A. INFORMASI AWAL

Penyusun	:	Muhammad Fajri, S.Kom
Nama Satuan Pendidikan	:	SMK Negeri 3 Kota Bekasi
Tahun Pelajaran	:	2023 / 2024
Mata Pelajaran	:	Teknik Komputer dan Jaringan
Fase / Kelas	:	F / XI
Alokasi Waktu	:	4 x 16 JP
Elemen	:	Keamanan Jaringan
Kompetensi Awal	:	Memahami sistem keamanan jaringan, firewall, server autentifikasi, sistem pendeteksi dan penahan ancaman / serangan yang masuk ke jaringan dan kriptografi.
Profil Pelajar Pancasila	:	1. Beriman dan bertakwa kepada Tuhan Yang Maha Esa 2. Berakhlak mulia 3. Mandiri 4. Bernalar kritis 5. Kreatif
Sarana dan Prasarana	:	1. Modul ajar 2. Video tutorial 3. Laptop / Komputer 4. Handphone 5. Jaringan internet 6. Aplikasi Whatsapp 7. Aplikasi Youtube
Target Peserta Didik	:	Semua peserta didik menjadi target yaitu : 1. Peserta didik reguler. 2. Peserta didik dengan kesulitan belajar (memiliki gaya belajar yang terbatas hanya satu gaya misalnya dengan audio). 3. Peserta didik dengan pencapaian tinggi: mencerna dan memahami dengan cepat, Mampu mencapai keterampilan berfikir aras tinggi (HOTS), dan memiliki Keterampilan memimpin.
Model Pembelajaran	:	Discovery Learning

B. KOMPETENSI INTI

1. Tujuan Pembelajaran

a. Fase F

b. Rumusan capaian pembelajaran masing-masing elemen adalah sebagai berikut :

Elemen	Capaian Pembelajaran
Keamanan Jaringan	Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server.

c. Tujuan pembelajaran yang ingin dicapai

- Menjelaskan kebijakan penggunaan jaringan yang tepat.
- Mengidentifikasi kemungkinan ancaman dan serangan terhadap keamanan jaringan.
- Menentukan sistem keamanan jaringan yang dibutuhkan berdasarkan analisis ancaman yang mungkin terjadi.
- Memahami konsep firewall dan mampu menjelaskan fungsinya pada host dan server.
- Mengidentifikasi persyaratan alat yang diperlukan untuk membangun server firewall.
- Menganalisis dan mengimplementasikan firewall di host dan server.

2. Asesmen

a. Asesmen diagnotik

b. Asesmen formatif

c. Asesmen sumatif

3. Pemahaman Bermakna

Melalui pembelajaran yang kolaboratif, peserta didik dapat memahami :

- Kebijakan penggunaan jaringan
- Kemungkinan ancaman dan serangan terhadap keamanan jaringan
- Sistem keamanan jaringan yang dibutuhkan
- Firewall pada host dan server
- Kebutuhan persyaratan alat-alat untuk membangun server firewall

- Konsep dan implementasi firewall di host dan server

4. Pertanyaan Pematik

1) Apa yang dimaksud dengan kebijakan penggunaan jaringan? Mengapa penting untuk memahami kebijakan tersebut dalam konteks keamanan jaringan?
2) Apa saja kemungkinan ancaman dan serangan yang dapat terjadi terhadap keamanan jaringan? Bagaimana cara mengidentifikasi dan menghadapinya?
3) Bagaimana cara menentukan sistem keamanan jaringan yang sesuai untuk melindungi infrastruktur dan data?
4) Apa itu firewall dan bagaimana fungsinya pada host dan server? Berikan contoh implementasi firewall di lingkungan jaringan.
5) Apa persyaratan alat yang diperlukan untuk membangun server firewall? Bagaimana cara menganalisis dan mengimplementasikan firewall di host dan server?

5. Kegiatan Pembelajaran

Pertemuan ke- 1 (4 JP x 45 menit)	
Kebijakan Penggunaan Jaringan	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Pendahuluan dan pengantar keamanan jaringan
2	Memperkenalkan topik keamanan jaringan dan pentingnya dalam dunia digital
3	Diskusi tentang kebijakan penggunaan jaringan
4	Menjelaskan konsep dan tujuan kebijakan penggunaan jaringan
5	Berdiskusi tentang konten yang harus ada dalam kebijakan penggunaan jaringan
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

Pertemuan ke- 2 (4 JP x 45 menit)	
Ancaman dan Serangan terhadap Keamanan Jaringan	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Menjelaskan ancaman dan serangan umum terhadap keamanan jaringan
2	Mengidentifikasi jenis-jenis ancaman dan serangan yang sering terjadi
3	Memberikan contoh kasus nyata tentang serangan keamanan jaringan
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

Pertemuan ke- 3 (4 JP x 45 menit)	
Kebutuhan Sistem Keamanan Jaringan	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Memberikan contoh keamanan jaringan yang umum ditemui di suatu organisasi
2	Menjelaskan perlindungan dari serangan dunia maya
3	Menjelasakan perlindungan aktivitas didalam situs website
4	Menjelaskan perlindungan akses jaringan nirkabel
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

Pertemuan ke- 4 (4 JP x 45 menit)	
Firewall pada Host dan Server	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Menjelaskan sistem keamanan jaringan dan komponen-komponennya
2	Mengidentifikasi dan menjelaskan komponen-komponen penting dalam sistem keamanan jaringan
3	Memahami konsep dan fungsionalitas firewall
4	Menerangkan konsep dasar firewall dan fungsinya dalam melindungi jaringan
5	Diskusi tentang jenis-jenis firewall dan implementasinya pada host dan server
6	Melakukan analisis konsep dan implementasi firewall pada host dan server
7	Menganalisis konsep dan metode implementasi firewall pada host dan server
8	Membahas prinsip-prinsip pengaturan kebijakan firewall yang efektif
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

Pertemuan ke- 5 (4 JP x 45 menit)	
Konsep dan Implementasi Firewall di Host dan Server	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Mengidentifikasi jenis-jenis firewall yang umum digunakan
2	Menganalisis kebutuhan dan implementasi firewall pada host dan server
3	Praktik langsung dalam mengonfigurasi dan menguji firewall
4	Melakukan praktik konfigurasi firewall menggunakan perangkat lunak simulasi
5	Menguji keefektifan firewall dalam melindungi jaringan
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

Pertemuan ke- 6 (4 JP x 45 menit)	
Kebutuhan Persyaratan Alat untuk Membangun Server Firewall	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Memahami kebutuhan persyaratan alat untuk membangun server firewall
2	Mengidentifikasi alat-alat yang diperlukan untuk membangun server firewall
3	Menganalisis kebutuhan perangkat keras dan perangkat lunak yang sesuai
4	Diskusi tentang strategi pengaturan kebijakan firewall yang efektif
5	Berdiskusi tentang pengaturan kebijakan firewall yang dapat melindungi jaringan dengan baik
6	Memahami pentingnya pembaruan kebijakan secara berkala
7	Praktik dalam mengkonfigurasi firewall untuk mengamankan jaringan
8	Melakukan praktik mengkonfigurasi firewall di lingkungan simulasi
9	Menguji keefektifan pengaturan firewall yang telah dikonfigurasi
Penutup (20 menit)	
1	Membuat kesimpulan dari materi yang sudah dipelajari
2	Memberikan refleksi dari kegiatan proses belajar
3	Memberikan evaluasi tentang materi yang diberikan

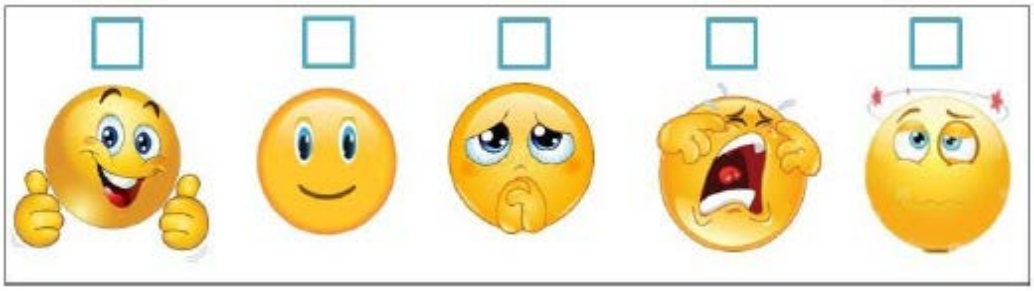
Pertemuan ke- 7 (4 JP x 45 menit)	
Evaluasi Keamanan Jaringan	
Pendahuluan (20 menit)	
1	Salam, berdoa, kondisikan kelas dan cek kehadiran peserta didik
2	Menyampaikan materi dan tujuan pembelajaran
Kegiatan Inti (140 menit)	
1	Evaluasi pemahaman peserta didik melalui tes atau kuis
2	Melakukan evaluasi pemahaman peserta didik terhadap materi keamanan jaringan
3	Memberikan tes atau kuis untuk mengukur pemahaman mereka
4	Proyek atau tugas kelompok terkait keamanan jaringan
5	Memberikan proyek atau tugas kelompok terkait keamanan jaringan
6	Mengarahkan peserta didik untuk menerapkan konsep dan keterampilan yang telah dipelajari
7	Presentasi dan diskusi hasil proyek atau tugas kelompok
8	Peserta didik mempresentasikan hasil proyek atau tugas kelompok mereka
9	Dilakukan diskusi untuk memperdalam pemahaman dan berbagi pengetahuan

Penutup (20 menit)	
1	Memberikan penutup untuk pembelajaran keamanan jaringan
2	Memberikan umpan balik kepada peserta didik mengenai perkembangan dan prestasi mereka

6. Refleksi Peserta Didik

Agar pembelajaran semakin menyenangkan dan bermakna untuk kalian, yuk sejenak berefleksi tentang aktivitas pembelajaran kali ini. Isilah penilaian diri ini dengan sejujur-jujurnya dan sebenar-benarnya sesuai dengan perasaan kalian ketika mengerjakan suplemen bahan materi ini!

Bubuhkanlah tanda centang (√) pada salah satu gambar yang dapat mewakili perasaan kalian setelah mempelajari materi ini!



1. Apa yang sudah kalian pelajari ?

   _____

   _____

2. Apa yang kalian kuasai dari materi ini ?

   _____

   _____

3. Bagian apa yang belum kalian kuasai ?

   _____

   _____

4. Apa upaya untuk menguasai yang belum kalian kuasai ?

   Coba diskusikan dengan teman maupun guru kalian

   _____

   _____

7. Refleksi Guru

Refleksi adalah kegiatan yang dilakukan dalam proses belajar mengajar dalam bentuk penilaian tertulis dan lisan oleh guru untuk siswa dan mengekspresikan kesan konstruktif, pesan, harapan dan kritik terhadap pembelajaran yang diterima, Guru dapat mengajukan pertanyaan kepada siswa,dengan minta pendapat tentang cara mengajar, suasana pembelajaran, pemahaman pembelajaran.ataupun meminta kritik dan saran kepada siswa terhadap pembelajaran dan dirinya. Hal ini dapat dilakukan menjelang pembelajaran berakhir sehingga tidak menggangu pembelajaran.

1. Apakah kegiatan membuka pelajaran yang saya lakukan dapat mengarahkan dan mempersiapkan peserta didik mengikuti pelajaran dengan baik ?
2. Bagaiaman tanggapan peserta didik terhadap materi atau bahan ajar yang saya sajikan sesuai yang diharapkan ? (apakah materi terlalu tinggi, terlalu rendah atau sesuai dengan kemampuan awal peserta didik) ?
3. Bagaimana respon peserta didik terhadap media pembelajaran yang digunakan ? apakah media sesuai dan mempermudah peserta didik menguasai kompetensi atau materi yang diajarkan ?
4. Bagaimana tanggapan peserta didik terhadap kegiatan belajar yang telah saya rancang ?
5. Bagaimana tanggapan peserta didik terhadap metode atau teknik pembelajaran yang saya gunakan ?

C. LAMPIRAN

1. Lembar Kerja Peserta Didik

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.001	Tanggal Pelaksanaan : _____	Durasi : 4 x 45 menit
	Tugas / Job : **KEBIJAKAN PENGGUNA JARINGAN**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Memperkenalkan topik keamanan jaringan dan pentingnya dalam dunia digital
2. Menjelaskan konsep dan tujuan kebijakan pengguna jaringan
3. Diskusi tentang kebijakan dan konten pengguna jaringan

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Carilah informasi dari beberapa faktor keamanan jaringan dibawah ini :

   Confidentiality

   _____

   _____

   Integrity

   _____

   _____

MUHAMMAD FAJRI

Availability

_____

_____

Authentication

_____

_____

Nonrepudiation

_____

_____

2. Tuliskan pengertian dari kebijakan organsasi dalam keamanan jaringan !

_____

_____

Berilah contoh tentang kebijakan organisasi !

_____

_____

3. Tuliskan pengertian dari etika menggunakan jaringan !

_____

_____

Berilah contoh etika menggunakan jaringan !

_____

_____

4. Tuliskan pengertian dari etika mengakses komputer !

_____

_____

Berilah contoh etika mengakses komputer !

_____

_____

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.002	Tanggal Pelaksanaan : _____	Durasi : 4 x 45 menit
	Tugas / Job : **ANCAMAN DAN SERANGAN TERHADAP KEAMANAN JARINGAN**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Menjelaskan ancaman dan serangan umum terhadap keamanan jaringan
2. Mengidentifikasi jenis-jenis ancaman dan serangan yang sering terjadi
3. Memberikan contoh kasus nyata tentang serangan keamanan jaringan

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Carilah pengertian serangan fisik terhadap keamanan jaringan !

   _____

   _____

   _____

   Berikan contoh beberapa kerugian dari serangan fisik !

   _____

   _____

MUHAMMAD FAJRI

2. Carilah pengertian serangan logic terhadap keamanan jaringan !

_____

_____

_____

Sebutkan contoh serangan logic terhadap keamanan jaringan !

_____

_____

_____

3. Apa yang kamu ketahui tentang Virus ?

_____

_____

_____

4. Apa yang kamu ketahui tentang Worm ?

_____

_____

_____

5. Apa yang kamu ketahui tentang Trojan Horse ?

_____

_____

_____

6. Apa yang kamu ketahui tentang Mallware ?

_____

_____

_____

MUHAMMAD FAJRI

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.003	Tanggal Pelaksanaan : _____	Durasi : 4 x 45 menit
	Tugas / Job : **SISTEM KEAMANAN JARINGAN YANG DIBUTUHKAN**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Memberikan contoh keamanan jaringan yang umum ditemui di suatu organisasi
2. Menjelaskan perlindungan dari serangan dunia maya
3. Menjelasakan perlindungan aktivitas didalam situs website
4. Menjelaskan perlindungan akses jaringan nirkabel

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Berilah penjelasan keamanan jaringan dalam perlindungan virus !

_____

_____

_____

_____

_____

_____

MUHAMMAD FAJRI

2. Berilah penjelasan keamanan jaringan dalam perlindungan web !

_____

_____

_____

3. Berilah penjelasan keamanan jaringan dalam perlindungan nirkabel !

_____

_____

_____

4. Berilah penjelasan keamanan jaringan dalam perlindungan keamanan aplikasi !

_____

_____

_____

5. Berilah penjelasan keamanan jaringan dalam perlindungan firewall pada windows !

_____

_____

_____

6. Berilah penjelasan keamanan jaringan dalam penyaringan konten !

_____

_____

_____

7. Berilah penjelasan keamanan jaringan dalam pencegahan kehilangan data !

_____

_____

_____

8. Berilah penjelasan keamanan jaringan dalam perlindungan email !

_____

_____

_____

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.004	Tanggal Pelaksanaan :	Durasi : 4 x 45 menit
	Tugas / Job : **FIREWALL PADA HOST DAN SERVER**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Menjelaskan sistem keamanan jaringan dan komponen-komponennya
2. Mengidentifikasi dan menjelaskan komponen-komponen penting dalam sistem keamanan jaringan
3. Memahami konsep dan fungsionalitas firewall
4. Menerangkan konsep dasar firewall dan fungsinya dalam melindungi jaringan
5. Diskusi tentang jenis-jenis firewall dan implementasinya pada host dan server
6. Melakukan analisis konsep dan implementasi firewall pada host dan server
7. Menganalisis konsep dan metode implementasi firewall pada host dan server
8 Membahas prinsip-prinsip pengaturan kebijakan firewall yang efektif

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Berilah penjelasan tentang Firewall !

2. Sebutkan fungsi Firewall !

3. Sebutkan jenis-jenis Firewall !

4. Cara Kerja Firewall !

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.005	Tanggal Pelaksanaan :	Durasi : 4 x 45 menit
	Tugas / Job : **KEBUTUHAN PRASYARAT ALAT-ALAT MEMBANGUN SERVER FIREWALL**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Memahami kebutuhan persyaratan alat untuk membangun server firewall
2. Mengidentifikasi alat-alat yang diperlukan untuk membangun server firewall
3. Menganalisis kebutuhan perangkat keras dan perangkat lunak yang sesuai
4. Diskusi tentang strategi pengaturan kebijakan firewall yang efektif
5. Berdiskusi tentang pengaturan kebijakan firewall yang dapat melindungi jaringan dengan baik
6. Memahami pentingnya pembaruan kebijakan secara berkala
7. Praktik dalam mengkonfigurasi firewall untuk mengamankan jaringan
8. Melakukan praktik mengkonfigurasi firewall di lingkungan simulasi
9. Menguji keefektifan pengaturan firewall yang telah dikonfigurasi

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Berilah penjelasan tentang Firewall !

_____

_____

2. Berilah penjelasan tentang Static Packet Filtering !

_____

_____

_____

3. Berilah penjelasan tentang Dynamic Packet Filtering !

_____

_____

_____

4. Berilah penjelasan tentang Proxy Server !

_____

_____

_____

5. Berikan langkah-langkah membangun server firewall !

_____

_____

_____

6. Berilah penjelasan tentang radius dalam keamanan jaringan !

_____

_____

_____

7. Berilah penjelasan tentang TACACS+ dalam keamanan jaringan !

_____

_____

_____

	SMK NEGERI 3 KOTA BEKASI TEKNIK KOMPUTER DAN JARINGAN		
	No. Jobsheet : XI.TKJ.JOB.006	Tanggal Pelaksanaan :	Durasi : 4 x 45 menit
	Tugas / Job : **KONSEP DAN IMPLEMENTASI FIREWALL DI HOST DAN SERVER**		

A. Elemen

Keamanan Jaringan

B. Capaian Pembelajaran

Pada akhir fase F, peserta didik mampu memahami kebijakan penggunaan jaringan, memahami kemungkinan ancaman dan serangan terhadap keamanan jaringan, menentukan sistem keamanan jaringan yang dibutuhkan, memahami firewall pada host dan server, memahami kebutuhan persyaratan alat-alat untuk membangun server firewall, menganalisis konsep dan implementasi firewall di host dan server

C. Tujuan Pembelajaran

1. Mengidentifikasi jenis-jenis firewall yang umum digunakan
2. Menganalisis kebutuhan dan implementasi firewall pada host dan server
3. Praktik langsung dalam mengonfigurasi dan menguji firewall
4. Melakukan praktik konfigurasi firewall menggunakan perangkat lunak simulasi
5. Menguji keefektifan firewall dalam melindungi jaringan

D. Alat dan Bahan

1. Komputer / Laptop / Handphone yang terhubung ke Internet
2. Buku Tulis dan Ballpoint
3. Modul Ajar Keamanan Jaringan

E. Langkah Kerja

1. Berilah penjelasan tentang firewall pada komputer !

_____

_____

_____

_____

_____

2. Sebutkan fungsi firewall pada keamanan jaringan !

_____

_____

_____

_____

_____

3. Berilah penjelasan tentang personal firewall !

_____

_____

_____

_____

_____

4. Berilah penjelasan tentang network firewall !

_____

_____

_____

_____

_____

5. Berilah penjelasan bagaimana cara kerja firewall !

_____

_____

_____

_____

_____

2. Asesmen

a. Asesmen Diagnostik

1) Asesmen Diagnostik Non-Koqnitif

Gaya belajar, karakter dan minat peserta didik

Berilah skor 1 bila jawaban "YA" dan 0 bila jawaban "TIDAK"

NO	PERNYATAAN	YA	TIDAK
1	Saya lebih suka banyak ilustrasi (gambar) saat belajar		
2	Saya lebih mudah memahami pelajaran dengan banyak ilustrasi (gambar)		
3	Saya sangat menyukai obyek yang warna warni		
4	Saya sering mengantuk dan susah fokus kalau guru menerangkan atau berbicara		
5	Saya lebih mudah mengingat materi tayangan film dari pada penjelasan guru		
6	Saya lebih mudah mengingat dari penjelasan atau pemapaparan guru		
7	Saya lebih mudah hafal apabila diucapkan berulangkali		
8	Saya lebih nyaman melafalkan dengan keras saat belajar		
9	Saya merasa asik kalau mendengarkan orang yang sedang berbicara		
10	Saya lebih suka mendengarkan rekaman daripada membaca buku teks		
11	Bongkar pasang peralatan adalah kegemaranku		
12	Saya lebih menyukai pembelajaran yang banyak melibatkan gerak badan		
13	Saya kurang suka diam lama dikit		
14	Saya lebih suka banyak gerak mesti saat belajar		
15	Saya lebih mudah belajar melalui praktik daripada mendengarkan		

2) Asesmen Diagnostik Kognitif

Untuk memperjelas pemahaman terhadap Untuk memperjelas pemahaman terhadap konsep ekonomi dan bisnis, maka perlu lakukan terlebih dahulu asesmen mandiri sebagai berikut:

Menjawab dengan jujur dari pernyataan berikut dengan memberi tanda ceklis pada kolom benar atau salah.

NO	PERNYATAAN	BENAR	SALAH
1	Integrity mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang		
2	Malicious code termasuk serangan logic terhadap keamanan jaringan		
3	Salah satu contoh perlindungan pada nirkabel adalah Wi-Fi Protected Access (WPA)		
4	Firewall server digunakan untuk melakukan akses layanan internet pada jaringan		
5	Tidak melakukan authentifikasi bukan merupakan fungsi dari firewall		

b. Asesmen Formatif

Informasi apa saja yang ingin digali ?	Pertanyaan kunci yang ingin ditanyakan
TP. 1 Mengidentifikasi faktor dari segi keamanan jaringan Mengidentifikasi konsep dan tujuan kebijakan penggunaan jaringan	 Sebutkan 3 faktor segi keamanan jaringan ? Jelaskan konsep dan tujuan kebijakan penggunaan jaringan ?
TP. 2 Menjelaskan ancaman dan serangan umum terhadap keamanan jaringan Mengidentifikasi jenis-jenis ancaman dan serangan yang sering terjadi	 Berikan 3 contoh ancaman dan serangan umum terhadap keamanan jaringan ? Sebut dan jelaskan jenis ancaman dan serangan yang terjadi ?
TP. 3 Mengidentifikasi keamanan jaringan yang umum ditemui di suatu organisasi Menjelaskan perlindungan dari serangan dunia maya	 Apa yang kamu ketahui tentang keamanan jaringan di suatu organisasi ? Sebutkan serangan dunia maya yang umum terjadi ?
TP. 4 Mengidentifikasi dan menjelaskan komponen-komponen penting dalam sistem keamanan jaringan Menerangkan konsep dasar firewall dan fungsinya dalam melindungi jaringan	 Sebut dan jelaskan komponen penting dalam sistem keamanan jaringan ? Jelaskan konsep dasar firewall ?

Informasi apa saja yang ingin digali ?	Pertanyaan kunci yang ingin ditanyakan
TP. 5 Mengidentifikasi alat-alat yang diperlukan untuk membangun server firewall Menganalisis kebutuhan perangkat keras dan perangkat lunak yang sesuai	Sebutkan alat-alat yang dibutuhkan membangun server firewall ? Bagaimana menentukan kebutuhan perangkat keras dan lunak untuk keamanan jaringan ?
TP. 6 Mengidentifikasi jenis-jenis firewall yang umum digunakan Menganalisis kebutuhan dan implementasi firewall pada host dan server	Sebutkan 3 jenis-jenis firewall yang umum digunakan ? Apa yang harus dipersiapkan untuk implementasi firewall pada host dan server?

Langkah-langkah apa saja yang akan dilakukan?	Alat bantu apa yang dibutuhkan?
✓ Membuat perangkat asesmen ✓ Menggandakan perangkat asesmen ✓ Menyiapkan lembar jawaban ✓ Membagikan lembar asesmen dan lembar jawaban ✓ Meminta siswa mengerjakan asesmen Memeriksa hasil asesmen Melakaukan penilaian ✓ Menganalisis hasil penialan ✓ Menindaklanjuti hasil penilaian	✓ Kertas HVS A4 ✓ Tinta ✓ Printer ✓ Komputer ✓ Handphone ✓ Akses internet

Waktu Asesmen	30 Menit	Durasi Asesmen	Proses pembelajaran

Identifikasi materi yang akan diujikan	Pertanyaan	Kemungkinan Jawaban	Skor (kategori)	Rencana Tindak Lanjut
Mengidentifikasi faktor dari segi keamanan jaringan	Sebutkan 3 faktor segi keamanan jaringan ?	Confidentiality Integrity Availability Authentication Nonrepudiation	B = 3 S = 0	Bila peserta didik menjawab salah, maka perlu diberikan pendampingan untuk memahami materi
Mengidentifikasi keamanan jaringan yang umum ditemui di suatu organisasi	Apa yang kamu ketahui tentang keamanan jaringan di suatu organisasi ?	Perlindungan Email, Perlindungan di Web, Perlindungan Nirkabel, Keamanan Aplikasi, Penyaringan Konten, Perlindungan Virus dan Malware		
Mengidentifikasi alat-alat yang diperlukan untuk membangun server firewall	Sebutkan alat-alat yang dibutuhkan membangun server firewall ?	Processor min. 3.0 GHz, HDD 500 Gb, RAM 2 Gb		

Lembar Observasi Diskusi Kelompok

No	Nama Peserta Didik	Aspek Yang Diamati			
		Kemampuan bekerjasama	Keaktifan dalam kelompok	Kemampuan menjelaskan materi	Kemampuan mempertahankan dan menanggapi pertanyaan atau sanggahan
1					
2					
3					
dst.					

Diisi dengan skor 1 - 4

1 Kurang 2 Cukup 3 Baik 4 Sangat Baik

Lembar Observasi Penilaian Sikap

No	Nama Peserta Didik	Sikap			
		Mandiri	Gotong Royong	Bernalar Kritis	Kreatif
1					
2					
3					
dst.					

Diisi dengan skor 1 - 4

1 Kurang 2 Cukup 3 Baik 4 Sangat Baik

c. Asesmen Sumatif

1) Pilihan Ganda

Jawablah pertanyaan berikut ini dengan memilih jawaban yang dianggap paling tepat !

1. Proses pengenalan peralatan, sistem operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer disebut...
   A. Enkripsi
   B. Deskripsi
   C. Autentikasi
   D. Konfirmasi
   E. Security

2. Berikut ini yang bukan merupakan fungsi dari Firewall adalah...
   A. Mengatur dan mengontrol lalu lintas jaringan
   B. Memcatat semua kejadian, dan melaporkan kepada administrator
   C. Melakukan autentikasi terhadap akses
   D. Melakukan pembuatan virus
   E. Melindungi sumber daya dalam jaringan privat

3. Ada beberapa faktor yang bukan Penyebab Resiko dalam Jaringan Komputer...
   A. Kelemahan manusia (human error)
   B. Kelemahan perangkat keras computer
   C. Kelemahan sistem operasi Jaringan
   D. Kelemahan sistem jaringan komunikasi
   E. Kehandalan manusia

4. Program yang sepertinya bermanfaat padahal tidak karena uploaded hidden program dan script perintah yang membuat sistem rentan gangguan adalah...
   A. Virus
   B. Spyware
   C. Worm
   D. Phising
   E. Trojan Horse

5. Serangan dengan menggunakan code berbahaya dengan menyisipkan virus, worm/trojan horse" merupakan pengertian dari...

   A. SQL injection

   B. DoS

   C. Malicious Code

   D. Traffic Flooding

   E. Social Enginering

2) Pengayaan dan Remedial

Pengayaan adalah kegiatan pembelajaran yang diberikan pada peserta didik dengan capaian tinggi agar mereka dapat mengembangkan potensinya secara optimal.

Remedial diberikan kepada peserta didik yang membutuhkan bimbingan untuk memahami materi atau pembelajaran mengulang. Saat merancang kegiatan pengayaan, perlu diperhatikan mengenai diferensiasi contohnya lembar belajar/kegiatan yang berbeda dengan kelas.

BAB I

KEBIJAKAN PENGGUNAAN JARINGAN

1.1 Pengertian

Keamanan jaringan adalah bentuk pencegahan atau deteksi pada hal yang bersifat gangguan dan akses tak seharusnya pada Sistem Jaringan Komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer.

Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Keamanan jaringan sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan dari kelima point ini.

- **Confidentiality**

  Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.

- **Integrity**

  Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

- **Availability**

  Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.

- **Authentication**

  Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.

- **Nonrepudiation**

  Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

1.2 Kebijakan Pengguna Jaringan

1.2.1 Kebijakan Organisasi

Adalah suatu kebijakan organisasi, istansi atau lembaga dalam ruang lingkup keamanan jaringanuntuk akses pada sistem jaringan di tempat tersebut. Diantara contoh dari kebijakan organisasi adalah :

- Tata kelola sistem komputer
- Pengaturan kerapian pengkabelan
- Pengaturan akses wi-fi
- Manajemen data organisasi
- Sinkronisasi antar sub-organ
- Manajemen Sumber Daya
- Maintenance dan Checking berkala

1.2.2 Etika Menggunakan Jaringan

Setiap kita melakukan suatu kegiatan pasti ada aturan atau etika yang harus dilakukan, karena jika tidak bisa berdampak negative bagi kita sendiri maupun orang lain. Begitu juga saat menggunakan jaringan kita juga harus memperhatikan etika- etika yang berlaku. Diantaranya etika tersebut adalah:

- Memahami Akses Pengguna
- Memahami kualitas daya Organisasi
- Pengaturan penempatan sub-organ

1.2.3 Kebijakan Mengakses Komputer

Dalam suatu kebijakan pengguna jaringan, tidak jarang juga terdapat kebijakan pengguna saat mengakses computer, diantaranya adalah :

- Manajemen pengguna
- Manajemen sistem komputer
- Manajemen waktu akses

BAB II

ANCAMAN DAN SERANGAN TERHADAP KEAMANAN JARINGAN

Saat kita saling terhubung dalam suatu jaringan baik jaringan kecil maupun besar, pasti terdapat ancaman ataupun seranagan yang bisa terjadi. Sehingga kita diharuskan untuk lebih berhati-hati saat berkomunikasi menggunakan jaringan. Diantara ancaman atau serangan yang bisa terjadi dari keamanan jaringan adalah :

2.1 Serangan Fisik

Kebanyakan orang beranggapan bahwa serangan terhadap keamanan jaringan cenderung pada non-hardwarenya saja, tetapi sebenarnya serangan tersebut bisa terjadi pada hardware itu sendiri. Sebagai contoh saat jaringan kita dihack oleh orang lain, maka software baik data, file ataupun aplikasi akan rusak yang bisa juga menyebabkan hardware kita tidak bekerja secara normal, sehinggan hardware kita akan mengalami kerusakan.

Serangan fisik terhadap keamanan jaringan dapat menyebabkan beberapa kerugian, diantaranya :

- Terjadi gangguan pada Kabel
- Kerusakan Harddisk
- Konsleting
- Data tak tersalur dengan baik
- Koneksi tak terdeteksi
- Akses bukan pengguna

2.2 Serangan Logik

Serangan logic pada keamanan jaringan adalah hal yang paling rawan terjadi, sehingga kita harus lebih memperhatikan lagi security dalam jaringan kita. Diantara serangan yang bisa terjadi adalah :

- SQL Injection

  adalah Hacking pada sistem komputer dengan mendapat akses Basis Data pada Sistem
- DoS (Denial of Service)

  adalah Serangan pada Sistem dengan mengabiskan Resource pada Sistem.
- Traffic Flooding

  adalah Serangan pada keamanan jaringan dengan membanjiri Traffic ata[illegible]alu lintas jaringan

- Request Flooding

  adalah Serangan dengan membanjiri banyak Request pada Sistem yang dilayani Host sehingga Request banyak dari pengguna tak terdaftar dilayani oleh layanan tersebut.

- Deface

  adalah adalah Serangan pada perubahan tampilan

- Social Engineering

  adalah Serangan pada sisi sosial dengan memanfaatkan kepercayaan pengguna. Hal ini seperti fake login hingga memanfaatkan kelemahan pengguna dalam socialmedia.

- Packet Sniffer

  adalah Serangan Menangkap paket yang lewat dalam sebuah Jaringan.

- Malicious Code

  adalah Serangan dengan menggunakan kode berbahaya dengan menyisipkan virus, worm atau Trojan Horse.

  - ✓ Virus

    Program merusak yang mereplikasi dirinya pada boot sector atau dokumen.

  - ✓ Worm

    Virus yang mereplikasi diri tidak merubah fle tapi ada di memory aktif.

  - ✓ Trojan Horse

    Program yang sepertinya bermanfaat padahal tidak karena uploaded hidden program dan scipt perintah yang membuat sistem rentan gangguan.

2.3 Peralatan Pemantau dari Ancaman dan Serangan

Peralatan pemantau (monitoring device) adalah suatu tool atau software yang digunakan para admin jaringan untuk memonitoring atau memantau jaringannya apakah ada serangan atau tidak. Dan dapat pula untuk mengetahui seseorang yang tidak diketahui atau pengguna asing.

Contoh software Pemandu:

- Autobuse

  Mendeteksi problem dengan memonitoring logfile.

- Courtney dan Portsentry

  Mendeteksi probling (port scanning) dengan memonitoring packet yang lalu lalang.

- Snort

  Mendeteksi pola (pattern) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi.

BAB III

SISTEM KEAMANAN JARINGAN YANG DIBUTUHKAN

Keamanan jaringan di perkantoran adalah upaya yang dilakukan untuk melindungi jaringan perkantoran dari akses yang tidak sah dan ancaman lainnya. Ini melibatkan berbagai macam teknik yang bisa meningkatkan keamanan jaringan, seperti pengaturan firewall, menggunakan enkripsi data, mengontrol akses ke jaringan, dan memastikan bahwa semua sistem di jaringan diperbarui dengan patch keamanan terbaru.

Keamanan jaringan penting bagi sebuah perkantoran karena ia melindungi informasi sensitif, berkas, dan data yang disimpan di jaringan. Menjaga koneksi jaringan aman dari serangan cyber, malware, dan ancaman lainnya membantu menjaga informasi rahasia dan mencegah akses tidak sah ke jaringan. Ini juga membantu menjamin bahwa data yang tersimpan di jaringan hanya dapat diakses oleh orang yang berwenang dan bahwa informasi tersebut aman dari pengakses yang tidak sah.

Ada banyak bentuk keamanan jaringan yang dirancang sesuai dengan fungsi dan tujuannya. Secara umum, jenis keamanan jaringan tertentu populer dan sering digunakan, tetapi ada juga sistem yang tidak kita kenal. Berikut ini adalah contoh keamanan jaringan yang umum ditemui untuk organisasi:

1. **Perlindungan Email**

   Email perlu dilindungi dari serangan dunia maya, pencurian data pribadi, atau informasi penting. Inilah mengapa keamanan email dirancang untuk mencegah serangan. Perlindungan email biasanya dilengkapi dengan perangkat lunak anti-spam yang berguna untuk melindungi pengguna.

2. **Perlindungan di Web**

   Keamanan jenis ini berguna untuk melindungi aktivitas di dalam situs web, terutama toko online yang penuh dengan data pelanggan. Keamanan internet biasanya berupa pemasangan sertifikat Secure Socket Layer untuk meningkatkan keamanan situs web. Situs web dengan sertifikat SSL yang terpasang ditandai dengan gembok di bilah alamat browser.

3. **Perlindungan Nirkabel**

   Jaringan nirkabel (wireless network) lebih rentan terhadap serangan, karena sistem konfigurasi dan jenis enkripsinya cukup rendah. Keamanan nirkabel berguna untuk mencegah serangan ini sehingga dapat diakses dengan lebih aman. Contohnya adalah Wi-Fi Protected Access (WPA).

4. **Perlindungan Titik Akhir**

   Perangkat yang Anda gunakan bisa menjadi target peretas untuk mencuri datanya. Endpoint Security berguna untuk melindungi perangkat pribadi seperti printer dan mesin fax yang terhubung dengan jaringan perusahaan.

5. **Keamanan Aplikasi**

   Tidak hanya website, aplikasi juga bisa menjadi hotspot pencurian data pelanggan. Untuk mencegah hal ini, organisasi harus memasang keamanan aplikasi untuk memastikan bahwa aplikasi mereka terlindungi dari serangan.

6. **Firewall**

   Sistem keamanan jaringan ini bertindak sebagai pelindung jaringan komputer internal terhadap jaringan eksternal yang mencurigakan. Firewall memeriksa lalu lintas jaringan terhadap beberapa protokol dan kemudian memblokir lalu lintas yang berpotensi berbahaya.

7. **Penyaringan Konten**

   Pemfilteran konten adalah komponen Firewall yang berguna untuk memfilter situs web atau email yang tidak pantas. Contohnya mencakup konten kekerasan, pornografi, merusak diri sendiri (bunuh diri), atau ujaran kebencian.

8. **Pencegahan Kehilangan Data**

   Pencegahan Kehilangan Data, atau singkatnya DLP, adalah alat untuk melindungi data sensitif dari insiden kehilangan atau pencurian oleh orang yang tidak berwenang. DLP dirancang untuk bekerja secara otomatis dalam memantau dan mengendalikan informasi dalam jaringan komputer.

9. **Analisis Perilaku**

   Seperti namanya, sistem keamanan jaringan ini dirancang untuk mendeteksi aktivitas atau perilaku yang aneh dan tidak normal pada jaringan komputer. Salah satu tools yaitu ADE (Anomaly Detection Engines) berguna untuk menganalisa jaringan kemudian memberitahu pengguna jaringan ketika terjadi pelanggaran.

10. **Perlindungan Virus dan Malware**

    Antivirus berguna untuk mengidentifikasi dan menghapus virus yang disematkan atau virus yang dikirim oleh penyusup. Anti-malware, di sisi lain, adalah perangkat lunak yang mendeteksi malware. Tahukah Anda, malware lebih berbahaya karena serangan ini dapat mematikan jaringan hingga beberapa minggu?

11. **Kontrol Akses**

    Jenis keamanan jaringan ini dirancang untuk mencegah perangkat yang tidak dikenal mengakses jaringan Anda. Ini dapat membatasi kemungkinan sabotase jaringan Anda. Selain itu, kontrol akses berguna untuk membatasi dan mengontrol akses pengguna jaringan ke file atau folder tertentu.

12. **Informasi Keamanan dan Manajemen Acara (SIEM)**

    SIEM bekerja dengan memberikan informasi tentang aktivitas atau catatan yang terjadi di jaringan komputer dan lingkungan TI perusahaan. Berkat SIEM ini, Anda dapat mendeteksi ancaman tersebut dan mengambil tindakan yang diperlukan.

13. **Segmentasi Jaringan**

    Segmentasi jaringan meningkatkan keamanan jaringan dengan membagi jaringan menjadi beberapa bagian. Hal ini dirancang untuk memungkinkan komputer mengelola berbagai jenis lalu lintas jaringan dan paparan terhadap ancaman jaringan.

14. **Jaringan Pribadi Virtual (VPN)**

    Alat-alat ini berguna sebagai alat otentikasi untuk komunikasi antara komputer dan perangkat jaringan. Cara kerjanya VPN membuat jalur dalam bentuk "terowongan" terenkripsi dan aman untuk menghubungkan perangkat kita untuk melindunginya dari ancaman atau gangguan jaringan.

15. **Sistem Alarm Penyusup**

    Istilah lainnya adalah Intrusion Detection and Prevention System (IDPS). Sistem ini memantau semua aktivitas online dan kemudian menganalisis aktivitas berbahaya dan mencurigakan. Selanjutnya, IDPS mengambil langkah-langkah untuk menekan serangan tersebut.

BAB IV

FIREWALL PADA HOST DAN SERVER

4.1 Pengertian Firewall

Firewall adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar. Saat ini, pengertian firewall difahami sebagai sebuah istilah generik yang merujuk pada fungsi firewall sebagai sistem pengatur komunikasi antar dua jaringan yang berlainan.

4.2 Fungsi Firewall

- Mengontrol dan mengawasi paket data yang mengalir di jaringan, Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall.
- Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan private.
- Melakukan autentifikasi terhadap akses.
- Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.
- Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

4.3 Jenis Firewall

4.3.1 Personal Firewall

Firewall yang didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya. Bahkan beberapa produk firewall lainnya dilengkapi dengan fungsi pendeteksian gangguan keamanan jaringan (Intrusion Detection System). Contoh dari firewall jenis ini adalah Microsoft Windows Firewall, Symantec Norton Personal Firewall, Kerio Personal Firewall.

4.3.2 Network Firewall

Firewall yang didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server.

Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc.

4.4 Cara Kerja Firewall

- Menolak dan memblokir paket data yang datang berdasarkan sumber dan tujaun yang tidak diinginkan.
- Menolak dan menyaring paket data yang berasal dari jaringan intenal ke internet. Contoh nya ketika ada pengguna jaringan internel akan mengakses situs-situs porno.
- Menolak dan menyaring paket data berdasakan konten yang tidak diinginkan seperti situs yang terdeteksi mengandung virus.
- Melaporkan semua aktivitas jaringan dan kegiatan firewall.

BAB V

TATA CARA PENGAMANAN PERALATAN PADA JARINGAN

5.1 Metode yang diterapkan membuat jaringan komputer aman

- **IDS / IPS**

  Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) adalah sistem yang banyak digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan oleh pihak luar maupun dalam.

- **Network Topology**

  Selain permasalahan aplikasi yang akan mempergunakan jaringan komputer, topologi jaringan komputer juga memiliki peranan yang sangat penting dalam keamanan jaringan komputer.

- **Port Scanning**

  Biasanya digunakan oleh penyerang untuk mengetahui port apa saja yang terbuka dalam sebuah sistem jaringan komputer. Tetapi metode yang sama juga dapat digunakan oleh pengelola jaringan komputer untuk menjaga jaringan komputernya.

- **Port Scanning sebagai bentuk serangan**

  Karena implementasinya yang cukup mudah dan informasinya yang cukup berguna, maka sering kali port scanning dilakukan sebagai tahap awal sebuah serangan. Untuk dapat melakukan penyerangan, seorang crackerperlu mengetahui aplikasi apa saja yang berjalan dan siap menerima koneksi dari lokasinya berada

- **Packet Fingerprinting**

  Karena keunikan setiap vendor peralatan jaringan komputer dalam melakukan implementasi protokol TCP/IP, maka paket-paket data yang dikirimkan setiap peralatan menjadi unik peralatan tersebut. Dengan melakukan Packet Fingerprinting, kita dapat mengetahui peralatan apa saja yang ada dalam sebuah jaringan komputer.

- **Security Information Management**

  Dalam usaha untuk meningkatkan keamanan jaringan komputer, sebuah organisasi mungkin akan meng-implementasikan beberapa teknologi keamanan jaringan komputer, seperti firewall, IDS dan IPS. Semua usaha tersebut dilakukan sehingga keamanan jaringan komputer organisasi tersebut menjadi lebih terjamin.

5.2 Cara Pengujian Jaringan

Adalah dengan perangkat yang digunakan seperti SO, firewall anti virus dan software maintenence dengan software tersebut, kita dapat melindungi komputer dari malware software yang bersifat merusak seperti virus dan konflik.

BAB VI

KEBUTUHAN PERSYARATAN ALAT-ALAT UNTUK MEMBANGUN SERVER FIREWALL

6.1 Pengertian Server Firewall

Sebuah server merupakan jantungnya kebanyakan Jaringan, merupakan komputer yang sangat cepat, mempunyai memori yang besar, harddisk yang memiliki kapasitas besar, dengan kartu jaringan yang cepat. Sistem operasi jaringan tersimpan disini, juga termasuk didalam nya beberapa aplikasi dan data yang dibutuhkan untuk jaringan

Sebuah server bertugas mengontrol komunikasi dan informasi diantara komponen dalam suatu jaringan. Sebagai contoh mengelola pengiriman file database atau pengolah kata dari workstation atau salah satu komponen, ke komponen yang lain, atau menerima email pada saat yang bersamaan dengan tugas lain.

Terlihat bahwa tugas server sangat kompleks, dia juga harus menyimpan informasi dan membaginya sangat cepat. Sehingga minimal sebuah server mempunyai beberapa karakter seperti dibawah ini :

- Processor minimal 3.0 GHz atau processor yang lebih cepat lagi.
- Sebuah Harddisk yang cepat dan berkapasitas besar atau kurang lebih 500 Gb.
- Mempunyai banyak port network.
- Kartu jaringan yang cepat dan Reliabilitas.
- Memiliki RAM yang besar, minimal 2 Gb.

Firewall, Apabila sudah menggunakan internet untuk beberapa waktu, dan terutama jika bekerja di perusahaan yang besar dan browse internet di tempat kerja, mungkin sudah mendengar istilah firewall. Sebagian contohnya, sering mendengar orang bilang, “Saya tidak bisa ke situs itu sebab mereka tidak mengijinkan melalui firewall”.

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN).

6.2 Filtering Firewall

Packet Filtering merupakan mekanisme yang dapat memblokir packet-packet data jaringan yang dilakukan berdasarkan peraturan yang telah ditentukan. Packet Filtering umumnya digunakan untuk memblokir lalu-lintas yang mencurigakan yang datang dari alamat IP yang mencurigakan, nomor port TCP/UDP yang mencurigakan, jenis protokol aplikasi yang mencurigakan, dsb.

Jenis Jenis Packet Filtering :

- **Static Packet Filtering**

  Jenis paket jenis filter yang diimplementasikan pada kebanyakan router, dimana modifikasi terdapat aturan-aturan filter yang harus dilakukan secara manual.

- **Dynamic Packet Filtering**

  Apabila proses-proses tertentu disisi luar jaringan dapat merubah aturan filter secara dinamis berdasarkan even-even tertentu yang diobservasi oleh router (sebagai contoh: paket FTP dari sisi luar dapat diijinkan apabila seseorang dari sisi dalam me-request sesi FTP)

6.3 Proxy

Pengertian proxy adalah server yang menyediakan suatu layanan untuk meneruskan setiap permintaan user kepada server lain yang terdapat di internet. Atau definisi proxy server yang lainnya yaitu suatu server atau program komputer yang mempunyai peran sebagai penghubung antara suatu komputer dengan internet.

6.4 Peralatan Membangun Firewall

Langkah langkah membangun server firewall

a) Mengidenftifikasi bentuk jaringan yang dimiliki. Mengetahui bentuk jaringan yang dimiliki khususnya topologi yang di gunakan serta protocol jaringan, akan memudahkan dalam mendesain sebuah firewall.

b) Menentukan kebijakan, Penentuan Kebijakan merupakan hal yang harus di lakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh kebijakan yang di terapkan. Diantaranya:

   - Menentukan apa saja yang perlu dilayani.
   - Menentukan individu atau kelompok yang akan dikenakan kebijakan tersebut.
   - Menentukan layanan yang akan dibutuhkan oleh pengguna jaringan.

c) Menyiapkan software atau hardware yang akan digunakan, baik itu operating system yang mendukung atau software khusus pendukung firewall seperti ipchains, atau iptables pada linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.

d) Melakukan tes 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. Bastion Host adalah sistem/bagian yang dianggap tempat terkuat dalam sistem keamanan jaringan oleh administrator atau dapat disebut bagian terdepan yang dianggap paling kuat dalam menahan serangan, sehingga menjadi bagian terpenting dalam pengamanan jaringan, biasanya merupakan komponen firewall atau bagian terluar sistem publik. Umumnya Bastion Host akan menggunakan sistem operasi yang dapat menangani semua kebutuhan (misal , Unix, linux, NT).

6.5 Radius

Radius adalah layanan keamanan untuk otentikasi dan otorisasi pengguna dial-up. Sebuah jaringan perusahaan yang khas mungkin memiliki server akses melekat kolam modem, bersama dengan server RADIUS untuk menyediakan layanan otentikasi. pengguna remote dial ke server akses, dan server akses mengirimkan permintaan otentikasi ke server RADIUS. RADIUS Server mengotentikasi pengguna dan wewenang akses ke sumber daya jaringan internal. pengguna jarak jauh adalah klien ke server akses dan server akses klien ke server RADIUS.

RADIUS pada awalnya dikembangkan oleh Livingston Enterprises untuk seri portmaster mereka server akses jaringan. Lucent Technologies membeli Livingston pada Oktober 1997, dan kini mengklaim software itu “diciptakan oleh Access Bisnis Unit Remote dari Lucent Technologies pada tahun 1992.” Sisa dari topik ini mengacu pada deskripsi RADIUS disediakan oleh Lucent. Perhatikan bahwa RADIUS merupakan protokol terbuka dan didistribusikan sebagai kode sumber.

Hal ini didefinisikan dalam RFC Internet berikut. Lihat “NAS (Network Access Server)” untuk RFC terkait. RFC 2139 (RADIUS Akuntansi, April 1997) RFC 2865 (Remote Authentication Dial Dalam Pengguna Jasa (RADIUS), Juni 2000) Karena RADIUS terbuka, dapat disesuaikan untuk bekerja dengan produk keamanan pihak ketiga atau sistem keamanan proprietary.

Server akses yang mendukung protokol client RADIUS dapat berkomunikasi dengan server RADIUS. RADIUS sering disebut sebagai RADIUS AAA, mengacu pada fungsi otentikasi, otorisasi, dan akuntansi. “Akuntansi” mengacu pada kemampuan RADIUS untuk mengumpulkan informasi tentang sesi pengguna yang dapat diolah untuk penagihan dan analisis jaringan. Sistem otentikasi RADIUS dasar menggunakan database pengguna sendiri, tetapi sumber-sumber informasi pengguna termasuk

UNIX file password, Sun NIS (Network Information Service), dan direktori yang dapat diakses melalui LDAP (Lightweight Directory Access Protocol).

6.6 TACACS

Terminal Access Controller Access-Control System (TACACS, biasanya diucapkan seperti tack-axe) mengacu pada keluarga protokol terkait yang menangani otentikasi jarak jauh dan layanan terkait untuk kontrol akses jaringan melalui server terpusat. Protokol TACACS asli, yang berasal dari tahun 1984, digunakan untuk berkomunikasi dengan server otentikasi, umum dalam jaringan UNIX lama; itu menelurkan protokol terkait:

- Extended TACACS (XTACACS) adalah ekstensi eksklusif untuk TACACS yang diperkenalkan oleh Cisco Systems pada tahun 1990 tanpa kompatibilitas mundur ke protokol asli. TACACS dan XTACACS memungkinkan server akses jauh untuk berkomunikasi dengan server otentikasi untuk menentukan apakah pengguna memiliki akses ke jaringan.
- Terminal Access Controller Access-Control System Plus (TACACS+) adalah protokol yang dikembangkan oleh Cisco dan dirilis sebagai standar terbuka mulai tahun 1993. Meskipun berasal dari TACACS, TACACS + adalah protokol terpisah yang menangani layanan otentikasi, otorisasi, dan akuntansi (AAA). TACACS + dan protokol AAA fleksibel lainnya telah menggantikan sebagian besar pendahulunya.

6.7 TACACS +

TACACS + dan RADIUS secara umum menggantikan TACACS dan XTACACS di jaringan yang baru-baru ini dibangun atau diperbarui. TACACS + adalah protokol yang sepenuhnya baru dan tidak kompatibel dengan pendahulunya, TACACS dan XTACACS. TACACS + menggunakan TCP (sementara RADIUS beroperasi melalui UDP). Karena TACACS + menggunakan otentikasi, otorisasi, dan akuntansi (AAA) arsitektur, komponen terpisah dari protokol ini dapat dipisahkan dan ditangani pada server terpisah.

Karena TCP adalah protokol berorientasi koneksi, TACACS + tidak harus menerapkan kontrol transmisi. RADIUS, bagaimanapun, memang harus mendeteksi dan memperbaiki kesalahan transmisi seperti kehilangan paket, timeout dll karena naik pada UDP yang tidak memiliki koneksi. RADIUS mengenkripsi hanya kata sandi pengguna saat ia melakukan perjalanan dari klien RADIUS ke server RADIUS. Semua informasi lain seperti nama pengguna, otorisasi, akuntansi dikirimkan dalam bentuk teks yang jelas. Oleh karena itu, rentan terhadap berbagai jenis serangan. TACACS + mengenkripsi semua informasi yang disebutkan di atas dan karena itu tidak memiliki kelemahan yang ada dalam protokol RADIUS.

BAB VII

KONSEP DAN IMPLEMENTASI FIREWALL PADA HOST DAN SERVER

Firewall adalah perangkat yang digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap private network dari pihak luar. Mengkin kita juga sering bertanya-tanya sendiri mengapa firewall selalu ditanamkan di sistem operasi windows besutan perusahaan raksasa yaitu Microsoft, apakah hanya agar terlihat lebih keren atau ada fungsi luar biasa didalamnya.

7.1 Fungsi Firewall

- Mengontrol dan mengawasi paket data yang mengalir di jaringan, dimana Firewall harus bisa mengatur juga melakukan filter akan data yang diizinkan untuk mengakses jaringan pribadi yang terprotect oleh firewall.
- Melakukan tindak pemeriksaan terhadap paket data yang akan melewati jaringan privat.
- Melakukan authentifikasi terhadap akses.
- Firewall mampu memeriksa lebih dari sekedar header dari paket suatu data.
- Melakukan pencatatan setiap transaksi kejadian yang telah terjadi di firewall.

7.2 Jenis-jenis Firewall

- **Personal Firewall**

  Adalah jenis firewall yang dirancang untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.

  Misalnya Microsoft Windows Firewall, Symantec Norton Personal Firewall, Kerio Personal Firewall.

- **Network Firewall**

  Adalah jenis firewall yang dirancang untuk melindungi jaringan secara keseluruhan dari berbagai serangan (Umumnya terjadi pada server) yang dilakukan orang yang tidak bertanggung jawab, baik hanya sekedar iseng-iseng saja ataupun tujuan lainnya.

  Contohnya Microsoft Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IP Tables dalam operating system GNU/Linux. PF dalam keluarga sistem operasi Unix BSD, Juga SunScreen dari Sun Microsystem, Inc.

7.3 Cara Kerja Firewall

- Menolak dan memblokir paket data yang akan datang berdasarkan source (Sumber) dan tujuan yang tak diinginkan.
- Menolak dan menyaring paket data yang berasal dari jaringan internal ke internet.

Misalnya ada pengguna jaringan yang akan mengakses situs-situs pornografi, judi online, tindak kekerasan ataupun website yang mengajarkan ke tindakan negatif lainnya.

7.4 Analisis dan Implementasi Firewall di Host

- Personal Firewall merupakan jenis firewall yang dirancang untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki.
- Implementasinya dengan cara menambahkan beberapa fitur pengaman tambahan seperti misalnya proteksi terhadap virus, anti spyware, anti spam.

7.5 Analisis dan Implementasi Firewall di Server

- Network Firewall merupakan jenis firewall yang dirancang untuk melindungi jaringan secara keseluruhan dari berbagai serangan (Umumnya terjadi pada server) yang dilakukan orang yang tidak bertanggung jawab, baik hanya sekedar iseng-iseng saja ataupun tujuan lainnya.
- Penerapannya dengan memakai Microsoft ISA Server, Cisco PIX, dan Cisco ASA.