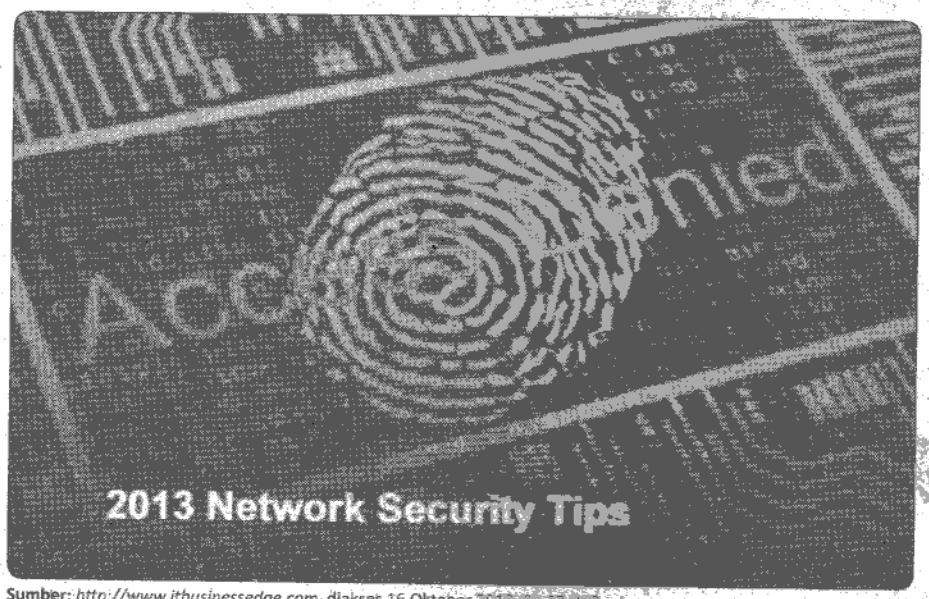
BAB VII
Mengevaluasi Sistem Keamanan Jaringan

Perhatikan gambar dan teks berikut dengan saksama!



Sumber: *http://www.itbusinessedge.com*, diakses 16 Oktober 2013, 14.27 WIB

Gambar 7.1 Akses yang terkunci

Suatu hal yang perlu diingat bahwa tidak ada jaringan yang antisadap atau tidak ada jaringan yang benar-benar aman. Karena sifat dasar dari jaringan adalah melakukan komunikasi maka setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Oleh sebab itu, keamanan jaringan sangatlah dibutuhkan. Komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada *host* yang tidak terhubung kemana-mana. Dengan mengendalikan *network security*, risiko tersebut dapat dikurangi. Namun *network security* biasanya bertentangan dengan *network access*, karena bila *network access* semakin mudah, *network security* makin rawan. Bila *network security* makin baik, *network access* semakin tidak nyaman. Suatu jaringan didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan didesain untuk mengontrol akses. Penyedia *network security* adalah sebagai aksi penyeimbang antara *open access* dengan *security*.

Pada pembelajaran kali ini akan membahas mengenai sistem keamanan jaringan. Untuk mengetahui lebih mendalam tentang sistem keamanan jaringan, maka bersungguh-sungguhlah dalam memahami materi berikut ini dengan saksama agar mendapat hasil yang maksimal.

A. Prinsip dan Ancaman Keamanan Jaringan

Keamanan jaringan komputer merupakan bagian dari sebuah sistem informasi sangat penting dalam menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Dengan demikian, sistem keamanan jaringan identik dengan proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer.

1. Prisip Keamanan Jaringan

Prinsip keamanan jaringan dikategorikan menjadi sebagai berikut.

a. *Kerahasiaan*

Kerahasiaan berhubungan dengan hak akses untuk membaca data atau informasi dan suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dibaca oleh pihak yang telah diberi hak atau wewenang secara legal.

b. *Integritas (Integrity)*

Integrity berhubungan dengan hak akses mengubah data atau informasi dari suatu sistem komputer. Dalam hal ini sistem komputer dapat dinyatakan aman jika suatu data/informasi hanya dapat diubah oleh pihak yang telah diberi hak.

c. *Ketersediaan (Availability)*

Availability berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak.

d. *Authentication*

Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang kita hubungi adalah betul-betul *server* yang asli. Untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi *watermarking* dan *digital signature*. Sedangkan untuk menguji keaslian orang atau *server* yang dimaksud bisa dilakukan dengan menggunakan *password*, *biometric* (ciri-ciri khas orang), dan sejenisnya.

e. *Akses Kontrol*

Akses kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana *user* dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumber daya yang lainnya. Akses kontrol melindungi sistem dan sumber daya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi. Kontrol akses adalah sebuah *term* yang mencakup beberapa tipe mekanisme berbeda yang menjalankan akses pada sistem komputer, jaringan, dan informasi. Kontrol akses sangatlah penting karena menjadi satu dari garis pertahanan pertama yang digunakan untuk menghadang akses yang tidak berhak ke dalam sistem dan sumber daya jaringan.

f. *Non-Repudiation*

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Penggunaan *digital signature*, *certificates*, dan teknologi kriptografi secara umum didukung oleh hukum sehingga status dari *digital signature* itu jelas legal.

2. Jenis-Jenis Gangguan, Serangan, dan Ancaman Keamanan Jaringan

Serangan terhadap keamanan sistem informasi (*security attack*) menjadi penyebab utama terjadinya kejahatan komputer (*cyber crime*) pada dunia maya yang dilakukan oleh kelompok orang yang ingin menembus suatu keamanan sebuah sistem. Beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang adalah sebagai berikut.

Tabel 7.1 Tipe Serangan terhadap *Security Attack*

No.	Tipe Serangan	Keterangan
1.	*Interception*	Pihak yang tidak memiliki wewenang telah berhasil mendapatkan hak akses informasi.
2.	*Interruption*	Penyerang yang telah dapat menguasai sistem, tetapi tidak keseluruhan. Karena *admin* yang asli masih bisa *login*.
3.	*Fabrication*	Penyerang telah menyisipkan objek palsu ke dalam sistem target.
4.	*Modification*	Penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

Dengan demikian, tujuan utama dalam membuat keamanan jaringan adalah untuk mengantisipasi risiko jaringan berupa bentuk ancaman fisik maupun logic secara langsung ataupun tidak langsung yang dapat menganggu aktivitas yang sedang berlangsung dalam jaringan. Jenis-jenis gangguan, serangan, dan ancaman keamanan jaringan antara lain sebagai berikut.

a. Gangguan

Jenis-jenis gangguan keamanan jaringam antara lain sebagai berikut.

Tabel 7.2 Jenis-Jenis Gangguan Keamanan Jaringan

No.	Jenis Gangguan	Keterangan
1.	*Carding*	Pencurian data terhadap identitas perbankan seseorang. Misalnya pencurian nomor kartu kredit yang digunakan untuk bertransaksi *online*.
2.	*Physing*	Pemalsuan terhadap data resmi atau menduplikasi tampilan *web* asli untuk membuat *web* palsu.
3.	*Deface*	Perubahan terhadap bentuk atau tampilan *website*.
4.	*Hacking*	Perusakan pada infrastruktur jaringan komputer yang sudah ada.

b. Serangan

Pada dasarnya serangan terhadap suatu data dalam suatu jaringan menurut jenisnya dapat dikategorikan menjadi dua yaitu sebagai berikut.

1) Serangan Pasif

Serangan pasif diterjemahkan sebagai serangan pada sistem autentikasi dengan hanya mengamati atau memonitor pengiriman informasi ke tujuan dan tidak bertujuan menyisipkan data pada aliran data tertentu. Informasi ini dapat digunakan di lain waktu oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data kemudian menggunakannya untuk memasuki sesi autentikasi dengan berpura-pura menjadi *user* yang *autentik* (asli) disebut dengan *repaly attack*. Beberapa informasi autentikasi seperti *password* atau *data biometric* yang dikirim melalui transmisi elektronik dapat direkam dan digunakan untuk memalsukan data sesungguhnya. Serangan pasif ini sulit dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu, untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksian.

2) Serangan Aktif

Serangan aktif merupakan serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket-paket

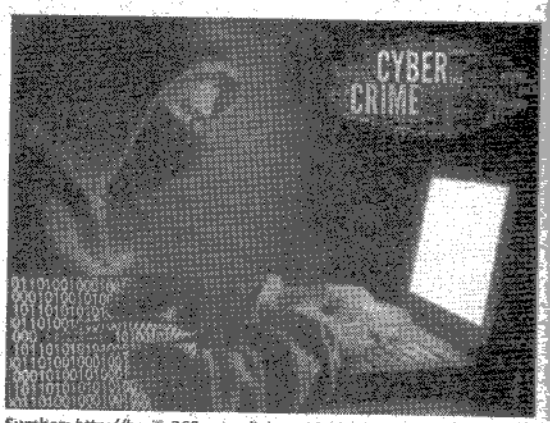
data yang salah ke dalam data *stream* atau dengan memodifikasi paket-paket yang melewati data *stream*. Kebalikan dari serangan pasif, serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Sehingga yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

c. *Ancaman*

Bentuk-bentuk ancaman keamanan jaringan antara lain sebagai berikut.

1) *Memaksa Masuk dan Kamus Password*

Jenis ancaman keamanan jaringan lebih umum disebut sebagai *Brute Force and Dictionary*, serangan ini adalah upaya masuk ke dalam jaringan dengan menyerang *database password* atau menyerang *login prompt* yang sedang *active*. Serangan masuk paksa ini adalah suatu upaya untuk menemukan *password* dari *account user* dengan cara yang sistematis mencoba berbagai kombinasi angka, huruf, atau simbol. Sementara serangan dengan menggunakan metode kamus *password* adalah upaya menemukan *password* dengan mencoba berbagai kemungkinan *password* yang biasa dipakai *user* secara umum dengan menggunakan daftar atau kamus *password* yang sudah didefinisikan sebelumnya. Untuk mengatasi serangan keamanan jaringan dari jenis ini *user* seharusnya memiliki suatu *policy* tentang pemakaian *password* yang kuat di antaranya untuk tidak memakai *password* yang dekat dengan kita misal nama, nama anak, tanggal lahir, dan sebagainya. Semakin panjang suatu *password* dan kombinasinya semakin sulit untuk ditemukan. Akan tetapi, dengan waktu yang cukup semua *password* dapat ditemukan dengan metoda *brute force* ini.



Sumber: *http://berita360.com*, diakses 18 Oktober 2018, 09.30 WIB

Gambar 7.2 Kejahatan *cyber*

2) *Denial of Services (DoS)*

Denial of Services (DoS) adalah salah satu ancaman keamanan jaringan yang membuat suatu layanan jaringan jadi mampet, serangan yang membuat jaringan tidak dapat diakses atau serangan yang membuat sistem tidak bisa memproses/merespons terhadap *traffic* yang legitimasi atau permintaan layanan terhadap *object* dan *resource* jaringan. Bentuk umum dari serangan *Denial of Services* (DoS) ini adalah dengan cara mengirim paket data dalam jumlah yang sangat besar terhadap suatu server di mana server tersebut tidak bisa memproses semuanya. Bentuk lain dari serangan keamanan jaringan *Denial of Services* (DoS) adalah memanfaatkan celah yang rentan dari suatu *operating system*, layanan, ataupun aplikasi. Exploitasi terhadap celah atau titik lemah sistem sering menyebabkan *system crash* atau pemakaian 100% CPU. Namun tidak semua *Denial of Services* (DoS) ini adalah merupakan akibat dari serangan keamanan jaringan. *Error* dalam *coding* suatu program bisa mengakibatkan kondisi yang disebut DoS ini. Jenis-jenis DoS antara lain sebagai berikut.

a) *Distributed Denial of Services* (DDoS)

Distributed Denial of Services (DDoS) terjadi saat penyerang berhasil mengkompromi beberapa layanan sistem dan menggunakannya atau memanfaatkannya sebagai pusat untuk menyebarkan serangan terhadap korban lain.

b) *Distributed Refelective Denial of Services* (DRDoS)

Ancaman keamanan jaringan *Distributed Refelective Denial of Services* (DRDoS) memanfaatkan operasi normal dari layanan Internet, seperti protocol-2 *update* DNS dan *router*. DRDoS ini menyerang fungsi dengan mengirim *update*, sesi, dalam jumlah yang sangat besar kepada berbagai macam layanan *server* atau *router* dengan menggunakan *address spoofing* kepada target korban.

c) Kebanjiran SYN

Serangan keamanan jaringan dengan membanjiri sinyal SYN kepada sistem yang menggunakan protokol TCP/IP dengan melakukan inisiasi sesi komunikasi. Seperti kita ketahui, sebuah *client* mengirim paket SYN kepada server, server akan merespon dengan paket SYN/ACK kepada *client* tadi, kemudian *client* tadi merespon balik juga dengan paket ACK kepada server. Ini proses terbentuknya sesi komunikasi yang disebut *Three-Way handshake* yang dipakai untuk transfer data sampai sesi tersebut berakhir. Kebanjiran SYN terjadi ketika melimpahnya paket SYN dikirim ke server, tetapi si pengirim tidak pernah membalas dengan paket akhir ACK.

d) Bentuk *Smurf Attack*

Serangan keamanan jaringan dalam bentuk *Smurf Attack* terjadi ketika sebuah server digunakan untuk membanjiri target dengan data sampah yang tidak berguna. Server atau jaringan yang dipakai menghasilkan respon paket yang banyak seperti ACMP ECHO paket atau UDP paket dari satu paket yang dikirim. Serangan yang umum adalah dengan jalan mengirimkan *broadcast* kepada segmen jaringan sehingga semua node dalam jaringan akan menerima paket *broadcast* ini. Sehingga setiap *node* akan merespon baik dengan satu atau lebih paket respons.

e) *Ping of Death*

Serangan keamanan jaringan *Ping of Death* adalah serangan *ping* yang *oversize*. Dengan menggunakan *tool* khusus, si penyerang dapat mengirimkan paket *ping aversized* yang banyak sekali kepada korbannya. Dalam banyak kasus sistem yang diserang mencoba memproses data tersebut, *error* terjadi yang menyebabkan *system crash*, *freeze* atau *reboot*. *Ping of Death* ini tidak lebih dari semacam serangan *Buffer overflow*, system yang diserang sering menjadi *down*, disebut *DoS attack*.

f) *Stream Attack*

Stream Attack terjadi saat banyak jumlah paket yang besar dikirim menuju ke *port* pada sistem korban menggunakan sumber nomor yang *random*.

3) Spoofing

Spoofing adalah seni untuk menjelma menjadi sesuatu yang lain. *Spoofing attack* terdiri atas *IP address* dan *node source* atau tujuan yang asli atau valid diganti dengan *IP address* atau *node source* atau tujuan yang lain.

4) Serangan Man-in-the-middle

Serangan keamanan jaringan *Man-in-the-middle* (serangan pembajakan) terjadi saat *user* perusak dapat memposisikan di antara dua titik *link* komunikasi.

a) Dengan jalan menggandakan atau menyusup *traffic* antara dua *party*, hal ini pada dasarnya merupakan serangan penyusup.

b) Para penyerang memposisikan dirinya dalam garis komunikasi di mana ia bertindak sebagai *proxy* atau mekanisme *store-and-forward* (simpan dan lepaskan).

c) Para penyerang ini tidak tampak pada kedua sisi *link* komunikasi dan dapat mengubah isi dan arah *traffic*. Dengan cara ini para penyerang bisa menangkap *logon credensial* atau data sensitif ataupun mampu mengubah isi pesan dari kedua titik komunikasi.

5) *Spamming*

Spam yang umum dijabarkan sebagai *email* yang tak diundang ini, *newsgroup*, atau pesan diskusi. Spam pada umumnya bukan merupakan serangan keamanan jaringan akan tetapi hampir mirip DoS. *Spam* dapat merupakan iklan dari *vendor* atau bisa berisi *Trojan horse*.

6) *Sniffer*

Suatu serangan keamanan jaringan dalam bentuk *Sniffer* dikenal sebagai *snooping attack* merupakan kegiatan *user* perusak yang ingin mendapatkan informasi tentang jaringan atau *traffic* lewat jaringan tersebut. Suatu *Sniffer* sering merupakan program penangkap paket yang dapat menduplikasikan isi paket yang lewat media jaringan ke dalam *file*. Serangan *Sniffer* sering difokuskan pada koneksi awal antara *client* dan server untuk mendapatkan *logon credensial*, kunci rahasia, *password* dan lainnya.

7) *Cracker*

Ancaman keamanan jaringan *Cracker* adalah *user* perusak yang bermaksud menyerang suatu sistem atau seseorang. *Cracker* biasanya termotivasi oleh ego, *power*, atau ingin mendapatkan pengakuan. Akibat dari kegiatan tersebut bisa berupa pencurian (data, ide, dan lain-lain), *disable system*, kompromi keamanan, opini *negatice public*, kehilangan pasar saham, mengurangi keuntungan, dan kehilangan profuktivitas. (**Sumber:** Patwiyanto, Sri Wahyuni, Sumari Agus Prasetyo, 2018)

Kegiatan 7.1

A. Judul Kegiatan : Menganalisis Sistem Keamanan Jaringan

B. Jenis Kegiatan : Kerja Mandiri

C. Tujuan Kegiatan : 1) Peserta didik dapat menjelaskan tentang sistem keamanan jaringan dengan tepat. (KD 3)

2) Peserta didik dapat melakukan penanganan keamanan terhadap jenis-jenis gangguan, serangan, dan ancaman keamanan jaringan dengan terampil. (KD 4)

D. Langkah-Langkah Kegiatan

1. Baca dan cermati cuplikan artikel tentang keamanan jaringan berikut ini!

Keamanan Jaringan

A. Pengertian

Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Maksudnya penggunaan yang tidak sah yaitu penyusup yang bermaksud untuk mengakses setiap bagian dari sistem jaringan komputer tersebut.

B. Tujuan Tujuan dari

Keamanan Jaringan ialah untuk mengantisipasi risiko jaringan komputer berupa bentuk ancaman fisik maupun logik. Maksudnya ancaman fisik adalah seorang pengganggu yang berniat untuk merusak bagian fisik komputer. Sedangkan ancaman logik adalah ancaman yang berupa pencurian data atau pembobolan terhadap akun seseorang.

Dikutip dari: *https://www.academia.edu/9380652/Ringkasan_Materi_KEAMANAN_JARINGAN_SMK_TKJ_XII_Semester_1?auto=download*, diakses 18 Oktober 2018, 10.35 WIB

Hasil pengamatan:

.....

.....

2. Kumpulkanlah beberapa informasi tentang sistem keamanan jaringan dari berbagai sumber yang dianggap relevan!
   Hasil informasi yang diperoleh:
   .....
   .....
3. Lakukanlah analisis tentang sistem keamanan jaringan meliputi:
   a. Pengertian sistem sistem keamanan jaringan.
   b. Prinsip keamanan jaringan.
   c. Jenis-jenis gangguan, serangan, dan ancaman keamanan jaringan.
   Hasil analisis:
   a. .....
   b. .....
   c. .....
4. Lakukanlah percobaan penanganan keamanan terhadap jenis-jenis gangguan, serangan, dan ancaman keamanan jaringan! Kemudian buatlah laporan dari hasil percobaan yang telah kamu lakukan!
   Hasil percobaan:
   .....
   Hasil laporan:
   .....
5. Setelah selesai membuat laporan, kemukakan hasilnya secara lisan di hadapan guru dan teman sekelas! Jika ada tanggapan dan pertanyaan dari guru dan teman sekelas, tanggapilah secara responsif!
   Tanggapan:
   .....
   .....

Permasalahan dan Penyelesaian

Permasalahan 7.1:

Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan. Apa saja elemen pembentuk keamanan jaringan?

Penyelesaian:

Ada dua elemen utama pembentuk keamanan jaringan, yaitu:

1. Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindungan pada jaringan, baik secara fisik (kenyataan) maupun maya (menggunakan *software*).
2. Rencana pengamanan, yaitu suatu rancangan yang nantinya akan diimplementasikan untuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan.

Bagaimana pendapatmu (minimal 10 kata):

.....
.....

Apa alasannya (minimal 20 kata):

.....
.....

Permasalahan 7.2:

Untuk menangkal dari segala macam gangguan, serangan, dan ancaman keamanan jaringan, apa yang harus kita lakukan dalam menghadapi hal tersebut?

Penyelesaian:

Tips Keamanan Jaringan

1. Gunakan AntiVirus.

   Tentu saja hal ini yang paling penting. Antivirus yang akan mencegah berbagai macam virus komputer. Gunakan antivirus yang sesuai dengan spesifikasi pada jaringan komputer. Dan *update* antivirus, agar antivirus dapat mendeteksi virus-virus baru.

2. Hati-hati saat *browsing*.

   Kebanyakan *pathogen* internet menyebar dari situs porno maupun mp3 ilegal, program bajakan dan sebagainya. Jika tidak mau terkena *pathogen*, jangan mengunjungi situs tersebut. Ini cara terbaik dalam mencegah *pathogen* komputer.

3. *Update* Komputer.

   Jangan lupa untuk selalu meng-*update* apapun demi keamanan komputer. Bukan hanya antivirus saja yang di-*update*. Semuanya saja, baik itu *Operating System*-nya, *software* yang ter-*install* maupun *driver*.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....

B. Metode dan Jenis Keamanan Jaringan

1. Metode Keamanan Jaringan

Secara mendasar terdapat dua elemen utama pembentuk keamanan jaringan berupa tembok pengaman dan rencana pengamanan. Tembok pengaman secara fisik maupun maya sebagai cara untuk memberikan proteksi atau perlindungan pada jaringan, baik secara fisik (kenyataan) maupun maya (menggunakan *software*). Sedangkan rencana pengamanan identik dengan suatu rancangan yang nantinya akan diimplementasikan untuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan. Oleh sebab itu, dalam merencanakan suatu sistem keamanan jaringan terdapat beberapa metode yang dapat ditetapkan. Metode-metode tersebut antara lain sebagai berikut.

a. Pembatasan Akses pada Suatu Jaringan

Beberapa konsep dalam pembatasan akses jaringan yaitu sebagai berikut.

1) Internet Password Authentication

Password local untuk login ke sistem harus merupakan *password* yang baik serta dijaga dengan baik. Pengguna aplikasi *shadow password* akan sangat membantu.

2) Server-Based Password Authentication

Metode ini misalnya sistem *kerbros server*, *TCP-wrapper*, di mana setiap *service* yang disediakan oleh *server* tertentu dengan suatu daftar *host* dan *user* yang boleh dan tidak boleh menggunakan *service* tersebut.

3) Server-Based Token Authentication

Metode ini menggunakan *authentication system* yang lebih ketat, yaitu dengan menggunakan token/*smart card*, sehingga untuk akses tertentu hanya bisa dilakukan oleh *login* tertentu dengan menggunakan token khusus.

4) *Firewall dan Routing Control*

Firewall melindungi *host-host* pada sebuah *network* dari berbagai serangan. Dengan adanya *firewall* semua paket ke sistem di belakang *firewall* dari jaringan luar tidak dapat dilakukan langsung. Semua hubungan harus dilakukan dengan mesin *firewall*.

b. *Menggunakan Metode dan Mekanisme Tertentu*

Dengan adanya pemantauan yang teratur maka penggunaan sistem oleh yang tidak berhak dapat dihindari/cepat diketahui. Untuk mendeteksi aktivitas yang tidak normal, maka perlu diketahui aktivitas yang normal. Bila hal-hal yang mencurigakan terjadi, maka perlu dijaga kemungkinan adanya intruder. Beberapa metode dan mekanisme tertentu dapat dilakukan dengan cara sebagai berikut.

Tabel 7.3 Metode dan Mekanisme untuk Mendeteksi Aktivitas yang Tidak Normal

No.	Metode	Keterangan
1.	Enkripsi	Salah satu pembatasan akses adalah dengan enkripsi. Proses enkripsi meng-*code* data dalam bentuk yang hanya dapat dibaca oleh sistem yang memiliki kunci untuk membaca data.
2.	Kriptografi	Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman.
3.	Enkripsi-Deskripsi	Proses yang digunakan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *cipertext*) adalah enkripsi (*encryption*). *Chipertext* adalan sebuah pesan yang sudah tidak dapat dibaca dengan mudah.
4.	*Digital Signature*	Digunakan untuk menyediakan *authentication*, perlindungan, integritas, dan *non-repudiation*.
5.	Algoritma Checksum/Hash	Digunakan untuk menyediakan perlindungan integritas, dan dapat menyediakan *authentication*. Satu atau lebih mekanisme dikombinasikan untuk menyediakan *security service*.

2. Jenis-Jenis Keamanan Jaringan

Jenis-jenis keamanan jaringan antara lain sebagai berikut.

a. Autentikasi adalah proses penganalan peralatan, sistem operasi, aplikasi, dan identitas *user* yang terhubung dengan jaringan komputer. Misalnya *user* memasukkan *username* dan *password* pada saat *login* ke jaringan.

b. Enkripsi (kerahasiaan data) adalah teknik pengkodean data yang dapat berguna untuk menjaga data.

c. VPN (*Virtual Private Network*) adalah jaringan komunikasi lokal yang dapat terhubung melalui media jaringan. Fungsi dari VPN sendiri adalah untuk memperoleh komunikasi yang aman melalui internet.

d. DMZ (*De-Militerized Zone*) berfungsi untuk melindungi sistem internal dari serangan *hacker*.

3. Klasifikasi Serangan ke Jaringan Komputer

Jika dilihat dari lubang keamanan yang ada pada suatu sistem, maka keamanan dapat dikategorikan sebagai berikut.

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 dapat memiliki akses).

b. *Keamanan Data dan Media*

Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada *software* yang digunakan untuk mengolah data. Cara lainnya adalah dengan memasang *backdoor* atau *Trojan horse* pada sistem target.

c. *Keamanan dari Pihak Luar*

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

d. *Keamanan dalam Operasi*

Keamanan dalam operasi merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Dengan demikian sistem tersebut dapat berjalan dengan baik atau menjadi normal kembali. **(Sumber:** Patwiyanto, Sri Wahyuni, Sumari Agus Prasetyo, 2018)

LKPD 7.2

A. Judul Kegiatan : Mengidentifikasi Metode dan Jenis Keamanan Jaringan

B. Jenis Kegiatan : Kerja Mandiri

C. Tujuan Kegiatan : 1) Peserta didik dapat menjelaskan metode dan jenis keamanan jaringan dengan tepat. (KD 3)

2) Peserta didik dapat mengimplementasikan metode dan jenis kemanan jaringan komputer dan melakukan klasifikasi perngamanan terhadap serangan jaringan komputer dengan terampil. (KD 4)

D. Langkah-Langkah Kegiatan

1. Baca dan cermati cuplikan artikel tentang sistem keamanan jaringan jaringan berikut ini!

Sistem Keamanan Jaringan Komputer

Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan. Tujuan membuat keamanan jaringan adalah untuk mengantisipasi risiko jaringan berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung yang dapat mengganggu aktivitas yang sedang berlangsung dalam jaringan.

Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan yang benar-benar aman. Karena sifat jaringan adalah melakukan komunikasi, dan setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan. Oleh sebab itu keamanan jaringan sangatlah dibutuhkan.

.....

Dikutip dari: *http://itgeek.id/sistem-keamanan-jaringan-komputer/*, diakses 18 Oktober 2018, 13.25 WIB

Hasil pengamatan:

.....

.....

2. Kumpulkanlah beberapa informasi tentang sistem keamanan jaringan dari berbagai sumber yang dianggap relevan!

Hasil informasi yang diperoleh:

.....

.....

3. Lakukanlah analisis tentang sistem keamanan jaringan meliputi:
   a. Metode keamanan jaringan.
   b. Jenis-jenis keamanan jaringan.
   c. Klasifikasi serangan ke jaringan komputer.

   Hasil analisis:

   a. .....
   b. .....
   c. .....

4. Coba implementasikan metode dan jenis kemanan jaringan komputer dan lakukan klasifikasi pengamanan terhadap serangan jaringan komputer! Kemudian buatlah laporan dari hasil percobaan yang telah kamu lakukan!

   Hasil percobaan:

   .....
   .....

   Hasil laporan:

   .....
   .....

5. Setelah selesai membuat laporan, kemukakan hasilnya secara lisan di hadapan guru dan teman sekelas! Jika ada tanggapan dan pertanyaan dari guru dan teman sekelas, tanggapilah secara responsif!

   Tanggapan:

   .....
   .....

Permasalahan dan Penyelesaian

Permasalahan 7.3:

Metodologi keamanan informasi bertujuan untuk meminimalisasi kerusakan dan memelihara keberlangsungan bisnis dengan memerhatikan semua kemungkinan kelemahan dan ancaman terhadap aset informasi. Untuk menjamin keberlangsungan bisnis, metodologi keamanan informasi berusaha memastikan kerahasiaan, integritas dan ketersediaan aset informasi internal. Apa alasan keamanan jaringan itu sangat penting? Berikan contohnya!

Penyelesaian:

Beberapa alasan keamanan jaringan sangat penting karena:

1. Dapat menjaga informasi dari orang yang tidak berhak mengakses.
   Contoh: data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, *social security*, number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya).
2. Informasi tidak boleh diubah tanpa seijin pemilik informasi.
   Contoh: *e-mail* di *intercept* di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
3. Berhubungan dengan ketersediaan informasi ketika dibutuhkan.
   Contoh: di mana *server* dikirimi permintaan (biasanya palsu) yang berturut-turut atau permintaan lain atau bahkan sampai *down*, *hang*, *crash*.

Bagaimana pendapatmu (minimal 10 kata):

.....
.....

Apa alasannya (minimal 20 kata):

.....
.....

Permasalahan 7.4:

Sistem keamanan jaringan memiliki beberapa syarat yang harus dipenuhi. Sebut dan jelaskan syarat-syarat keamanan jaringan!

Penyelesaian:

Syarat-syarat keamanan jaringan:

1. *Prevention* (pencegahan), akses yang tidak diinginkan ke dalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (*services*) yang berjalan dengan hati-hati.
2. *Observation* (observasi), perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. Sistem IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidakpedulian pada informasi *log* yang disediakan.
3. *Response* (respons), bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu sistem telah berhasil disusupi, maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktivitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....

C. Konfigurasi Sistem Keamanan Jaringan

Di masa sekarang, penggunaan *Firewall* menjadi istilah yang merujuk pada sistem yang mengatur komunikasi antara dua jenis jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan jaringan berbadan hukum di dalamnya, maka perlu adanya perlindungan terhadap piranti digital dari serangan pemata-mata, para peretas, ataupun pencuri data lainnya menjadi sebuah realita. Dengan demikian, *Firewall* identik dengan suatu sistem piranti lunak yang mengizinkan lalu lintas jaringan yang dianggap aman. Umumnya, sebuah *Firewall* diterapkan dalam sebuah mesin terdedikasi yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dengan jaringan internet. *Firewall* digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

1. Dasar-Dasar Konfigurasi Sistem Keamanan Jaringan

Firewall berfungsi untuk memfilter semua paket yang lewat pada dirinya, baik dari jaringan lokal ataupun internet. Aplikasi *server* yang satu ini sangatlah penting untuk melindungi jaringan lokal dari serangan luar. Supaya *client* bisa mendapatkan koneksi internet dari Debian 8 yang dijadikan *router* harus men-*setting Firewall*. Aplikasi *Firewall* yang terkenal pada Linux adalah *IpTables* dan *Shorewall*. Pada distribusi Linux jenis terbaru, *IpTables* secara *default* sudah ter-*install*. Dengan catatan, bahwa kernel dari Linux OS yang digunakan minimal kernel 2.4 ke atas dengan *IpTables* (*netfilter*) aktif. Beberapa *tools* yang berhubungan dengan *Firewall* (*IpTables*) dikategorikan sebagai berikut.

a. IpTables

IpTables identik dengan tools dalam Linux OS yang berfungsi sebagai sarana dalam melakukan filter (penyaringan) terhadap *traffic* lalu lintas data. Dengan *IpTables* inilah seorang *administrator* akan mengatur semua arus lalu lintas yang masuk/keluar ke komputer, ataupun *traffic* yang sekedar melewati komputer *client*.

b. *Prerouting*

Prerouting digunakan untuk melakukan NAT paket data yang memasuki *Firewall*. Pada umunya digunakan pada *transparency proxy server* dan membangun beberapa server dengan satu IP publik.

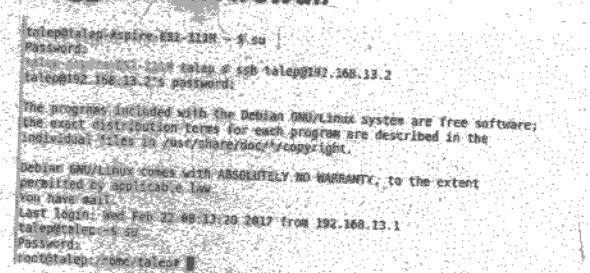
c. *Postrouting*

Postrouting digunakan untuk melakukan NAT paket data yang keluar dari *Firewall*. Pada umumnya banyak digunakan untuk translasi alamat IP.

2. Konfigurasi Sistem Keamanan Jaringan Menggunakan *Firewall*

Langkah-langkah dalam menjalankan *IpTables* dengan *user root* yaitu sebagai berikut.

a. Diawali dengan melakukan *remote server* terlebih dahulu. Perhatikan Gambar 7.4 di samping.



Sumber: *https://3.bp.blogspot.com*, diakses 19 Oktober 2018, 13.40 WIB

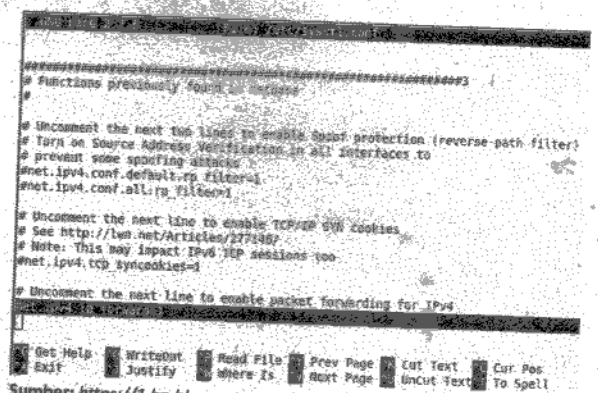
Gambar 7.4 *Remote server*

b. Selanjutnya untuk mengaktifkan *forwarder* pada Debian dengan cara mengedit *file sysctl.conf* yang terletak di folder */etc/* menggunakan *text editor nano*. Perintah yang digunakan adalah sebagai berikut.

```
# nano /etc/sysctl.conf
```

c. Selanjutnya, hilangkan tanda pagar pada teks "*net.ipv4.IP_forward=1*". Perhatikan Gambar 7.5 di samping.

Selanjutnya, simpan dengan menekan tombol kombinasi CTRL+X dilanjutkan dengan menekan tombol "Y" dan diakhiri dengan menekan tombol Enter.



Sumber: *https://1.bp.blogspot.com*, diakses 19 Oktober 2018, 14.00 WIB

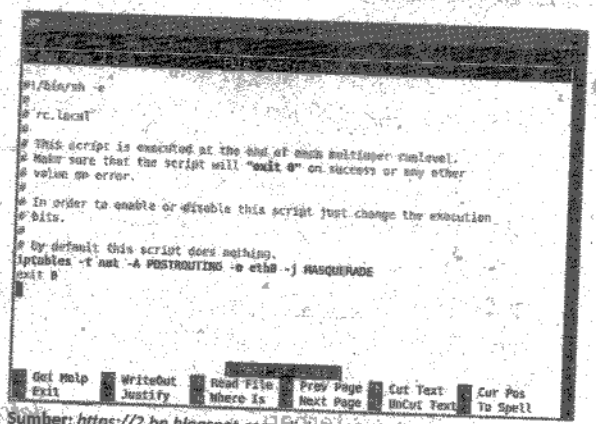
Gambar 7.5 Menghilangkan tanda pagar pada teks "*net.ipv4.ip_forward=1*"

d. Untuk mengedit *file rc.local* yang terletak di folder */etc/* menggunakan *text editor nano*. Perintah yang digunakan sebagai berikut.

```
# nano /etc/rc.local
```

e. Selanjutnya, menambahkan teks "*ip tables -t nat -A POSTROUTING -o etho -j MASQUER*" dengan cara seperti pada Gambar 7.6 di samping.

Selanjutnya, simpan dengan menekan tombol kombinasi CTRL+X dilanjutkan dengan menekan tombol "Y" dan diakhiri dengan menekan tombol Enter.



Sumber: *https://2.bp.blogspot.com*, diakses 19 Oktober 2018, 14.20 WIB

Gambar 7.6 Menambahkan teks "*ip tables -t nat -A POSTROUTING -o eth0 - j MASQUER*"

f. Ketikkan perintah untuk membuat *IP_forward* dengan cara sebagai berikut.

```
# echo 1 >> /proc/sys/net/ipv4/
ip_forward
```

g. Pada tahap terakhir, melakukan *restart* dengan memberikan perintah sebagai berikut.

```
# service rc.local start
```

(**Sumber:** Patwiyanto, Sri Wahyuni, Sumari Agus Prasetyo, 2018)

Kegiatan 7.3

A. **Judul Kegiatan** : Memahami Konfigurasi Sistem Keamanan Jaringan Menggunakan *Firewall*
B. **Jenis Kegiatan** : Praktikum Kelompok
C. **Tempat** : Laboratorium Komputer/Ruang Kelas
D. **Tujuan Kegiatan** : 1) Peserta didik dapat mengetahui dan memahami cara melakukan konfigurasi sistem keamanan jaringan menggunakan *firewall* dengan tepat. (KD 3)
2) Peserta didik dapat melakukan konfigurasi sistem keamanan jaringan menggunakan *firewall* dengan terampil. (KD 4)
E. **Alat dan Bahan:** *Debian router*, koneksi internet, laptop/PC, dan *server*.
F. **Langkah-Langkah Praktikum**

1. Bentuklah kelompok dengan membagi jumlah peserta didik dalam kelasmu menjadi 5 kelompok. Lalu pertama kali siapkan alat dan bahan yang diperlukan dalam melakukan konfigurasi sistem keamanan jaringan menggunakan *firewall*!
2. Setelah semua peralatan dan bahan siap, maka mulai melakukan praktik konfigurasi sistem keamanan jaringan menggunakan *firewall*!
3. Praktikkan langkah demi langkah dalam konfigurasi sistem keamanan jaringan menggunakan *firewall* seperti pada pembahasan materi di atas dengan runtut!
4. Setelah berhasil melakukan praktik di atas, selanjutnya buatlah laporan hasil kerja dalam kolom yang sudah disediakan di bawah ini!

G. **Laporan Praktikum**

.....

.....

.....

Permasalahan dan Penyelesaian

Permasalahan 7.5:

Salah satu tugas *firewall* adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa peraturan pengaturan akses (*access control*), penggunaan SPI, *application proxy*, atau kombinasi dari semuanya untuk mencegah *host* yang dilindungi dapat diakses oleh *host-host* yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan. *Firewall* juga mampu mencatat semua kejadian, dan melaporkan kepada *administrator*. mencatat apa-apa saja yang terjadi di *firewall* amatlah penting, sehingga bisa membantu kita untuk memperkirakan kemungkinan penjebolan keamanan atau memberikan umpan balik yang berguna tentang kinerja *firewall*. Bagaimana cara kerja *firewall*?

Penyelesaian:

Cara kerja *firewall* yaitu sebagai berikut.

1. Menutup *traffic* yang datang (*incoming network traffic*) berdasarkan sumber atau tujuan dari *traffic* tersebut: memblok *incoming network traffic* yang tidak diinginkan adalah fitur yang paling umum yang disediakan oleh *firewall*.
2. Menutup *traffic* yang keluar (*outgoing network traffic*) berdasarkan sumber atau tujuan dari *traffic* tersebut: *firewall* juga bisa menyaring *traffic* yang yang berasal dari jaringan internal ke Internet, misalnya ketika ingin mencegah *user* mengakses situs-situs porno.

3. Menutup *traffic* berdasarkan kontennya: *firewall* yang lebih canggih dapat memonitor *traffic* dari konten-konten yang tidak diinginkan, misalnya *firewall* yang di dalamnya terintegrasi antivirus ia dapat mencegah *file* yang terinveksi oleh virus masuk ke komputer atau jaringan komputer internal yang dimiliki.
4. Melaporkan *traffic* di jaringan dan kegiatan *firewall*: ketika memonitor *traffic* jaringan dari dan ke Internet, yang juga penting adalah mengetahui apa yang dikerjakan oleh *firewall*, siapa yang mencoba membobol jaringan internal dan siapa yang mencoba mengakses informasi yang tidak layak dari Internet.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....

Permasalahan 7.6:

Untuk membangun sebuah jaringan yang memiliki pengamanan *firewall*, maka dibutuhkan *hardware* yang digunakan sebagai *server*. Selain *hardware*, sistem operasi harus diinstalasi agar jaringan dapat berfungsi dengan baik, seperti: Windows Server 2000, Windows Server 2003, Linux, Fedora, Mandriva, Debian, Ubuntu, FreeBSD dan Sun Solaris. Selanjutnya pada server tersebut diinstalasi Paket program *Firewall*, seperti: WinGate, Microsoft ISA, Firestarter, dan Shorewall. Bagaimana langkah-langkah membangun *firewall*?

Penyelesaian:

Langkah-langkah membangun *firewall*, yaitu sebagai berikut.

1. Mengidentifikasi bentuk jaringan yang dimiliki.

   Mengetahui bentuk jaringan yang dimiliki khususnya toplogi yang digunakan serta protokol jaringan, akan memudahkan dalam mendesain sebuah *firewall*.
2. Menentukan *Policy* atau kebijakan dengan mengidentifikasi hal-hal berikut.
   a. Menentukan apa saja yang perlu dilayani.
   b. Menentukan individu atau kelompok-kelompok yang akan dikenakan *policy* atau kebijakan tersebut.
   c. Menentukan layanan-layanan yang dibutuhkan oleh tiap-tiap individu atau kelompok yang menggunakan jaringan.
   d. Berdasarkan setiap layanan yang di gunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman.
   e. Menerapkan semua *policy* atau kebijakan tersebut.
3. Menyiapkan *Software/Hardware* yang akan digunakan.

   Baik itu *operating system* yang mendukung atau *software-software* khusus pendukung *firewall* seperti *ipchains*, atau *iptables* pada linux, dan sebagainya. Serta konfigurasi *hardware* yang akan mendukung *firewall* tersebut.
4. Melakukan test konfigurasi.

   Pengujian terhadap *firewall* yang telah selesai dibangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan *tool-tool* yang biasa dilakukan untuk mengaudit seperti nmap.

Bagaimana pendapatmu (minimal 10 kata):

.....

.....

Apa alasannya (minimal 20 kata):

.....

.....

HOTS *(High Order Thinking Skills)*

A. Pilihlah satu jawaban yang paling benar dengan cara memberi tanda silang (X) pada huruf *A, B, C, D,* atau *E* serta tuliskan alasannya!

1. *Firewall* berfungsi untuk memfilter semua paket yang lewat pada dirinya, baik dari jaringan lokal ataupun internet. Aplikasi server yang satu ini sangatlah penting untuk melindungi jaringan lokal dari serangan luar. Supaya *client* bisa mendapatkan koneksi internet dari Debian 8 yang dijadikan *router* harus men-*setting Firewall*. Aplikasi *Firewall* yang terkenal pada Linux adalah *IpTables* dan *Shorewall*. Pada distribusi Linux jenis terbaru, *IpTables* secara *default* sudah ter-*install*. Dengan catatan, bahwa kernel dari Linux OS yang digunakan minimal kernel ....

   A. 2.4
   B. 2.3
   C. 2.2
   D. 2.1
   E. 2.2

   Alasan: .....

2. Jenis *tools* dalam Linux OS yang berfungsi sebagai sarana dalam melakukan *filter* (penyaringan) terhadap *traffic* lalu lintas data identik dengan ....

   A. *IpConflict*
   B. *Prerouting*
   C. *IpTables*
   D. *IpRecord*
   E. *Postrouting*

   Alasan: .....

3. Untuk mengaktifkan *forwarder* pada Debian dengan cara mengedit *file sysctl.conf* yang terletak di folder */etc/* menggunakan *text editor nano*. Perintah yang digunakan adalah ....

   A. `# nano /etc/rc.local`
   B. `# nano /etc/sysctl.conf`
   C. `# echo 1 >> /proc/sys/net/ipv4/ip_forward`
   D. `# service rc.local start`
   E. semua jawaban salah

   Alasan: .....

4. Jika dilihat dari lubang keamanan yang ada pada suatu sistem, proses pengawasan dan penyadapan untuk mendapatkan *password* agar bisa memiliki akses masuk ke dalam kategori ....

   A. *physical*
   B. *backdoor*
   C. *trojan horse*
   D. *wiretapping*
   E. *cracker*

   Alasan: .....

5. Untuk mengedit *file rc.local* yang terletak di folder */etc/* menggunakan *text editor nano*. Perintah yang digunakan adalah ....

   A. `# nano /etc/sysctl.conf`
   B. `# nano /etc/rc.local`
   C. `# echo 1 >> /proc/sys/net/ipv4/ip_forward`
   D. `# service rc.local start`
   E. semua jawaban salah

   Alasan: .....

B. Jawablah pertanyaan berikut dengan tepat!

1. Jabarkan yang kamu ketahui tentang perbedaan serangan pasif dan serangan aktif dalam sebuah jaringan!

   Jawaban: .....

2. Terangkan yang kamu ketahui tentang *Denial of Services* (DoS)!

Jawaban: .....

3. Sebutkan dan jelaskan jenis-jenis keamanan jaringan jika dilihat dari lubang keamanan yang ada pada suatu sistem!

Jawaban: .....

4. Uraikan yang kamu ketahui tentang dasar-dasar konfigurasi sistem keamanan jaringan!

Jawaban: .....

5. Jelaskan yang kamu ketahui tentang langkah-langkah konfigurasi sistem keamanan jaringan mengggunakan *Firewall*!

Jawaban: .....

Studi Kasus

I. Baca dan pahamilah teks berikut!

Sistem Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu *system* yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

1. Elemen pembentukan keamanan jaringan

   Ada dua elemen utama pembentuk keamanan jaringan:

   a. Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindugan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan *software*).

   b. Rencana pengamanan, yaitu suatu rancangan yang nantinya akan diimplementasikan untuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan.

Disarikan dari: *http://ppg.spada.ristekdikti.go.id/pluginfile.php/5727/mod_resource/content/2/UNM-TKI2-KB3-PDF-.pdf*, diakses 20 Oktober 2018

Dalam rangka memperdalam pemahamanmu mengenai materi sistem keamanan jaringan, kerjakan tugas berikut dengan menggunakan model pembelajaran *Discovery Learning*. Analisislah sistem keamanan jaringan yang telah kamu pelajari selama ini sesuai dengan teks di atas. Tulislah hasil analisismu sesuai dengan tahapan berikut.

A. Rumusan Masalah

1. .....
2. .....

B. Kajian Pustaka

1. .....
2. .....

C. Pengumpulan Data dan Informasi

1. .....
2. .....

D. Analisis Data

1. .....
2. .....

E. Simpulan

.....

.....

II. Cermati dan pahamilah teks berikut!

Keamanan Jaringan Internet dan *Firewall*

Serangan terhadap keamanan sistem informasi (*security attack*) dewasa ini seringkali terjadi. Kejahatan kcomputer (*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:

1. *Interception* yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi.
2. *Interruption* yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa *login*.
3. *Fabrication* yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target.
4. *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:

1. 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.

Disarikan dari: *https://aptika.kominfo.go.id/index.php/artikel/190-keamanan-jaringan-internet-dan-firewall.html*, diakses 23 Mei 2018

Teks di atas menjelaskan tentang keamanan jaringan internet dan *firewall*. Semua permasalahan yang sering terjadi pada sistem keamanan jaringan akan dapat teratasi apabila mengetahui dan memahami prosedur dalam melakukan konfigurasi sistem keamanan jaringan yang baik dan benar. Untuk mempertajam analisismu secara komprehensif mengenai permasalahan yang sering terjadi pada sistem keamanan jaringan seperti pada teks di atas, lakukan analisis masalah menggunakan model *Problem Based Learning* dengan melengkapi tahapan-tahapan berikut. Analisislah mengenai permasalahan yang sering terjadi pada sistem keamanan jaringan.

A. Rumusan Masalah

1. .....
2. .....

B. Aktivitas/Kegiatan Belajar untuk Menyelesaikan Masalah

No	Aktivitas Pembelajaran Penyelesaian Masalah	Hasil yang Dicapai
1.	Diskusi Kelompok	Simpulan hasil diskusi: 1. ..... 2. .....
2.	Observasi	Hasil praktik: 1. ..... 2. .....

C. Analisis Data

.....

.....

D. **Simpulan Solusi Masalah secara Kelompok**

.....

.....

III. **Buatlah kelompok yang beranggotakan 4–5 orang! Bersama kelompokmu carilah informasi mengenai langkah-langkah melakukan konfigurasi sistem keamanan jaringan menggunakan *firewall*! Buatlah rancangan konfigurasi sistem keamanan jaringan menggunakan *firewall*! Kerjakan tugas di bawah ini dengan menggunakan model *Project Based Learning*. Kemudian, lengkapilah langkah-langkah berikut.**

A. **Judul Projek:** .....

B. **Jenis Tugas**: Kelompok

C. **Jadwal Pelaksanaan**

Tahapan	Tanggal Pelaksanaan	Jenis Kegiatan
1. Persiapan	....	1. Mencari referensi. 2. Mempersiapkan perlengkapan yang dibutuhkan. 3. .....
2. Pelaksanaan	....	1. ..... 2. ..... 3. .....
3. Pelaporan dan Evaluasi	....	1. Membuat laporan hasil pengamatan secara sederhana. 2. ..... 3. .....

D. **Sumber Data**

1. Pengamatan di lingkungan sekitar.
2. Narasumber:
   a. Guru TIK.
   b. .....
3. Referensi:
   a. .....
   b. .....

E. **Cara Mengumpulkan Data**

1. Melakukan observasi
   a. .....
   b. .....
2. Melakukan praktik konfigurasi sistem keamanan jaringan menggunakan *firewall*
   a. .....
   b. .....

F. **Analisis Data**

1. Hasil analisis data observasi
   a. .....
   b. .....
2. Hasil analisis data praktik
   a. .....
   b. .....

G. **Simpulan Hasil Analisis**

.....

.....

Uji Kompetensi

Pilihlah satu jawaban yang paling benar dengan cara memberi tanda silang (X) pada huruf *A, B, C, D* atau *E* serta tuliskan alasannya!

1. Prinsip yang menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi dengan penggunaan digital *signature, certificates,* dan teknologi kriptografi secara umum adalah ....
   A. kerahasiaan
   B. integritas
   C. ketersediaan
   D. *authentication*
   E. *non-repudiation*

   Alasan: .....

2. Berikut ini tipe serangan yang mana penyerang telah menyisipkan objek palsu ke dalam sistem target disebut ....
   A. *interception*
   B. *interruption*
   C. *fabrication*
   D. *modification*
   E. *identification*

   Alasan: .....

3. Pencurian nomor kartu kredit yang digunakan untuk bertransaksi *online* termasuk jenis gangguan keamanan jaringan yang bernama ....
   A. *carding*
   B. *physing*
   C. *deface*
   D. *hacking*
   E. *sniffer*

   Alasan: .....

4. Serangan pasif diterjemahkan sebagai serangan yang hanya mengamati atau memonitor pengiriman informasi ke tujuan dan tidak bertujuan menyisipkan data pada aliran data tertentu pada sistem ....
   A. jaringan
   B. autentikasi
   C. komunikasi
   D. identifikasi
   E. *interruption*

   Alasan: .....

5. Jika seseorang dengan sengaja mengirimkan paket data dalam jumlah yang sangat besar terhadap suatu *server* di mana *server* tersebut tidak bisa memproses semuanya, merupakan bentuk serangan ....
   A. *system crash*
   B. *refelective deniel*
   C. *brute force and dictionary*
   D. *deniel of services*
   E. *man-in-the-midle*

   Alasan: .....

6. Serangan keamanan jaringan *Ping of Death* adalah serangan ping yang ....
   A. *oversize*
   B. *config.sys*
   C. *buffers.sys*
   D. *lowersize*
   E. *mediumsize*

   Alasan: .....

7. Berikut ini yang bukan termasuk konsep dalam pembatasan akses jaringan adalah ....
   A. *internal password authentication*
   B. *server based password authentication*
   C. *server-based token authentication*
   D. *firewall* dan *routing control*
   E. *system crash and freeze power*

   Alasan: .....

8. Ilmu dan seni untuk menjaga pesan agar aman sering disebut ....
   A. *encription*
   B. *description*
   C. *digital signature*
   D. *cryptography*
   E. *algoritma checksum*

   Alasan: .....

Perhatikan petunjuk berikut untuk dapat menyelesaikan soal nomor 9 dan 10!

Petunjuk:

A. *Jika pernyataan benar, alasan benar, dan keduanya menunjukkan hubungan sebab–akibat.*
B. *Jika pernyataan benar, alasan benar, tetapi keduanya tidak menunjukkan hubungan sebab–akibat.*
C. *Jika pernyataan benar, alasan salah.*
D. *Jika pernyataan salah, alasan benar.*
E. *Jika pernyataan dan alasan salah.*

Pernyataan:

9. Secara mendasar terdapat dua elemen utama pembentuk keamanan jaringan berupa tembok pengaman dan rencana pengamanan. Tembok pengaman secara fisik maupun maya sebagai cara untuk memberikan proteksi atau perlindungan pada jaringan, baik secara fisik (kenyataan) maupun maya (menggunakan *software*).

Sebab

Sedangkan rencana pengamanan identik dengan suatu rancangan yang nantinya akan diimplementasikan untuk melindungi jaringan agar terhindar dari berbagai ancaman dalam jaringan. Oleh sebab itu, dalam merencanakan suatu sistem keamanan jaringan terdapat beberapa metode yang dapat ditetapkan.

Jawaban: .....

Alasan: .....

10. Di masa sekarang, penggunaan *Firewall* menjadi istilah yang merujuk pada sistem yang mengatur komunikasi antara dua jenis jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan jaringan berbadan hukum di dalamnya, maka perlu adanya perlindungan terhadap piranti digital dari serangan pemata-mata, para peretas, ataupun pencuri data lainnya menjadi sebuah realita.

Sebab

Dengan demikian, *Firewall* identik dengan suatu sistem piranti lunak yang mengizinkan lalu lintas jaringan yang dianggap aman. Umumnya, sebuah *Firewall* diterapkan dalam sebuah mesin terdedikasi yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dengan jaringan internet. *Firewall* digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

Jawaban: .....

Alasan: .....

Refleksi

Pada Bab VII, peserta didik telah mempelajari tentang Mengevaluasi Sistem Keamanan Jaringan. Materi yang telah dipahami maupun yang belum dipahami akan diberi tanda centang (✓) pada kolom di bawah ini. Peserta didik juga akan bertanya jika ada materi yang belum dipahami.

No.	Pernyataan	Keterangan	
		Paham	Belum Paham
1.	Menjelaskan dan memahami sistem keamanan jaringan.	....	....
2.	Menjelaskan cara kerja sistem keamanan jaringan.	....	....
3.	Melakukan konfigurasi sistem keamanan jaringan.	....	....
....	.....	....	....

Setelah mempelajari materi tentang Mengevaluasi Sistem Keamanan Jaringan, kamu dapat mengambil refleksi sikap sebagai berikut.

1. Kritis dalam mengamati permasalahan-permasalahan nyata yang berkaitan dengan Sistem Keamanan Jaringan.
2. .....
3. .....
4. .....

Muatan Aktivitas Peserta Didik
(Berdasar Permendikbud Nomor 8 Tahun 2016)

A. Tugas Mandiri

1. Pelajarilah kembali materi tentang sistem keamanan jaringan dengan saksama!
   Hasil pemahaman materi:
   .....
   .....
2. Buatlah makalah/*resume*/rangkuman/artikel yang berkaitan dengan dasar-dasar konfigurasi sistem keamanan jaringan terutama tentang IpTables, *Prerouting*, dan *Postrouting* beserta implementasinya!
   Hasil makalah:
   .....
   .....
3. Sumber-sumber data untuk membuat makalah/*resume*/rangkuman/artikel yang berkaitan dengan dasar-dasar konfigurasi sistem keamanan jaringan terutama tentang *IpTables*, *Prerouting*, dan *Postrouting* beserta implementasinya di atas bisa diambil dari media cetak maupun elektronik yang relevan!
   Hasil informasi yang diperoleh:
   .....
   .....
4. Susunlah makalah/*resume*/rangkuman/artikel yang kamu buat ke dalam lembar kertas HVS ukuran A4 dengan spasi 1,5 serta cetak dengan menggunakan printer!
   Hasil penyusunan makalah/*resume*/rangkuman/artikel:
   .....
   .....
5. Serahkan tugas makalah/*resume*/rangkuman/artikel yang telah kamu buat pada gurumu dengan tepat waktu untuk mendapatkan penilaian!
   Saya mengumpulkan tugas dengan:
   .....
   .....

B. Tugas Diskusi

1. Bentuklah kelompok yang beranggotakan 2–3 orang teman sekelasmu (terdiri atas laki-laki dan perempuan)!
   Ketua kelompok : .....
   Anggota I : .....
   Anggota II : .....
2. Pelajarilah kembali materi tentang sistem keamanan jaringan dengan saksama!
   Hasil pemahaman materi:
   .....
   .....
3. Coba uraikan kembali informasi yang diperoleh tentang masalah masalah konfigurasi sistem keamanan jaringan menggunakan *firewall* terutama menjalankan *IpTables* dengan *user root*!
   Hasil tugas:
   .....
   .....

4. Buatlah kesimpulan tentang masalah mengaktifkan *forwarder* pada Debian terutama dalam hal penggunaan *text editor nano*, kemudian presentasikan!

   Hasil kesimpulan:

   .....

   .....

   Hasil presentasi:

   .....

   .....

C. Tugas Projek

1. Bentuklah kelompok yang beranggotakan 2–3 orang teman sekelasmu (terdiri atas laki-laki dan perempuan)!

   Ketua kelompok : .....

   Anggota I : .....

   Anggota II : .....

2. Setelah kelompok terbentuk, berdiskusilah untuk membuat perencanaan langkah-langkah konfigurasi sistem keamanan jaringan terutama tentang *IpTables*, *Prerouting*, dan *Postrouting*! Sumber-sumber data bisa diambil dari media cetak dan elektronik yang relevan.

   Hasil diskusi:

   .....

   .....

3. Siapkan alat dan bahan yang diperlukan untuk melakukan langkah-langkah konfigurasi sistem keamanan jaringan terutama tentang *IpTables*, *Prerouting*, dan *Postrouting*!

   Alat : .....

   Bahan : .....

   Langkah kerja:

   a. .....

   b. .....

   c. .....

   d. ..... dst.

4. Lengkapilah konsep rancangan percobaan kalian dengan tabel rencana pelaksanaan projek dan perkiraan waktunya!

   Hasil konsep rancangan percobaan:

   .....

   .....

5. Laksanakanlah percobaan berdasarkan konsep rancangan yang telah kamu buat!

   Hasil percobaan:

   .....

   .....

6. Kerjakan tugas ini dalam waktu satu minggu setelah guru memberikan perintah!

   Saya mengumpulkan tugas dengan:

   .....

   .....

Interaksi Guru dan Orang Tua

Untuk mengisi *form* tabel interaksi guru dan orang tua, ikuti petunjuk gurumu!

Tabel 7.4 *Form* Interaksi Guru dan Orang Tua

Nama : ..... NIS : .....

Kelas : .....

No.	Kompetensi		Keterangan Pencapaian Kompetensi			Paraf Guru	Paraf Orang Tua
			Baik	Cukup	Kurang		
1.	KI 1	Menghayati dan mengamalkan ajaran agama yang dianutnya.	....	....	....	....	....
2.	KI 2	Menghayati dan mengamalkan perilaku jujur, disiplin, santun, peduli (gotong royong, kerja sama, toleran, damai), bertanggungjawab, responsif, dan proaktif melalui keteladanan, pemberian nasihat, penguatan, pembiasaan, dan pengondisian secara berkesinambungan serta menunjukkan sikap sebagai bagian dari solusi atas berbagai permasalahan dalam berinteraksi secara efektif dengan lingkungan sosial dan alam serta dalam menempatkan diri sebagai cerminan bangsa dalam pergaulan dunia.	....	....	....	....	....
3.	KD 3.16	Mengevaluasi sistem keamanan jaringan.	....	....	....	....	....
4.	KD 4.16	Mengonfigurasi sistem keamanan jaringan.	....	....	....	....	....

Keterangan: *Berilah tanda centang (✓) sesuai dengan pencapaian kompetensi peserta didik.*