PERTEMUAN 10
NETWORK SECURITY (LANJUTAN)

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai lanjutan dari keamanan jaringan komputer. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Mahasiswa cara kerja *firewall*
2. Memahami cara kerja *protocol tunneling*
3. Memahami cara kerja IDS dan IPS

B. URAIAN MATERI

1. Memahami Cara Kerja Firewall

Firewall adalah sistem yang dirancang untuk melindungi komputer atau jaringan komputer dari serangan berbasis jaringan. Firewall melakukan ini dengan menyaring paket data yang melintasi jaringan. Firewall perimeter tipikal diimplementasikan dengan dua (atau lebih) koneksi jaringan.

Firewall tetap menjadi fondasi teknologi keamanan jaringan. Ada sejumlah opsi, jenis, dan teknologi yang terkait dengan pemilihan, penerapan, dan pemeliharaan firewall di jaringan. Ada juga sejumlah faktor yang membantu menentukan solusi yang tepat untuk memenuhi kebutuhan bisnis.

a. Firewall Policy

Sebelum memeriksa secara spesifik bagaimana firewall diimplementasikan, penting untuk memahami pendekatan konseptual yang berbeda untuk menentukan kebijakan firewall untuk organisasi atau mesin. Paket yang melintas melalui firewall dapat memiliki salah satu dari tiga hasil:

1) *Accepted*: diizinkan melalui firewall.
2) *Dropped*: tidak diizinkan melintas tanpa ada indikasi kegagalan.
3) *Rejected*: tidak diizinkan melintas, disertai dengan upaya untuk menginformasikan sumber bahwa paket tersebut ditolak.

Kebijakan yang digunakan oleh firewall untuk menangani paket didasarkan pada beberapa properti paket yang sedang diperiksa, termasuk protokol yang digunakan (seperti TCP atau UDP), alamat IP sumber dan tujuan, port sumber dan tujuan, dan, dalam beberapa kasus, *payload* tingkat aplikasi dari paket (misalnya, apakah berisi virus).

b. Hardware Filewalls

Dalam lingkup jaringan saat ini, sebagian besar firewall produksi berbasis perangkat keras. Firewall perangkat keras adalah firewall yang berjalan pada platform khusus, yang dirancang khusus, dioptimalkan, dan diperkuat (proses pengamanan sistem) untuk menjalankan perangkat lunak aplikasi firewall.

Meskipun ada berbagai jenis firewall, dengan karakteristik yang berbeda-beda, firewall memiliki beberapa fungsi dasar. Firewall memfilter traffic berdasarkan sekumpulan aturan yang dikonfigurasi. Umumnya, aturan ini didasarkan pada informasi yang terdapat dalam paket data yang berjalan melintasi jaringan. Informasi header yang terdapat dalam paket data tersebut memberikan informasi yang dibutuhkan firewall untuk menerapkan aturan ini dengan benar.

Ada berbagai jenis firewall yang berbeda, dan orang yang berbeda terkadang menentukan jenis firewall dengan cara yang berbeda. Kuncinya adalah memahami dasar-dasarnya secara menyeluruh, karena selain lulus tes sertifikasi, kita biasanya tidak akan diminta untuk mengidentifikasi jenis firewall dalam tugas sehari-hari.

c. Packet Filtering

Jenis firewall pertama dikenal sebagai firewall packet-filtering. Jenis firewall ini dianggap sebagai firewall generasi pertama karena firewall pertama berfungsi sebagai filter paket. Seperti yang telah kita bahas, tujuan utama firewall adalah untuk memfilter *traffic*. Firewall pemfilteran paket memeriksa paket data saat mencoba melintasi firewall, dan berdasarkan aturan yang telah ditetapkan di firewall, firewall mengizinkan atau menolak setiap paket.

Salah satu versi pertama dari firewall ini adalah router packet-filtering. Router dapat melakukan beberapa pemfilteran paket yang belum sempurna, seperti mengizinkan semua *traffic* keluar sambil menolak semua *traffic* masuk,

atau memblokir protokol tertentu agar tidak melewati router, seperti Telnet atau FTP.

Firewall secara signifikan meningkatkan kemampuan firewall pemfilteran paket, karena mereka mengizinkan aturan yang lebih terperinci. Kita dapat mengonfigurasi firewall pemfilteran paket untuk memblokir penjelajahan web di Internet, kecuali ke situs web Internet perusahaan, sementara mengizinkan traffic web keluar dari jaringan internal kita ke Internet. Opsi lainnya adalah menyiapkan aturan yang akan membatalkan permintaan ping apa pun, kecuali permintaan itu berasal dari seseorang di workstation tim jaringan.

Saat mengonfigurasi aturan firewall pemfilteran paket, satu atau lebih dari atribut TCP / IP berikut biasanya digunakan:

1) Alamat IP sumber
2) Alamat IP tujuan
3) Protokol IP (Telnet, FTP, HTTP, HTTPS, dan sebagainya)
4) Port TCP dan UDP sumber (misalnya, protokol HTTP berjalan pada port TCP 80)
5) Port TCP dan UDP tujuan
6) Antarmuka jaringan firewall masuk
7) Antarmuka jaringan firewall keluar

Beberapa protokol dan port yang lebih umum yang akan ditemukan di jaringan produksi meliputi:

FTP (file transfer): 20/tcp and 21/tcp
Telnet (Terminal logon): 23/tcp
DNS: 53/udp and 53/tcp
HTTP (web): 80/tcp
HTTPS (web): 443/tcp
SMTP (email): 25/tcp
POP3 (email): 110/tcp
IMAP3 (email): 220/tcp
IMAP4 (email): 143/tcp
LDAP (directory services): 389/tcp
SQL Server: 1433/tcp
RDP (Terminal Services): 3389/tcp

Daftar berikut bukanlah daftar lengkap, karena ada ribuan protokol dan port yang berbeda, tetapi ini adalah protokol umum yang akan kita lihat saat mengonfigurasi aturan pada firewall pemfilteran paket.

d. Circuit Level Firewalls

Firewall tingkat sirkuit biasanya dianggap sebagai teknologi firewall generasi kedua. Mereka bekerja mirip dengan firewall packet-filtering, tetapi beroperasi pada lapisan transport dan sesi model OSI.

Dibandingkan menganalisis setiap paket individu, firewall level sirkuit memantau sesi TCP / IP dengan memantau handshaking TCP antar paket untuk memvalidasi sesi. Traffic difilter berdasarkan aturan sesi tertentu dan mungkin dibatasi hanya untuk komputer resmi. Ketika sesi dibuat, firewall memelihara tabel koneksi yang valid dan membiarkan data lewat ketika informasi sesi cocok dengan entri dalam tabel. Entri tabel dihapus, dan sirkuit ditutup saat sesi diakhiri. Salah satu fitur unik dari firewall level sirkuit adalah bahwa sesi yang melintasi firewall jenis ini tampaknya berasal dari firewall itu. Ini memungkinkan jaringan internal disembunyikan dari jaringan publik.

Jenis firewall ini juga dikenal sebagai proxy transparan, karena semua sesi tampaknya berasal dari firewall. Firewall tingkat sirkuit hampir selalu digunakan bersama dengan jenis firewall lainnya karena mereka hanya dapat mengizinkan sesi dari komputer resmi. Perincian tambahan biasanya diperlukan di sebagian besar lingkup produksi.

e. Application Level Firewalls

Firewall tingkat aplikasi juga dikenal sebagai server proxy bekerja dengan melakukan pemeriksaan mendalam terhadap data aplikasi saat melintasi firewall. Aturan ditetapkan berdasarkan analisis permintaan klien dan respons aplikasi, kemudian menegakkan aturan aplikasi yang benar.

Firewall tingkat aplikasi dapat memblokir aktivitas berbahaya, mencatat aktivitas pengguna, menyediakan pemfilteran konten, dan bahkan melindungi dari spam dan virus. Microsoft Internet Security and Acceleration Server adalah contoh firewall tingkat aplikasi.

Sekarang untuk sisi negatifnya pemeriksaan mendalam terhadap data aplikasi merupakan aktivitas intensif sumber daya dan dapat memerlukan daya pemrosesan yang signifikan untuk mengurangi kemungkinan firewall

memengaruhi kinerja jaringan. Semakin dalam pemeriksaan, semakin tinggi persyaratan sumber daya, dan semakin tinggi kemungkinan dampak kinerja jaringan. Saat menerapkan firewall tingkat aplikasi, penting untuk mengukurnya dengan tepat. Satu kemampuan yang tersedia di beberapa firewall tingkat aplikasi yang dapat membantu mengimbangi dampak kinerja pemeriksaan mendalam data aplikasi adalah penambahan *caching*. *Caching* memungkinkan firewall untuk menyimpan data yang biasa diunduh dan menyediakannya sebagai tanggapan atas permintaan dari pengguna daripada harus mengambil data dari Internet. Sebagian besar browser web memiliki kemampuan ini untuk penyimpanan lokal halaman yang umum digunakan, firewall *caching* memperluas kemampuan ini ke semua pengguna di jaringan. Misalnya, jika 50 karyawan semuanya membaca halaman depan suatu situs web ketika mereka datang ke kantor, firewall menyimpan cache kunjungan pertama ke situs tersebut dan kemudian menyajikan halaman yang disimpan kepada 49 pengunjung berikutnya.

Caching adalah teknologi yang jauh lebih efektif selama masa-masa awal Internet, ketika sebagian besar kontennya statis. Dengan munculnya tampilan yang dapat disesuaikan, *mashup*, dan konten interaktif, efektivitas *cache* menjadi semakin terbatas.

f. Perbandingan Hardware Firewall dan Software Firewall

Ada dua tipe dasar firewall perangkat lunak:

1) Host Firewall. Salah satu jenis firewall perangkat lunak adalah aplikasi firewall yang diinstal pada host, digunakan untuk melindungi host dari serangan berbasis jaringan. Contoh dari jenis firewall perangkat lunak ini adalah firewall Windows yang disertakan dengan versi terbaru sistem operasi Microsoft. Firewall host juga dikenal sebagai firewall pribadi.
2) Firewall Jaringan. Jenis lain dari perangkat lunak firewall adalah aplikasi firewall yang dipasang di server yang digunakan untuk melindungi segmen jaringan dari segmen jaringan lain. Jenis firewall ini menawarkan fungsionalitas yang mirip dengan firewall perangkat keras. Firewall jaringan paling populer adalah yang diproduksi oleh Cisco.

Satu-satunya keadaan yang sangat tidak masuk akal untuk menggunakan firewall perangkat keras adalah melindungi satu host. Untuk melindungi satu host, solusi terbaik adalah menginstal firewall perangkat lunak pada host,

dengan seperangkat aturan khusus berdasarkan apa yang perlu dilindungi. Jika host adalah bagian dari jaringan yang lebih besar, yang hampir selalu demikian, host juga akan dilindungi oleh firewall jaringan apa pun yang ditempatkan di jaringan.

2. Memahami Protocol Tunneling

Tunneling merupakan cara di mana data ditransfer antara dua jaringan dengan aman. Protocol tunneling tidak mengirimkan frame seperti yang dihasilkan oleh node asalnya begitu saja, melainkan membungkusnya dalam header tambahan yang lebih kecil untuk kemudian melewati terowongan. I

si dari paket TCP biasanya tidak dienkripsi, jadi jika seseorang menyadap koneksi TCP, dia sering dapat melihat isi lengkap dari *payload* di sesi ini. Salah satu cara untuk mencegah penyadapan semacam itu tanpa mengubah perangkat lunak yang melakukan komunikasi adalah dengan menggunakan protokol *tunneling*.

a. Secure Shell (SSH)

Protokol administrasi jarak jauh awal seperti telent, FTP, dan login memungkinkan administrator untuk mengontrol mesin dari jarak jauh melalui command prompt atau shell, tetapi tidak memberikan bentuk enkripsi dan sebagai gantinya mengirim data dalam teks biasa. Untuk memperbaiki protokol yang tidak aman ini, SSH dibuat untuk menggunakan kriptografi simetris dan kunci publik untuk berkomunikasi di Internet menggunakan saluran terenkripsi.

Keamanan SSH didasarkan pada kombinasi kekuatan masing-masing dari algoritma enkripsi, dekripsi, dan pertukaran kunci yang digunakan SSH. Karena keamanannya yang kuat, protokol SSH digunakan untuk berbagai tugas selain untuk mengamankan administrasi jarak jauh, termasuk transfer file melalui Secure Copy Protocol (SCP) sederhana atau sebagai bagian dari Secure File-Transfer Protocol (SFTP).

Selain itu, salah satu penggunaan paling umum dari protokol SSH adalah untuk secure tunneling. Karena protokol dirancang sedemikian rupa sehingga penyadap tidak dapat menyimpulkan konten *traffic* SSH, *tunnel* yang dibuat menggunakan SSH akan mencegah banyak serangan berdasarkan

packet sniffing. Untuk membuat koneksi SSH, klien dan server harus melalui langkah-langkah berikut:

1) Klien terhubung ke server melalui sesi TCP.
2) Klien dan server bertukar informasi tentang detail administratif, seperti metode enkripsi yang didukung dan versi protokolnya, masing-masing memilih sekumpulan protokol yang didukung yang lain.
3) Klien dan server memulai pertukaran kunci-rahasia untuk membuat kunci sesi rahasia bersama, yang digunakan untuk mengenkripsi komunikasi mereka (tetapi tidak untuk otentikasi). Kunci sesi ini digunakan bersama dengan *block cipher* yang dipilih (biasanya AES, 3DES, Blowfish, atau IDEA) untuk mengenkripsi semua komunikasi lebih lanjut.
4) Server mengirimkan kepada klien daftar bentuk otentikasi yang dapat diterima, yang akan dicoba oleh klien secara berurutan. Mekanisme yang paling umum adalah menggunakan sandi atau metode otentikasi kunci publik berikut:
   a) Jika otentikasi *public-key* adalah mekanisme yang dipilih, klien mengirimkan kunci publiknya ke server.
   b) Server kemudian memeriksa apakah kunci ini disimpan dalam daftar kunci resminya. Jika demikian, server mengenkripsi sebuah tantangan menggunakan kunci publik klien dan mengirimkannya ke klien.
   c) Klien mendekripsi tantangan dengan kunci pribadinya dan menanggapi server, membuktikan identitasnya.
5) Setelah otentikasi berhasil diselesaikan, server memungkinkan klien mengakses sumber daya yang sesuai, seperti *command prompt*.

b. Virtual Private Networking (VPN)

Virtual private networking (VPN) adalah teknologi yang memungkinkan jaringan pribadi diperpanjang dengan aman melalui jarak fisik yang jauh dengan memanfaatkan jaringan publik, seperti Internet, sebagai alat transport. VPN memberikan jaminan kerahasiaan, integritas, dan otentikasi data, meskipun menggunakan jaringan yang tidak tepercaya untuk transmisi. Ada dua jenis utama VPN, *remote access* VPN, dan *site-to-site* VPN.

Remote access VPN memungkinkan klien yang berwenang untuk mengakses jaringan pribadi yang disebut sebagai intranet. Solusi *site-to-site*

VPN dirancang untuk menyediakan jembatan yang aman antara dua atau lebih jaringan yang jauh secara fisik. VPN menyediakan keamanan yang sama tetapi menggunakan Internet untuk komunikasi daripada mengandalkan lapisan fisik pribadi. Untuk membuat koneksi *site-to-site* VPN, kedua jaringan memiliki titik akhir VPN yang terpisah, yang masing-masing berkomunikasi satu sama lain dan mengirimkan *traffic* dengan tepat.

3. Memahami Cara Kerja IDS dan IPS

Dua teknologi keamanan lain yang tersedia untuk mengamankan jaringan adalah *Intrusion Detection System (IDS)* dan Intrusion Prevention System (IPS).

a. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sistem perangkat lunak atau perangkat keras yang digunakan untuk mendeteksi tanda-tanda aktivitas berbahaya di jaringan atau komputer individual. Fungsi IDS dibagi antara sensor IDS (*IDS sensors)*, yang mengumpulkan data waktu nyata tentang fungsi komponen jaringan dan komputer, dan manajer IDS (*IDS manajer)*, yang menerima laporan dari sensor.

Manajer IDS mengumpulkan data dari sensor IDS untuk menentukan apakah telah terjadi intrusi. Penentuan ini biasanya didasarkan pada sekumpulan kebijakan situs, yang merupakan kumpulan aturan dan kondisi statistik yang menentukan kemungkinan intrusi. Jika manajer IDS mendeteksi intrusi, maka itu akan membunyikan alarm sehingga administrator sistem dapat bereaksi terhadap kemungkinan serangan.

IDS dirancang untuk mendeteksi sejumlah ancaman, termasuk yang berikut:

1) *Masquerader:* penyerang yang secara tidak benar menggunakan identitas dan/atau kredensial pengguna yang sah untuk mendapatkan akses ke sistem atau jaringan komputer.
2) *Misfeasor:* pengguna sah yang melakukan tindakan yang tidak diizinkan untuk dilakukannya.
3) *Clandestine user:* pengguna yang mencoba memblokir atau menutupi tindakannya dengan menghapus file audit dan/atau log sistem.

Selain itu, IDS dirancang untuk mendeteksi serangan dan ancaman otomatis, termasuk yang berikut ini:

1) *Port scans:* pengumpulan informasi yang dimaksudkan untuk menentukan port mana pada host yang terbuka untuk koneksi TCP.
2) *Denial-of-service attacks:* serangan jaringan yang dimaksudkan untuk membanjiri host dan menutup akses yang sah.
3) *Malware attacks:* mereplikasi serangan perangkat lunak berbahaya, seperti *Trojan horses*, *worms*, virus, dll.
4) *ARP spoofing:* upaya untuk mengarahkan *traffic* IP di jaringan area lokal
5) *DNS cache poisoning:* serangan pharming yang ditujukan untuk mengubah cache DNS host untuk membuat asosiasi nama-domain / alamat IP yang dipalsukan.

b. Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) sangat mirip dengan IDS, kecuali bahwa selain mendeteksi dan memberi peringatan, IPS juga dapat mengambil tindakan untuk mencegah terjadinya pelanggaran.

Ada dua jenis utama teknologi IDS / IPS:

1) Network-based: IDS berbasis jaringan (NIDS) memantau *traffic* jaringan menggunakan sensor yang terletak di lokasi utama dalam jaringan, sering kali di zona demiliterisasi (DMZ) atau di perbatasan jaringan. Sensor ini menangkap semua *traffic* jaringan dan menganalisis konten paket individu untuk *traffic* berbahaya. NIDS akan memperoleh akses ke *traffic* jaringan dengan menghubungkan ke hub, sakelar jaringan yang dikonfigurasi untuk *port mirroring*, atau *network tap*.
2) Host-based: IDS berbasis host (HIDS) umumnya memiliki agen perangkat lunak yang bertindak sebagai sensor. Agen ini memantau semua aktivitas host di tempat diinstalnya, termasuk memantau sistem file, log, dan kernel, untuk mengidentifikasi dan memperingatkan jika ada perilaku yang mencurigakan. Sebuah HIDS biasanya digunakan untuk melindungi host yang diinstal.

Ada dua metodologi penerapan umum yang digunakan saat menempatkan IDS / IPS untuk melindungi jaringan dari Internet. Masing-masing memiliki kelebihan dan kekurangan:

1) Tidak disaring. Penginstalan IDS / IPS yang tidak difilter memeriksa aliran data Internet mentah sebelum melewati firewall. Ini memberikan jumlah visibilitas tertinggi untuk serangan, tetapi juga berarti bahwa ada volume

data yang jauh lebih tinggi untuk dipantau, dengan kemungkinan positif palsu yang lebih tinggi. Ada juga kemungkinan bahwa selama periode *traffic* tinggi, IDS / IPS mungkin tidak dapat memproses semua paket, dan serangan dapat terlewatkan.

2) Disaring. Solusi IDS / IPS yang disaring memantau lalu lintas yang melewati firewall penyaringan. Keuntungan model ini adalah secara dramatis mengurangi jumlah *traffic* yang perlu dipantau, mengurangi kemungkinan positif palsu dan paket hilang selama volume *traffic* tinggi. Ada kehilangan visibilitas dengan model ini, karena serangan tidak dapat dilihat pada penyaringan firewall.

C. SOAL LATIHAN/ TUGAS

1. Apa yang dimaksud dengan firewal!
2. Sebutkan tiga contoh serangan pada keamanan yang bersifat fisik!
3. Sebutkan dan jelaskan perbandingan hardware firewall dengan software firewall!
4. Jelaskan apa yang dimaksud dengan intrusion detection system(IDS)!
5. Sebutkan dan jelaskan metodologi penerapan umum yang digunakan saat menempatkan IDS / IPS untuk melindungi jaringan dari Internet!

D. REFERENSI

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

Bishop, M. (2019). Computer Security Art and Science. 2nd Edition. Boston: Pearson Education Inc.

Bosworth, S., Kabay, M. E., & Whyne, E. (2014). Computer Security Handbook. 6th Edition. Canada: John Wiley & Sons, Inc.

Easttom, D., C. (2020). Computer Security Fundamentals. 4th Edition. Pearson Education, Inc.

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.

Pfleeger, P. C., Pfleeger, S. L., & Margulies, J. (2015). Security in Computing. 5th Edition. Westford: Pearson Education 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

http://www.iana.org/assignments/port-numbers