie, B. S. (2012). Computer Networks A System Approach. 5th Edition. Amsterdam: Elsevier Inc.

Alani, M. M. (2014). *Guide to OSI and TCP/IP Models*. New York: Springer.

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary