

MODUL AJAR FASE F

SISTEM KEAMANAN JARINGAN



TUJUAN
PEMBELAJARAN



Modul 2

TP : Memahami cara kerja firewall dan penerapanya dalam mengamankan jaringan



Idiarso, S.Kom

SISTEM INFORMASI
JARINGAN DAN APLIKASI



MODUL AJAR 2
Cara kerja firewall dan penerapanya
dalam mengamankan jaringan
Konsentrasi Keahlian
Sistem Informatika Jaringan Dan Aplikasi

Konsentrasi Keahlian	: Sistem Informatika Jaringan Dan Aplikasi
Mata Pelajaran	: Sistem Keamanan Jaringan
Fase	: F
Nama Penyususn	: Idiarso,S.Kom
Instansi	: SMK Negeri 1 Punggelan
Jumlah Jam	: 72 JP (18 x Pertemuan)

1. TUJUAN PEMBELAJARAN

Memahami cara kerja firewall dan penerapannya dalam mengamankan jaringan

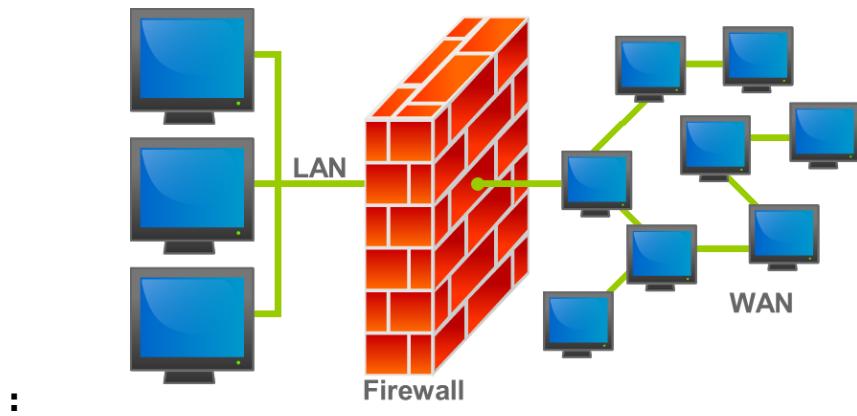
Indikator Ketercapaian Tujuan Pembelajaran

- 2.1. Memahami firewall
- 2.2. Menganalisa jenis-jenis firewall
- 2.3. Mengkonfigurasi dan manajemen firewall untuk melindungi jaringan
- 2.4. Memahami konsep dasar packet filtering dan dalam keamanan jaringan
- 2.5. Menerapkan Implementasi packet filtering dalam firewall untuk mengontrol akses Jaringan

2. LANGKAH PEMBELAJARAN

Pertemuan 1 (4x45 menit)

- Pendahuluan** : 1) Apersepsi diberikan guru kepada peserta didik melalui pertanyaan pemandik yang disampaikan guru;
- a. Apa yang kalian ketahui tentang Firewall ?
 - b. Apa peranan Firewall dalam Sistem Keamanan Jaringan ?
- 2) Sebagai asesmen awal, peserta didik diminta untuk menjelaskan apa yang ada di benaknya ketika guru menayangkan gambar berikut;



Selanjutnya peserta didik diminta untuk

- a. Menjelaskan pengertian fungsi dan ciri-ciri Firewall
- b. Menjelaskan tujuan tujuan utama dari penggunaan firewall
- c. Mencari tahu perbedaan antara firewall jaringan dan firewall host
- d. Bagaimana cara kerja firewall dalam melindungi jaringan

- Inti :**
- 1) Peserta didik difasilitasi untuk memperhatikan materi yang disampaikan oleh guru baik baik melalui media pembelajaran video maupun media pembelajaran lain.
 - 2) Peserta didik diminta untuk browsing materi tentang firewall dan praktik penggunaannya dalam jaringan-jaringan.
 - 3) Peserta didik dibagi menjadi 8 kelompok diskusi sebagaimana tercantum pada LKPD 1 (**Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya**)
 - 4) Peserta didik membuat laporan hasil diskusi dengan menyertakan file hasil karya/hasil diskusi dalam bentuk PPt atau Video, kemudian dipresentasikan di depan kelas secara bergiliran sementara kelompok lain memberikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan
 - 5)) Peserta didik diminta menyimpulkan keseluruhan materi dan guru memberikan penguatan dilanjutkan dengan penyampaian refleksi antar peserta didik dan kepada guru terkait penyampaian materi firewall apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apa kah semua peserta didik paham, siapa saja yang belum
 - 6) paham adakah materi yang susah dipahami, materi mana yang perlu diperbaiki ?
 - 7) Peserta didik mendengarkan pesan dari guru tentang materi yang harus disiapkan untuk pertemuan selanjutnya dan pembelajaran ditutup dengan doa

Pertemuan 2 (8x45 menit)

Pendahuluan	: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal; a. Apa yang kalian ketahui tentang packet filtering ? b. Bagaimana Implementasi Firewall Filter disisi router ? c. Bagaimana konfigurasi firewall menggunakan mikrotik ?
Inti	: 1) Peserta didik diajak untuk mencari diinternet tentang Packet filtering. 2) Peserta didik diminta untuk mempraktikan filtering packet menggunakan mikrotik 3) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 2 4) Hasil diskusi kelompok dituangkan dalam bentuk file form di mana peserta didik mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan (Dimensi P3 kreatif: Mengeksplorasi dan menekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya)

Penutup (45 menit)

- : 1) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 2) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi packet filtering menggunakan mikrotik , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 3) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 2 (8x45 menit)**Pendahuluan**

- : 2) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;
 - a. Apa yang kalian ketahui tentang packet filtering ?
 - b. Bagaimana Implementasi Firewall Filter disisi router ?
 - c. Bagaimana konfigurasi firewall menggunakan mikrotik ?

Inti	<p>: 5) Peserta didik diajak untuk mencari diinternet tentang Packet filtering.</p> <p>6) Peserta didik diminta untuk mempraktikan filtering packet menggunakan mikrotik</p> <p>7) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 2</p> <p>8) Hasil diskusi kelompok dituangkan dalam bentuk file form di mana peserta didik mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan (Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya)</p>
Penutup (45 menit)	<p>: 4) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.</p> <p>5) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi packet filtering menggunakan mikrotik , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.</p> <p>6) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam</p>

Pertemuan 3 (8x45 menit)

Pendahuluan : 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;

- a. Bagaimana cara konfigurasi Mikrotik berdasarkan:
 1. Konfigurasi Blokir Akses IP Tertentu
 2. Konfigurasi Blokir Website Tertentu
 3. Konfigurasi Akses Waktu Tertentu

Inti : 9) Peserta didik diajak menonton bersama tayangan video tentang serangan pada jaringan melalui link

<https://www.youtube.com/watch?v=5LhE8rN4F3Q&t=992s>

- 10) Setelah melakukan pengamatan dari hasil menonton video, Peserta didik diminta untuk Mempraktikan menggunakan alat dan bahan yang telah disediakan
- 11) Peserta Didik memberikan tanggapan dan mengisikannya dalam bentuk form seperti tercantum dalam LKPD 3.
- 12) Peserta didik dibagi menjadi 18 kelompok diskusi Masing-masing kelompok diberikan waktu untuk melakukan kolaborasi praktik.

Penutup (45 menit)

- 13) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 14) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi Blokir akses berdasarkan ip, website dan waktu yang ditentukan menggunakan mikrotik dengan pemakaianya, adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 15) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 4 (16x45 menit)

Pendahuluan	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Setelah kalian melakukan praktik packet filtering menggunakan Mikrotik , bisakah kalian praktik menggunakan selain mikrotik ?</p> <p>b. Apa yang kalian pahami tentang iptables ?</p> <p>c. Bagaimana cara kerja iptables disisi ?</p>
Inti	<p>: 2) Peserta didik diajak untuk mencari diinternet tentang implemenatsi iptables di internet mencakup :</p> <p>beberapa konsep dasar:</p> <ul style="list-style-type: none">•Apa itu iptables dan peranannya dalam sistem firewall Linux? Bagaimana iptables bekerja dan bagaimana paket data melewati tabel dan rantai aturan?•Apa itu tabel dan bagaimana tabel digunakan dalam iptables? Apa itu rantai dan bagaimana rantai berhubungan dengan tabel? <p>Tabel-filter, tabel-nat, dan tabel-mangle: Perbedaan dan kegunaannya.</p> <ul style="list-style-type: none">•Bagaimana membuat aturan iptables? Apa itu kebijakan default dan bagaimana mengatur kebijakan default untuk rantai aturan? Bagaimana menentukan kondisi paket yang akan dicocokkan oleh aturan?•Apa itu tindakan dalam iptables dan bagaimana menggunakannya? Contoh tindakan umum seperti ACCEPT, DROP, REJECT, dan LOG.•Bagaimana melihat, menambahkan, menghapus, dan mengubah aturan iptables? Menyimpan dan memuat konfigurasi iptables. Konfigurasi iptables yang persisten.•NAT (Network Address Translation): Meneruskan paket antara jaringan internal dan eksternal.

Port forwarding dan masquerading.

Pembatasan koneksi dan pencegahan serangan DoS (Denial of Service).

- Contoh penggunaan iptables untuk mengamankan server web atau server jaringan.

Penggunaan iptables dalam lingkungan jaringan yang kompleks.

- 16) Peserta didik diminta untuk Iptables pada sistem operasi Linux menggunakan mesin virtual.
- 17) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 4
- 18) Hasil diskusi kelompok dituangkan dalam bentuk file presentasi atau Video di mana peserta didik mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan
(Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya)

Penutup (45 menit)

- : 7) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 8) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman Iptables , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 9) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 5 (4x45 menit)

Pendahuluan	: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal; a. Setelah kalian melakukan praktek dan melakukan konfigurasi pada menggunakan Mikrotik , bisakah kalian melakukan backup mikrotik ? b. Mengapa penting melakukan Backup ? c. Bagaimana metode backup Mikrotik ?
Inti	: 2) Peserta didik diajak untuk mencari diinternet tentang implemenatsi backup pada perangkat MikroTik mencakup : - Backup melalui Winbox - Backup melalui Terminal - Backup melalui FTP - Backup secara otomatis menggunakan Skrip 3) Peserta didik diminta untuk mempraktikan Backup mikrotik menggunakan alat dan bahan yang telah disediakan 4) Peserta didik secara mandiri sebagaimana tercantum pada LKPD 5 5) Hasil diskusi kelompok dituangkan dalam bentuk file form di mana peserta didik mengunjungi semua hasil karya kelompok lain dengan menyampaikan tanggapan dalam bentuk pertanyaan, masukan ataupun sanggahan (Dimensi P3 kreatif: Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya)

Penutup (45 menit)

- : 6) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 7) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman backup mikrotik , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 8) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 6 (4x45 menit)**Pendahuluan**

- : 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;
 - a. Setelah kalian melakukan praktek dan melakukan konfigurasi pada menggunakan Mikrotik ,bagaimana cara mengamankan mikrotik ?

Inti

- : 2) Peserta didik diajak untuk mencari diinternet tentang pengamanan mikrotik melalui link
<https://www.youtube.com/watch?v=nDMRoWLka1s&t=104s>
- 3) Peserta didik diminta untuk mempraktikan pengamanan mikrotik menggunakan alat dan bahan yang telah disediakan
- 4) Peserta didik secara mandiri sebagaimana tercantum pada LKPD 6
- 5) Hasil praktik kelompok dituangkan dalam bentuk file form yang Guru berikan melalui Google Classroom
- 6) Hasil dari pengumpulan form kemudian guru tampilkan untuk mengoreksi setiap jawaban Peserta didik
- 7) Guru mengajak berdiskusi dari setiap konfigurasi pengamanan mikrotik bilamana ditemukan konfigurasi yang kurang tepat

Penutup (45 menit)

- : 8) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 9) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman pengamanan mikrotik , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 10) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 7 (4x45 menit)**Pendahuluan**

- : 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;
 - a. Setelah kalian melakukan praktek dan melakukan konfigurasi pada menggunakan Mikrotik , bagaimana setting Email Via Winbox & Script Di Mikrotik mikrotik ?
 - b. Mengapa penting melakukan alternatif notifikasi via Email ?

Inti

- : 2) Peserta didik diajak untuk membuka Link di internet tentang setting Email Via Winbox & Script Di Mikrotik mikrotik Dan mengunjungi Link <https://www.blues-pedia.com/2017/02/cara-setting-email-gmail-via-winbox.html>
- 3) Peserta didik diminta untuk mempraktikan menggunakan mikrotik dan alat serta bahan yang telah disediakan
- 4) Peserta didik secara mandiri sebagaimana tercantum pada LKPD 7
- 5) Hasil praktik kelompok dituangkan dalam bentuk file form yang Guru berikan melalui Google Classroom
- 6) Hasil dari pengumpulan form kemudian guru tampilkan untuk mengoreksi setiap jawaban Peserta didik
- 7) Guru mengajak berdiskusi dari setiap konfigurasi pengamanan mikrotik bilamana ditemukan konfigurasi yang kurang tepat

Penutup (45 menit)

- : 8) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.
- 9) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman setting gmail dan script , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.
- 10) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam

Pertemuan 8 (16x45 menit)

Pendahuluan	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Setelah kalian melakukan praktek dan melakukan konfigurasi pada menggunakan Mikrotik dapatkah kalian memperinci penggunaan firewall Mikrotik ?</p> <p>b. Dapatkah kalian menjelaskan semua jenis-jenis pada firewall mikrotik ?</p>
Inti	<p>: 2) Peserta didik diajak untuk mereview kembali dan menghubungkan semua konfigurasi fierewall yang ada pada mikrotik</p> <p>3) Peserta didik diminta untuk mempraktikan menggunakan mikrotik dan alat serta bahan yang telah disediakan dengan aturan jenis jenis firewall :</p> <ul style="list-style-type: none">a) Firewall NAT Menggunakan Masqueradeb) Firewall NAT Masquerade Port Tertentuc) Firewall Filter Input & Forwardd) Firewall Chain Inpute) Firewall Forwardf) Firewall Forward Blokir Website berdasarkan IP Addressg) Firewall Forward Blokir Website Berdasarkan Kontenh) Address Listi) Firewall Manglej) Connection Markk) Packet Mark <p>4) Peserta didik praktik secara mandiri sebagaimana tercantum pada LKPD 8</p> <p>5) Hasil praktik kelompok dituangkan dalam bentuk file form yang Guru berikan melalui Google Classroom</p> <p>6) Hasil dari pengumpulan form kemudian guru tampilkan untuk mengoreksi setiap jawaban Peserta didik</p> <p>7) Guru mengajak berdiskusi dari setiap konfigurasi pengamanan mikrotik bilamana ditemukan konfigurasi yang kurang tepat</p>

Penutup (45 menit)	<ul style="list-style-type: none"> : 8) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan. 9) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman konfigurasi menyeluruh firewall pada mikrotik , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham. 10) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam
---------------------------	--

LEMBAR KERJA PESERTA DIDIK (LKPD)

LEMBAR KEGIATAN PESERTA DIDIK 1

Apa itu firewall?

1. Apa tujuan utama dari penggunaan firewall?
2. Apa perbedaan antara firewall jaringan dan firewall host?
3. Apa yang dimaksud dengan firewall stateful dan stateless?
4. Apa itu rule firewall?
5. Bagaimana cara kerja firewall dalam melindungi jaringan?
6. Apa jenis-jenis firewall yang umum digunakan?
7. Apa perbedaan antara firewall hardware dan firewall perangkat lunak?
8. Apa itu DMZ dalam konteks firewall?
9. Bagaimana Anda bisa memastikan bahwa konfigurasi firewall Anda efektif dan aman?

Jawaban

1. Apa itu firewall?

Firewall adalah sebuah sistem keamanan yang berfungsi untuk melindungi jaringan komputer dari ancaman yang datang dari luar, seperti serangan dari internet atau jaringan yang tidak terpercaya.

Firewall berfungsi untuk mengatur lalu lintas data yang masuk dan keluar dari jaringan, serta menerapkan kebijakan keamanan yang telah ditentukan.

2. Apa tujuan utama dari penggunaan firewall?

Tujuan utama penggunaan firewall adalah untuk mencegah akses yang tidak sah atau tidak diizinkan ke jaringan, serta melindungi sistem dan data dari serangan atau eksploitasi yang mungkin terjadi. Firewall juga digunakan untuk mengontrol dan memantau lalu lintas data yang melewati jaringan.

3. Apa perbedaan antara firewall jaringan dan firewall host?

Firewall jaringan adalah firewall yang ditempatkan di antara jaringan lokal dan jaringan eksternal (misalnya internet). Tujuannya adalah untuk melindungi seluruh jaringan lokal dari serangan yang datang dari luar. Firewall jaringan sering kali berupa perangkat fisik atau perangkat lunak yang diimplementasikan pada router atau gateway.

Sementara itu, firewall host adalah firewall yang dijalankan pada host atau server individual. Firewall host fokus pada melindungi host tersebut dan mengontrol lalu lintas data yang masuk dan keluar dari host tersebut. Firewall host dapat mengatur kebijakan keamanan yang lebih spesifik untuk host tersebut.

4. Apa yang dimaksud dengan firewall stateful dan stateless?

Firewall stateful (berbasis status) adalah jenis firewall yang mampu memantau dan mengingat status koneksi jaringan. Firewall ini dapat menganalisis paket data secara menyeluruh dan menentukan apakah paket tersebut sesuai dengan koneksi yang sudah ada atau merupakan koneksi baru yang sah. Dengan menggunakan informasi status ini, firewall stateful dapat mengizinkan lalu lintas yang merupakan bagian dari koneksi yang sudah terbuka dan memblokir lalu lintas yang mencoba menginisiasi koneksi baru yang tidak diizinkan.

Di sisi lain, firewall stateless (berbasis paket) tidak menyimpan informasi status tentang koneksi. Firewall ini menganalisis setiap paket secara terpisah tanpa mempertimbangkan koneksi sebelumnya. Firewall stateless hanya menggunakan aturan-aturan yang telah ditetapkan untuk mengizinkan atau memblokir paket berdasarkan alamat IP, port, dan protokol.

5. Apa itu rule firewall?

Rule firewall adalah aturan atau kebijakan yang ditetapkan dalam firewall untuk mengatur lalu lintas data yang masuk atau keluar dari jaringan. Setiap rule firewall mengandung kriteria yang harus dipenuhi oleh paket data untuk diterima atau diblokir oleh firewall. Kriteria-kriteria ini dapat berupa alamat IP, port, protokol, dan kondisi lainnya. Dengan menggunakan rule firewall, administrator dapat

mengontrol dan mengamankan lalu lintas data sesuai dengan kebijakan yang ditetapkan.

6. Bagaimana cara kerja firewall dalam melindungi jaringan?

Firewall bekerja dengan mener

apkan kebijakan keamanan yang telah ditetapkan oleh administrator. Ketika paket data melewati firewall, firewall akan memeriksa paket tersebut berdasarkan aturan-aturan yang ada. Jika paket memenuhi kriteria pada salah satu rule, maka paket tersebut akan diterima atau diblokir sesuai dengan kebijakan yang ditentukan.

Firewall juga dapat melakukan fungsi-fungsi tambahan seperti NAT (Network Address Translation) untuk menyembunyikan alamat IP internal dari jaringan lokal, IDS/IPS (Intrusion Detection System/Intrusion Prevention System) untuk mendeteksi serangan dan ancaman keamanan, dan VPN (Virtual Private Network) untuk mengamankan komunikasi jaringan melalui koneksi terenkripsi.

7. Apa jenis-jenis firewall yang umum digunakan?

Beberapa jenis firewall yang umum digunakan meliputi:

- Firewall Jaringan: Melindungi jaringan lokal dari serangan yang datang dari jaringan eksternal.
- Firewall Host: Melindungi host atau server individual dari serangan yang datang dari jaringan.
- Firewall Stateful: Memantau status koneksi dan menerapkan kebijakan berdasarkan koneksi yang ada.
- Firewall Stateless: Menganalisis setiap paket secara terpisah tanpa menyimpan status koneksi.
- Firewall Aplikasi: Melindungi aplikasi atau layanan khusus dengan membatasi akses ke port dan protokol yang digunakan oleh aplikasi tersebut.
- Firewall Berbasis Perimeter: Menggunakan kombinasi dari firewall jaringan, host, dan fitur-fitur keamanan tambahan untuk melindungi perimeter jaringan.

8. Apa perbedaan antara firewall hardware dan firewall perangkat lunak?

Firewall hardware adalah perangkat fisik yang didesain khusus untuk melakukan fungsi firewall. Perangkat ini biasanya memiliki kecepatan dan kapasitas yang tinggi, serta dilengkapi dengan fitur-fitur khusus seperti deteksi intrusi, VPN, dan manajemen lalu lintas yang canggih. Firewall hardware sering digunakan untuk jaringan yang lebih besar atau yang memerlukan kinerja tinggi.

Sementara itu, firewall perangkat lunak adalah perangkat lunak yang diinstal pada sistem operasi komputer atau server. Firewall perangkat lunak dapat dijalankan pada perangkat keras yang ada atau sebagai mesin virtual. Firewall perangkat lunak lebih fleksibel dalam hal konfigurasi dan dapat

diintegrasikan dengan solusi keamanan lainnya. Firewall perangkat lunak umumnya digunakan pada jaringan kecil hingga menengah.

9. Apa itu DMZ dalam konteks firewall?

DMZ (Demilitarized Zone) adalah area jaringan yang terletak di antara firewall internal dan eksternal. DMZ digunakan untuk menempatkan sistem atau layanan yang harus diakses dari jaringan eksternal, seperti server web atau server email. Dengan menempatkan sistem-sistem tersebut di DMZ, lalu lintas yang ditujukan ke sistem tersebut dapat diatur dan difilter oleh firewall dengan kebijakan keamanan yang lebih ketat.

10. Bagaimana Anda bisa memastikan bahwa konfigurasi firewall Anda efektif dan aman?

Untuk memastikan bahwa konfigurasi firewall Anda efektif dan am

an, Anda dapat melakukan beberapa langkah berikut:

- Audit secara berkala: Lakukan audit keamanan secara berkala untuk memeriksa apakah konfigurasi firewall Anda masih memenuhi kebutuhan keamanan. Periksa apakah ada celah keamanan yang dapat dimanfaatkan dan perbarui kebijakan keamanan jika diperlukan.
- Monitoring lalu lintas: Pantau lalu lintas yang melewati firewall untuk mendeteksi aktivitas yang mencurigakan atau serangan yang mungkin terjadi. Gunakan alat monitoring jaringan yang sesuai untuk membantu dalam tugas ini.
- Update keamanan: Pastikan bahwa firewall Anda diperbarui dengan versi terbaru dari perangkat lunak atau firmware yang digunakan. Perbarui juga rule dan kebijakan keamanan sesuai dengan ancaman terbaru yang ada.
- Penetration testing: Lakukan uji penetrasi atau penetration testing secara teratur untuk menguji keamanan firewall dan melihat apakah ada celah yang dapat ditembus oleh serangan dari luar.
- Konfigurasi yang sesuai: Pastikan konfigurasi firewall Anda sesuai dengan kebutuhan dan kebijakan keamanan yang telah ditetapkan. Hapus atau nonaktifkan fitur-fitur yang tidak diperlukan untuk mengurangi potensi serangan.
- Pelatihan pengguna: Berikan pelatihan keamanan kepada pengguna jaringan Anda untuk memastikan bahwa mereka memahami kebijakan keamanan yang ada dan tidak mengakses sumber daya yang tidak diizinkan.

LEMBAR KEGIATAN PESERTA DIDIK 2

Soal Latihan LKPD 2

1. Apa perbedaan antara fitur "filter" dan "nat" dalam firewall MikroTik? Bagaimana Anda akan menggunakannya secara efektif?
2. Apa itu "address-list" dalam firewall MikroTik? Bagaimana cara Anda membuat daftar alamat dan menggunakannya dalam rule firewall?
3. Bagaimana cara menggunakan fitur "connection tracking" pada firewall MikroTik untuk melacak koneksi jaringan dan mengelola lalu lintas yang berhubungan?
4. Apa itu "mangle" pada firewall MikroTik dan bagaimana cara Anda menggunakannya untuk memodifikasi header paket atau melakukan tindakan khusus?
5. Bagaimana cara mengkonfigurasi "Layer 7 Protocol" pada firewall MikroTik untuk mengidentifikasi dan mengontrol lalu lintas berdasarkan pola string di dalam paket?
6. Apa manfaat menggunakan fitur "logging" pada firewall MikroTik? Bagaimana cara Anda mengaktifkan dan menganalisis log firewall?

7. Bagaimana cara mengkonfigurasi firewall MikroTik untuk melindungi jaringan LAN dari serangan luar? Apa saja langkah-langkah yang dapat Anda lakukan untuk meningkatkan keamanan jaringan?
8. Bagaimana Anda dapat menggunakan firewall MikroTik untuk mengizinkan akses ke layanan khusus, seperti SSH atau VPN, dari jaringan eksternal?
9. Apa itu "Web Proxy" pada MikroTik dan bagaimana Anda mengkonfigurasi fitur ini dalam firewall? Apa manfaat dari menggunakan Web Proxy dalam jaringan?
10. Bagaimana cara mengatur kebijakan firewall MikroTik pada jaringan hotspot untuk melindungi pengguna dari ancaman dan membatasi akses ke konten yang tidak diinginkan?

Jawaban Soal LKPD 2

1. Perbedaan antara fitur "filter" dan "nat" dalam firewall MikroTik:
 - Filter: Fitur "filter" digunakan untuk mengontrol lalu lintas jaringan berdasarkan alamat IP, port, protokol, dan kondisi lainnya. Anda dapat membuat aturan firewall untuk mengizinkan atau memblokir lalu lintas berdasarkan parameter yang ditentukan.
 - NAT (Network Address Translation): Fitur "nat" pada firewall MikroTik digunakan untuk melakukan Network Address Translation, yaitu mengubah alamat IP dan/atau port pada paket yang melewati firewall. Ini memungkinkan Anda untuk menyembunyikan alamat IP internal dan mengarahkan lalu lintas ke tujuan yang tepat.
2. "Address-list" dalam firewall MikroTik:
 - "Address-list" adalah fitur di firewall MikroTik yang memungkinkan Anda untuk membuat daftar alamat IP yang dapat digunakan dalam rule firewall. Anda dapat membuat daftar alamat IP sumber atau tujuan yang dapat diterapkan dalam aturan firewall. Ini mempermudah pengelolaan dan pemeliharaan rule firewall yang lebih kompleks.
3. Penggunaan fitur "connection tracking" pada firewall MikroTik:
 - Fitur "connection tracking" pada firewall MikroTik memungkinkan Anda melacak koneksi jaringan dan mengelola lalu lintas yang berhubungan. Dengan menggunakan "connection tracking", Anda dapat membuat aturan firewall yang berkaitan dengan status koneksi, seperti mengizinkan atau memblokir koneksi baru yang terkait dengan koneksi yang ada.
4. "Mangle" pada firewall MikroTik:
 - "Mangle" adalah fitur dalam firewall MikroTik yang memungkinkan Anda untuk memodifikasi header paket atau melakukan tindakan khusus pada paket yang melewati firewall. Dengan "mangle", Anda dapat memodifikasi nilai tos (type of service), melakukan mark connection atau mark packet, serta mengatur tindakan seperti membatasi bandwidth atau mengatur prioritas paket.
5. Konfigurasi "Layer 7 Protocol" pada firewall MikroTik:

- "Layer 7 Protocol" pada firewall MikroTik digunakan untuk mengidentifikasi dan mengontrol lalu lintas berdasarkan pola string di dalam paket. Dengan menggunakan "Layer 7 Protocol", Anda dapat membuat aturan firewall yang berkaitan dengan aplikasi atau protokol tertentu. Ini memungkinkan Anda untuk melakukan tindakan khusus, seperti membatasi atau memblokir akses ke aplikasi atau jenis lalu lintas tertentu.

6. Manfaat menggunakan fitur "logging" pada firewall MikroTik:

- Dengan mengaktifkan fitur "logging" pada firewall MikroTik, Anda dapat memantau aktivitas lalu lintas dan mendeteksi serangan potensial. Log firewall akan mencatat informasi tentang koneksi yang diblokir atau diizinkan, serta informasi penting lainnya seperti alamat IP sumber/tujuan, port, dan protokol. Analisis log firewall dapat membantu dalam pemecahan masalah, deteksi serangan, dan perbaikan kebijakan keamanan.

7

. Konfigurasi firewall MikroTik untuk melindungi jaringan LAN:

- Untuk melindungi jaringan LAN, Anda dapat mengatur beberapa langkah dalam firewall MikroTik, seperti:
 - Mengizinkan hanya lalu lintas yang diperlukan dengan aturan firewall yang tepat.
 - Memastikan bahwa jaringan LAN tersembunyi dari jaringan publik dengan menggunakan fitur NAT.
 - Mengaktifkan fitur "connection tracking" untuk memastikan hanya koneksi yang diizinkan yang dapat berlangsung.
 - Mengaktifkan fitur "address-list" untuk mengelola daftar alamat IP yang diizinkan atau diblokir.
 - Mengaktifkan logging dan memantau log firewall untuk mendeteksi aktivitas mencurigakan.
 - Memperbarui firmware MikroTik secara teratur untuk memastikan keamanan terbaru.

8. Mengizinkan akses ke layanan khusus dengan firewall MikroTik:

- Untuk mengizinkan akses ke layanan khusus, seperti SSH atau VPN, dari jaringan eksternal, Anda dapat menggunakan aturan firewall yang spesifik, seperti:
 - Membuat aturan filter yang mengizinkan lalu lintas yang masuk ke port dan protokol yang sesuai dengan layanan yang ingin diakses.
 - Mengatur aturan NAT agar lalu lintas dari jaringan eksternal diarahkan ke alamat IP dan port yang benar di jaringan internal.
 - Memastikan bahwa hanya lalu lintas yang sah dan aman yang diizinkan dengan menggunakan pengaturan kebijakan keamanan yang tepat.

9. "Web Proxy" pada MikroTik:

- "Web Proxy" adalah fitur di MikroTik yang memungkinkan penyimpanan cache dan mempercepat akses ke situs web. Dengan mengaktifkan dan mengkonfigurasi Web Proxy, MikroTik akan menyimpan salinan halaman web yang pernah diakses dan dapat memberikan akses yang lebih cepat saat halaman web tersebut diminta lagi. Anda juga dapat mengatur kebijakan cache, mengkonfigurasi ACL (Access Control List), dan memantau kinerja proxy.

10. Konfigurasi firewall MikroTik pada jaringan hotspot:

- Untuk melindungi pengguna hotspot dan membatasi akses ke konten yang tidak diinginkan, Anda dapat mengatur beberapa langkah dalam firewall MikroTik, seperti:
 - Membuat aturan filter yang membatasi akses ke layanan tertentu atau konten yang tidak diinginkan.
 - Menggunakan "address-list" untuk membatasi akses ke situs web atau konten berbahaya.
 - Mengatur aturan NAT untuk mengarahkan lalu lintas hotspot ke jaringan internal atau sumber daya terkait.
 - Mengaktifkan logging dan memantau log firewall untuk mendeteksi aktivitas yang mencurigakan di jaringan hotspot.
 - Menggunakan SSL/TLS untuk mengamankan koneksi pengguna hotspot.

LEMBAR KEGIATAN PESERTA DIDIK 3

1. Praktikan menggunakan Router Mikrotik penerapan sbb :
 - a) Konfigurasi Blokir Akses IP Tertentu
 - b) Konfigurasi Blokir Website Tertentu
 - c) Konfigurasi Akses Waktu Tertentu
2. Dokumentasikan hasil kerja kalian kedalam sebuah video
3. Upload hasil kerja kedalam youtube atau social media lainnya yang kalian miliki

LEMBAR KEGIATAN PESERTA DIDIK 4

Soal Latihan 4

Iptables biasanya sudah terpasang secara default di banyak distribusi Linux modern. Namun, jika Anda perlu memastikan bahwa iptables terinstal, Anda dapat mengikuti langkah-langkah berikut untuk menginstalnya:

1. Buka terminal atau konsol pada sistem operasi Linux Anda.
2. Untuk distribusi berbasis Debian (misalnya Ubuntu), gunakan perintah berikut untuk menginstal iptables:

```
```bash
sudo apt update
sudo apt install iptables
````
```

Perintah `apt update` memperbarui daftar paket yang tersedia, dan perintah `apt install iptables` menginstal iptables.

3. Untuk distribusi berbasis Red Hat (misalnya CentOS atau Fedora), gunakan perintah berikut:

```
```bash
sudo yum install iptables
````
```

Perintah `yum install iptables` akan menginstal iptables melalui manajer paket yum.

Setelah langkah-langkah di atas selesai, iptables seharusnya terinstal di sistem Anda.

Untuk memastikan bahwa iptables berhasil terinstal, Anda dapat menjalankan perintah `iptables --version` di terminal atau konsol. Jika versi iptables ditampilkan, itu berarti iptables telah terinstal dengan sukses.

Harap dicatat bahwa instalasi iptables biasanya membutuhkan hak superuser (sudo). Pastikan Anda memiliki akses administratif yang cukup untuk menginstal paket.

Buatlah konfigurasi iptables untuk sebuah server Linux dengan tiga kebijakan dasar: mengizinkan akses SSH, mengizinkan akses HTTP, dan memblokir semua akses yang tidak diizinkan.

```
```bash
Membersihkan semua aturan dan kebijakan yang ada
iptables -F
iptables -X

Set kebijakan default untuk INPUT, FORWARD, dan OUTPUT menjadi DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

Mengizinkan akses SSH (port 22)
iptables -A INPUT -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

Mengizinkan akses HTTP (port 80 dan 443)
iptables -A INPUT -p tcp -m multiport --dports 80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp -m multiport --sports 80,443 -m state --state ESTABLISHED -j ACCEPT

Blokir akses selain SSH dan HTTP
iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
```

```

Penjelasan konfigurasi di atas:

- Baris pertama membersihkan semua aturan dan kebijakan yang mungkin sudah ada sebelumnya.
- Baris kedua mengatur kebijakan default untuk INPUT, FORWARD, dan OUTPUT menjadi DROP, yang berarti semua paket akan diblokir kecuali diizinkan secara eksplisit.
- Baris berikutnya mengizinkan akses SSH dengan memperbolehkan paket TCP baru ke port 22 (INPUT) dan memperbolehkan paket TCP yang terkait dengan koneksi SSH yang sudah ada (OUTPUT).
- Baris selanjutnya mengizinkan akses HTTP dengan memperbolehkan paket TCP baru ke port 80 dan 443 (INPUT) dan memperbolehkan paket TCP yang terkait dengan koneksi HTTP yang sudah ada (OUTPUT).
- Baris terakhir adalah aturan penutup yang akan memblokir semua akses yang tidak diizinkan, baik

masuk maupun keluar.

LEMBAR KEGIATAN PESERTA DIDIK 5

Soal Latihan 5

Terdapat beberapa cara yang dapat digunakan untuk melakukan backup pada perangkat MikroTik.

Berikut adalah beberapa macam cara backup pada MikroTik:

1. Backup melalui Winbox:

- Buka aplikasi Winbox dan terhubung ke perangkat MikroTik.
- Pilih menu "Files" di panel sebelah kiri.
- Klik kanan di area kosong dan pilih "Backup" untuk membuat backup konfigurasi.
- Pilih opsi "Backup" untuk mengambil backup konfigurasi penuh atau opsi lain sesuai kebutuhan.
- Pilih lokasi penyimpanan dan beri nama file backup.
- Klik tombol "Save" untuk membuat backup.

2. Backup melalui Terminal:

- Buka terminal atau koneksi SSH ke perangkat MikroTik.
- Gunakan perintah berikut untuk membuat backup konfigurasi:

```

/system backup save name=mybackup

```

- Ganti "mybackup" dengan nama file backup yang diinginkan.

- Backup akan disimpan di direktori "Files" pada perangkat MikroTik.

3. Backup melalui FTP:

- Pastikan Anda memiliki server FTP yang tersedia untuk penyimpanan backup.
- Buka terminal atau koneksi SSH ke perangkat MikroTik.
- Gunakan perintah berikut untuk membuat backup dan mengirimkannya ke server FTP:

```

/system backup save name=mybackup

/tool fetch mode=ftp address=alamat\_ftp user=nama\_pengguna password=sandi\_ftp

src=mybackup.backup dst=mybackup.backup

```

- Ganti "alamat_ftp", "nama_pengguna", dan "sandi_ftp" dengan informasi FTP yang benar.

- Backup akan disimpan di server FTP yang ditentukan.

4. Backup secara otomatis menggunakan Skrip:

- Buka terminal atau koneksi SSH ke perangkat MikroTik.

- Gunakan perintah berikut untuk membuat skrip backup:

```

```
/system script add name=backup_script source="/system backup save name=(nama_file)"
```

```
/system scheduler add name=backup_schedule interval=1d on-event=backup_script
```

```

- Ganti "(nama_file)" dengan nama file backup yang diinginkan.

- Skrip backup akan dijadwalkan untuk berjalan setiap hari dengan menggunakan perintah "interval=1d" (interval dapat disesuaikan).

- Backup akan disimpan di direktori "Files" pada perangkat MikroTik.

Dengan menggunakan berbagai cara backup tersebut, Anda dapat membuat salinan konfigurasi MikroTik yang penting dan memastikan pemulihan yang cepat dalam situasi kegagalan atau kehilangan konfigurasi. Pastikan untuk mengamankan backup dengan aman agar dapat diakses jika diperlukan.

LEMBAR KEGIATAN PESERTA DIDIK 6

1) Setelah menonton Video dari link

<https://www.youtube.com/watch?v=nDMRoWLka1s&t=104s> Buatlah konfigurasi sederhana untuk mengamankan mikrotik sesuai dengan yang kalian pahami dari video yang ditampilkan

2) Kumpulkanlah hasil penggerjaan kalian melalui Google Form yang Guru berikan

LEMBAR KEGIATAN PESERTA DIDIK 7

Lembar panduan

1. Pastikan Anda telah terhubung ke perangkat MikroTik menggunakan Winbox.

2. Masuk ke menu "System" dan pilih opsi "Scripts".

3. Klik tombol "+" untuk membuat script baru.

4. Beri nama pada script, misalnya "Email_Gmail_Setup".

5. Di bagian "Source", masukkan kode berikut ini untuk mengatur pengiriman email menggunakan Gmail melalui SMTP:

```bash

```
/tool e-mail set address=smtp.gmail.com port=587 from=<your-email@gmail.com> user=<your-
email@gmail.com> password=<your-password> start-tls=yes
```

```

Gantilah `<your-email@gmail.com>` dengan alamat email Gmail Anda dan `<your-password>` dengan kata sandi Gmail Anda.

6. Klik tombol "OK" untuk menyimpan script.

7. Kembali ke menu "System" dan pilih opsi "Scheduler".

8. Klik tombol "+" untuk membuat scheduler baru.

9. Atur waktu dan interval sesuai kebutuhan Anda.

10. Di bagian "On Event", masukkan perintah berikut ini untuk menjalankan script yang telah Anda buat sebelumnya:

```
```bash
/system script run Email_Gmail_Setup
````
```

Pastikan "Email_Gmail_Setup" sesuai dengan nama script yang Anda buat sebelumnya.

11. Klik tombol "OK" untuk menyimpan scheduler.

LEMBAR KEGIATAN PESERTA DIDIK 8

1. Buatlah konfigurasi Firewall menggunakan mikrotik secara menyeluruh menggunakan aturan sbb :

- NAT Menggunakan Masquerade
- Firewall NAT Masquerade Port Tertentu
- Firewall Filter Input & Forward
- Firewall Chain Input
- Firewall Forward
- Firewall Forward Blokir Website berdasarkan IP Address
- Firewall Forward Blokir Website Berdasarkan Konten
- Address List
- Firewall Mangle
- Connection Mark
- Packet Mark

2. Sebagai bahan pertimbangan kalian bisa menggunakan rule berikut :

Berikut adalah contoh konfigurasi lengkap untuk perangkat MikroTik RB750Gr2:

1. Konfigurasi Dasar:

```
/interface ethernet
set [ find default-name=ether1 ] name=WAN
set [ find default-name=ether2 ] name=LAN

/ip address
add address=192.168.1.1/24 interface=LAN network=192.168.1.0
add address=<IP_WAN>/<SUBNET_MASK> interface=WAN

/ip dns
set servers=8.8.8.8,8.8.4.4

/ip route
add gateway=<GATEWAY_IP>
```

2. DHCP Server:

```
/ip pool  
add name=pool1 ranges=192.168.1.100-192.168.1.200  
  
/ip dhcp-server  
add address-pool=pool1 disabled=no interface=LAN name=dhcp1  
  
/ip dhcp-server network  
add address=192.168.1.0/24 gateway=192.168.1.1
```

3. Firewall:

```
/ip firewall filter  
add action=accept chain=input comment="Accept established connections" connection-state=established  
add action=accept chain=input comment="Accept related connections" connection-state=related  
add action=drop chain=input comment="Drop invalid connections" connection-state=invalid  
add action=accept chain=input comment="Accept ICMP" protocol=icmp  
add action=accept chain=input comment="Accept SSH" dst-port=22 protocol=tcp  
add action=accept chain=input comment="Accept HTTP" dst-port=80 protocol=tcp  
add action=accept chain=input comment="Accept HTTPS" dst-port=443 protocol=tcp  
add action=drop chain=input comment="Drop all other input traffic"  
add action=accept chain=forward comment="Accept established connections" connection-state=established  
add action=accept chain=forward comment="Accept related connections" connection-state=related  
add action=drop chain=forward comment="Drop invalid connections" connection-state=invalid  
add action=drop chain=forward comment="Drop all other forward traffic"
```

4. NAT (Network Address Translation):

```
/ip firewall nat  
add action=masquerade chain=srcnat comment="Masquerade LAN traffic" out-interface=WAN
```

5. PPPoE Client:

```
/interface pppoe-client  
add disabled=no interface=WAN name=pppoe-out1 password=<PPPOE_PASSWORD>  
user=<PPPOE_USERNAME>
```

6. Wireless Access Point:

```
/interface wireless  
set [ find default-name=wlan1 ] band=2ghz-b/g/n channel-width=20/40mhz-Ce disabled=no  
mode=ap-bridge ssid=<WIFI_SSID> wireless-protocol=802.11
```

```
/interface wireless security-profiles  
set [ find default=yes ] authentication-types=wpa2-psk mode=dynamic-keys supplicant-  
identity=MikroTik
```

7. Web Proxy:

```
/ip proxy  
set enabled=yes  
  
/ip proxy access  
add action=allow disabled=no dst-host=www.google.com
```

8. Logging:

```
/system logging action
```

```
set 1 memory-lines=100
```

```
/system logging  
add action=memory topics=info
```

Setelah melakukan konfigurasi di atas, pastikan untuk menyesuaikan nilai-nilai seperti `<IP_WAN>`, `<SUBNET_MASK>`, `<GATEWAY_IP>`, `<PPPOE_USERNAME>`, `<PPPOE_PASSWORD>`, `<WIFI_SSID>` sesuai dengan kebutuhan jaringan Anda.

Konfigurasi ini memberikan dasar-dasar untuk mengonfigurasi MikroTik RB750Gr2 dengan fungsi dasar seperti mengatur antarmuka, alamat IP

, DHCP server, firewall, NAT, klien PPPoE, akses poin nirkabel, web proxy, dan logging. Anda dapat menyesuaikan konfigurasi ini sesuai dengan kebutuhan jaringan Anda.

3. Upload Tugas dalam bentuk Video yang diunggah melalui youtube kalian masing-masing

3. ASESMEN PEMBELAJARAN, REMEDIAL DAN PENGAYAAN

1. Teknik penilaian

- | | |
|---------------------------|---|
| a. Sikap Prilaku Karakter | : Observasi (Format Penilaian Sikap) |
| b. Sikap Sosial | : Observasi (Format Penilaian Sikap) |
| c. Produk | : LKPD Peserta Didik |
| d. Proses | : Tes Lisan (Format Assessmen Kinerja Proses) |
| e. Keterampilan | : Praktikum (Format Assessmen Kinerja Keterampilan) |

2. Instrumen penilaian

- | | |
|-----------------------|-----------------------------------|
| a. Lembar Penilaian | : Sikap Perilaku Karakter |
| b. Lembar Penilaian 2 | : Sikap Sosial |
| c. Lembar Penilaian 3 | : Produk dilengkapi kunci jawaban |
| d. Lembar Penilaian 4 | : Proses |
| e. Lembar Penilaian 5 | : Keterampilan |

3. Pembelajaran remedial dan pengayaan

a) Remedial

Remedial dilaksanakan setelah diadakan penilaian pengetahuan bagi peserta didik yang mendapat nilai di bawah KKM dengan memberi tugas berupa:

- Mengulang Pendalaman Materi terkait rincian materi yang sulit
- Memanfaatkan peserta didik yang nilainya paling baik dan mempunyai kemampuan lebih untuk melakukan tutor sebaya
- Mengulang Melakukan Evaluasi dengan materi yang sama

b) Pengayaan

Peserta didik yang mendapat nilai di atas KKM diberikan pengayaan berupa:

- Memberikan tugas baru yang sepadan

- Mengembangkan materi yang sudah dikuasai dan membandingkan dari berbagai sumber belajar.

Lampiran

1. Bahan Ajar (materi ajar, e-book)
2. Jobsheet (LKPD)
3. Media
4. Rubrik Penilaian (P,K,S) dan Kisi – kisi

Mengetahui
Kepala SMK Negeri 1 Punggelan

Banjarnegara, 19 Juni 2023
Guru Mata Pelajaran,

Drs. Supriyadi
NIP. 19660128 199302 1 002

Idiarso, S.Kom
NIP.19830804 202221 1 006

- Mengembangkan materi yang sudah dikuasai dan membandingkan dari berbagai sumber belajar.

Lampiran

1. Silabus
2. Bahan Ajar (materi ajar, e-book)
3. Jobsheet (LKPD)
4. Media
5. Rubrik Penilaian (P,K,S) dan Kisi – kisi
6. Soal pre test dan Post tes (QR Code)

Mengetahui
Kepala SMK Negeri 1 Punggelan

Banjarnegara, 19 Juni 2023
Guru Mata Pelajaran,

Drs. Supriyadi
NIP. 19660128 199302 1 002

Idiarso, S.Kom
NIP.19830804 202221 1 006

MATERI

Kompetensi Dasar:

- Mengevaluasi firewall jaringan.
- Mengkonfigurasi firewall jaringan.

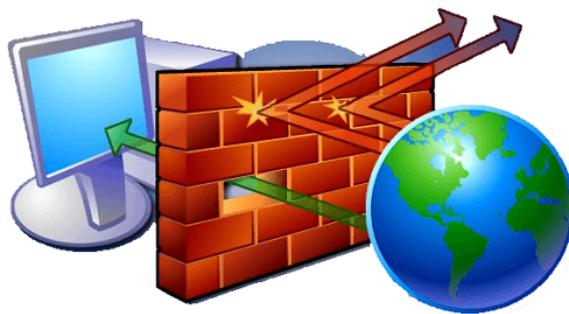
FIREWALL JARINGAN

Di era internet yang semakin canggih ini, setiap komputer dapat terhubung dengan komputer lainnya secara mudah. Pertukaran file atau dokumen pun semakin tanpa batas dan dapat dilakukan oleh siapa saja. Tentunya hal ini membawa dampak positif yang juga diiringi dengan dampak negatif.

Positifnya, orang semakin dimudahkan untuk berbagi berbagai dokumen yang diperlukan. Namun negatifnya, tidak semua orang berbagi dengan tujuan baik. Beberapa berusaha untuk menyerang komputer sebagai hacker, memata-matai (spionase) komputer tertentu demi kepentingan pribadi, atau bahkan mencuri data yang ada dalam suatu komputer.

Untuk mencegah dampak negatif tersebut, dibutuhkan *firewall* sebagai pengatur sistem komunikasi antara dua buah jaringan. Pada artikel di bawah ini, akan dijelaskan secara lengkap mengenai pengertian firewall,

Pengertian Firewall



Firewall dapat didefinisikan sebagai sistem yang didesain khusus untuk mencegah akses mencurigakan masuk ke dalam jaringan pribadi. Firewall sendiri dapat berupa perangkat keras atau perangkat lunak, bisa juga terdiri dari kombinasi keduanya.

Firewall (tembok penahan api) sendiri sebetulnya terinspirasi dari benda fisik bernama firewall yang dipasang di gedung-gedung untuk mencegah menjalarnya api dari sumbernya. Firewall untuk gedung banyak dipasang misalnya di kompleks-kompleks apartemen. Untuk memisahkan dua unit apartemen, dipasanglah sebuah firewall sehingga jika terjadi kebakaran api tidak dengan cepat menjalar dari satu unit ke unit lainnya.

Karena firewall berfungsi sebagai pembatas dengan dunia luar, maka untuk satu unit apartemen yang memiliki empat sisi misalnya, harus memasang firewall di keempat titik perbatasan. Jika salah satu sisi tidak dibatasi dengan firewall sementara ketiga sisi lainnya dipasangi firewall, maka akan sia-sia usaha menahan api yang akan menyebar dengan cepat. Begitu pula halnya dengan firewall untuk komputer.

Supaya dapat berfungsi secara efektif, sebuah firewall wajib memenuhi standar tertentu, mampu mendirikan suatu ‘pagar pengaman’ di sekeliling sebuah jaringan pribadi, mencegah masuknya akses tanpa izin dan berbagai gangguan terhadap dokumen atau file yang ada di komputer pengguna. Di pasaran, ada cukup banyak produk firewall yang ditawarkan dengan fungsi yang bervariasi. Perbedaan firewall satu dengan lainnya biasanya terdapat pada seberapa ketat pengamanan dan selektivitas akses, dan cakupan perlindungannya pada berbagai lapisan OSI (*Open System Interconnection*).



Fungsi Firewall



Firewall sebagai pos keamanan jaringan

Firewall sendiri memiliki beberapa fungsi untuk melindungi jaringan komputer yang dapat dijabarkan dalam beberapa poin berikut:

1. Sebagai Pos Keamanan Jaringan. Semua lalu lintas yang masuk atau keluar jaringan harus melalui firewall sebagai pos kemanan yang akan melakukan pemeriksaan. Setiap terjadi lalu-lintas, firewall akan berusaha menyaring agar lalu lintas sesuai dengan keamanan yang telah ditentukan.
2. Mencegah Informasi Berharga Bocor Tanpa Sepengatahan. Untuk fungsi yang satu ini, firewall banyak dipasang untuk *File Transfer Protocol* (FTP), sehingga setiap lalu-lintas data dikendalikan oleh firewall. Dalam hal ini, firewall bermanfaat untuk mencegah pengguna di jaringan mengirim file berharga yang sifatnya konfidensial (rahasia) kepada pihak lain.
3. Mencatat Aktivitas Pengguna. Setiap kali akan mengakses data, pengguna jaringan akan melalui firewall yang kemudian mencatatnya sebagai dokumentasi (*log files*) yang di kemudian hari bisa dibuka catatannya untuk mengembangkan sistem keamanan. Firewall mampu mengakses data log sekaligus menyediakan statistik mengenai penggunaan jaringan.
4. Memodifikasi Paket Data yang Datang. Dikenal juga dengan istilah NAT (*Network Address Translation*). NAT digunakan untuk menyembunyikan sebuah IP adress, sehingga membuat para pengguna dapat mengakses internet tanpa IP adress publik, yang sering juga disebut dengan istilah *IP masquerading*.
5. Mencegah Modifikasi Data Pihak Lain. Misalnya dalam urusan bisnis untuk informasi laporan keuangan, spesifikasi produk, dan lainnya yang menjadi rahasia perusahaan dan akan berdampak negatif jika diketahui pihak lain. Firewall mencegah modifikasi data-data tersebut sehingga tetap berada dalam keadaan aman.

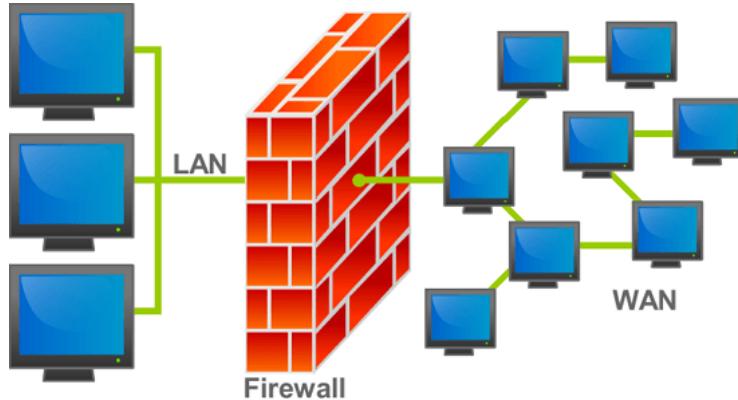
Ciri – Ciri Firewall

1. Firewall harus dapat lebih kuat dan tangguh terhadap serangan di luar. Hal ini artinya sistem operasi komputer akan lebih aman dan penggunaan sistem bisa diandalkan.
2. Yang dapat melakukan hubungan adalah aktivitas yang dikenal atau terdaftar pada jaringan. Dalam hal ini dilaksanakan dengan cara setting policy pada konfigurasi keamanan lokal.
3. Seluruh kegiatan yang asalnya dari dalam ke luar harus melalui firewall lebih dulu. Hal ini dilaksanakan dengan memberikan batasan atau meblokir setiap akses kepada jaringan lokal, terkecuali jika melalui firewall terlebih dahulu.



Cara Kerja Firewall

Pada dasarnya, firewall bekerja dengan cara membatasi komputer pribadi dengan internet. Firewall bekerja layaknya penjaga keamanan di depan gerbang rumah dan mengidentifikasi pengunjung yang datang, sekaligus menyaring penyusup yang berusaha memasuki komputer pribadi. Firewall bekerja seperti garda pertahanan terdepan untuk menahan segala usaha *hacking* yang masuk ke dalam komputer.



Firewall melakukan filter terhadap data masuk yang berasal dari WAN (internet)

Teknologi firewall pun kian hari kian berkembang. Sebelumnya, firewall bekerja menyaring lalu lintas komputer dengan menggunakan alamat IP, nomor port, serta protokol. Seiring dengan perkembangannya, kini firewall mampu menyaring data yang masuk dengan mengidentifikasi terlebih dahulu pesan konten yang dibawanya. Untuk mengatur lalu-lintas perpindahan data komputer dan internet, firewall dapat menggunakan salah satu atau gabungan dari beberapa metode berikut :

1. Packet Filtering

Merupakan sebuah cara kerja firewall dengan memonitor paket yang masuk dan keluar, mengizinkannya untuk lewat atau tertahan berdasarkan alamat *Internet Protocol* (IP), protokol, dan portnya. Packet filtering biasanya cukup efektif digunakan untuk menahan serangan dari luar sebuah LAN. Packet filtering disebut juga dengan firewall statis.

Selama terjadinya komunikasi dengan jaringan internet, packet yang datang disaring dan dicocokkan dengan aturan yang sebelumnya telah dibuat dalam membangun firewall. Jika data tersebut cocok, maka data dapat diterima dan sebaliknya jika tidak cocok dengan aturan, maka data tersebut ditolak.

Dalam metode packet filtering, firewall mengecek sumber dan tujuan alamat IP. Pengirim packet mungkin saja menggunakan aplikasi dan program yang berbeda, sehingga packet filtering juga mengecek sumber dan tujuan protokol, seperti UDP (*User Datagram Protocol*) dan TCP (*Transmission Control Protocol*).

2. Inspeksi Stateful

Berkebalikan dengan *Packet Filtering*, *Inspeksi Stateful* dikenal pula dengan firewall dinamis. Pada inspeksi stateful, status aktif koneksi dimonitor, kemudian info yang didapatkan akan dipakai untuk menentukan apakah sebuah packet jaringan dapat menembus firewall.

Inspeksi stateful secara besar-besaran telah menggantikan packet filtering. Pada firewall statis, hanya header dari packet dicek, artinya seorang hacker dapat mengambil informasi melalui firewall dengan sederhana, yaitu mengindikasikan “reply” melalui header.

Sementara dengan firewall dinamis, sebuah packet dianalisis hingga ke dalam lapisan-lapisannya, dengan merekam alamat IP dan juga nomor portnya, sehingga keamanannya lebih ketat dibandingkan packet filtering. Jadi itulah pembahasan mengenai pengertian firewall, fungsi firewall, dan cara kerja firewall.

Konfigurasi firewall pada Mikrotik router

Firewall adalah sebuah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluiinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Firewall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program firewall) perangkat yang menyaring lalu lintas jaringan antara jaringan. Perlindungan dengan Firewall adalah mutlak diperlukan untuk komputasi perangkat seperti komputer yang diaktifkan dengan koneksi Internet. Meningkatkan tingkat keamanan jaringan komputer dengan memberikan informasi rinci tentang pola-pola lalu lintas jaringan. Perangkat ini penting dan sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaringan komputer internal dan jaringan komputer eksternal.

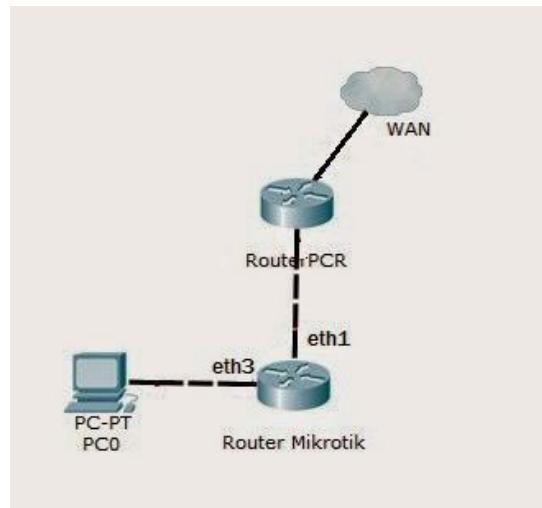
Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi Firewall mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi, beberapa kriteria yang dilakukan fire-wall apakah memperbolehkan paket data lewati atau tidak, antara lain :

- Alamat IP dari komputer sumber
- Port TCP/UDP sumber dari sumber.
- Alamat IP dari komputer tujuan.
- Port TCP/UDP tujuan data pada komputer tujuan
- Informasi dari header yang disimpan dalam paket data.

Secara spesifik Fungsi Firewall adalah melakukan autentifikasi terhadap akses kejaringan. Applikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntutnya untuk mampu mendekripsi protokol aplikasi tertentu yang spesifikasi.

Pada kesempatan kali ini, akan dijelaskan tentang cara memblock user pada mikrotik dan juga mem-block beberapa situs yang tidak diinginkan untuk dibuka oleh user.

Adapun Topologi yang digunakan dalam percobaan ini ialah sebagai berikut :



1. Jika sudah terhubung dengan benar, Buka aplikasi winbox pada pc yang terhubung ke mikrotik. Lalu klik *connect*.
2. Set mikrotik menjadi client bagi jaringan luar dan pc menjadi client dari mikrotiknya. sehingga Mikrotik





mendapat IP dari jaringan luar, dalam hal ini adalah jaringan kampus PCR, dan PC mendapat IP yang disediakan oleh mikrotik.

| Interface List | | | | | | | | | | | |
|----------------|----------------|----------|-------------|-----------|------------|------|-----------|----------|-----|---|---|
| | Interface | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE | | |
| R | bridge-local | Bridge | | | | 1598 | 67.5 kbps | 1416 bps | 7 | 2 | 0 |
| R | ether1-gateway | Ethernet | | | | 1600 | 0 bps | 0 bps | 0 | 0 | 0 |
| R | ether2-LAN | Ethernet | | | | 1598 | 67.5 kbps | 1640 bps | 7 | 2 | 0 |
| S | ether3-WAN | Ethernet | | | | 1598 | 0 bps | 0 bps | 0 | 0 | 0 |

| DHCP Client | | | | | | |
|----------------------|----------|----------|-----------------|---------------|--------------|--|
| + | | - | | Find | | |
| Interface | Use P... | Add D... | IP Address | Expires After | Status | |
| X ether2-LAN | yes | yes | 172.16.30.58... | 2d 23:59:49 | bound | |
| X ether3-WAN | yes | yes | | | searching... | |
| X ether5-slave-local | yes | yes | | | searching... | |

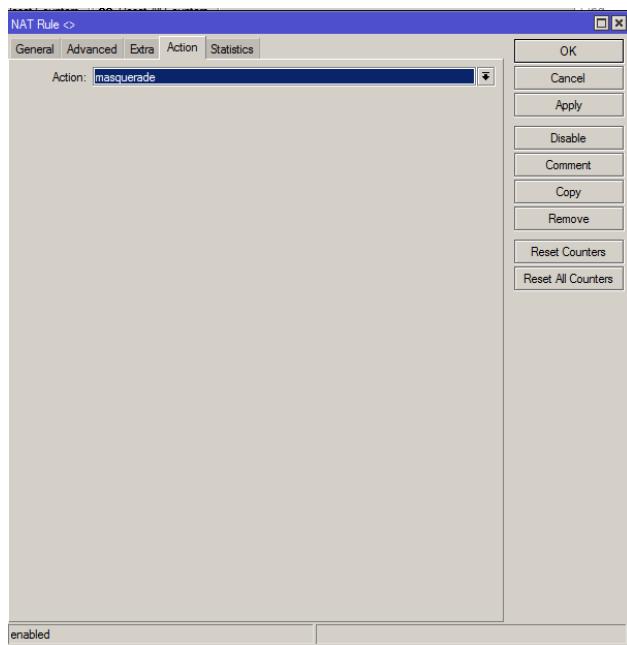
3 items (1 selected)

| DHCP Server | | | | | | |
|-------------|------------|--------------|-------------|--------------|-----------|--------|
| DHCP | | Networks | | Leases | | Alerts |
| Name | Interface | Relay | Lease Time | Address Pool | Add AR... | |
| I LAN | ether2-LAN | 192.168.3.2 | 3d 00:00:00 | dhcp_pool4 | no | |
| X dhcp1 | ether2-LAN | 192.168.10.1 | 3d 00:00:00 | dhcp_pool5 | no | |

3. Atur konfigurasi NAT nya agar bisa terhubung ke jaringan luar, seperti yang telah kami jelaskan pada postingan sebelumnya

| NAT Rule < > | |
|--|--|
| General Advanced Extra Action Statistics | |
| Chain: | srcnat |
| Src. Address: | |
| Dst. Address: | |
| Protocol: | |
| Src. Port: | |
| Dst. Port: | |
| Any. Port: | |
| In. Interface: | |
| Out. Interface: | <input checked="" type="checkbox"/> ether3-WAN |
| Packet Mark: | |
| Connection Mark: | |
| Routing Mark: | |
| Routing Table: | |
| Connection Type: | |
| <input type="checkbox"/> enabled | |

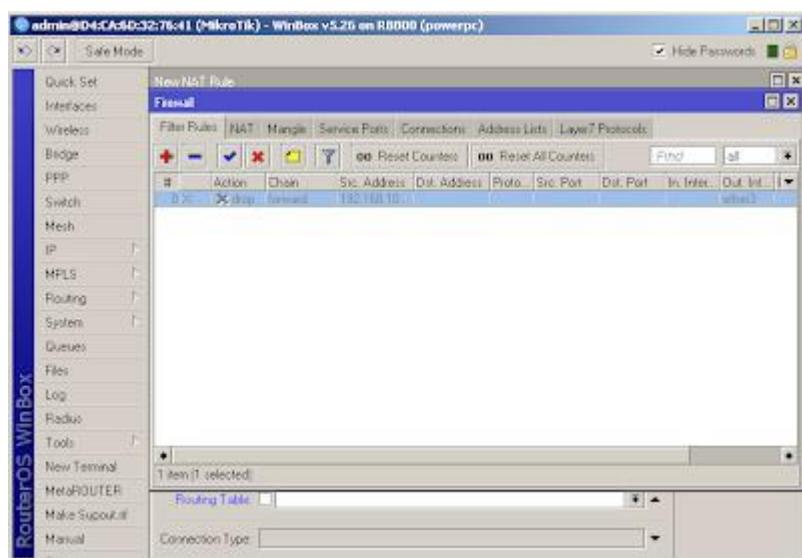




Maka kita akan mendapatkan ip dari mikrotik tersebut

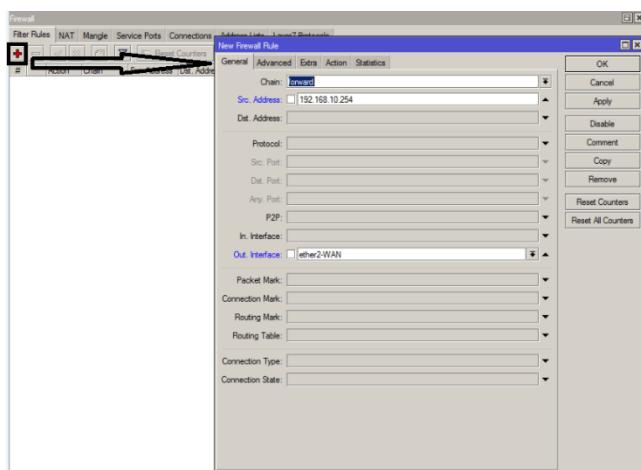
```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . . . . : 
Description . . . . . : Intel(R) 82579U Gigabit Network Connection
Physical Address. . . . . : 44-37-E6-45-0F-21
DHCP Enabled. . . . . : Yes
Power Connection Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1e8:45ff%10:254(PREFERRED)
IPv4 Address. . . . . : 192.168.10.254(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Thursday, January 08, 2015 10:44:07 AM
Lease Expires . . . . . : Sunday, January 11, 2015 10:44:06 AM
Default Gateway . . . . . : 192.168.10.1
DHCP Server . . . . . : 192.168.10.1
DHCPv6 RAID . . . . . : 239351282
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-5E-F7-07-44-37-E6-45-0F-21
DNS Servers . . . . . : 192.168.10.1
172.25.30.1
113.212.113.212
```

4. Selanjutnya kita akan mencoba mem-block suatu IP, Klik IP -> Firewall. Lalu akan didapat tampilan seperti dibawah ini.



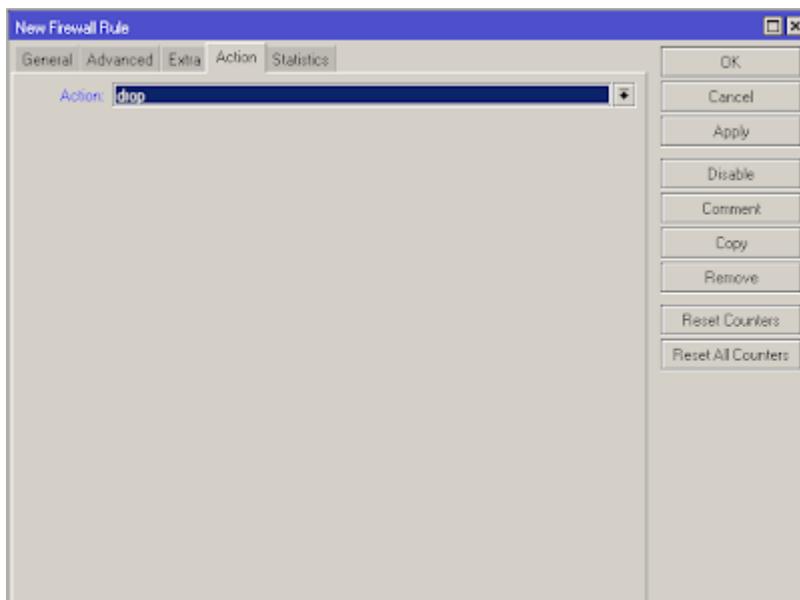


5. Pilih **Filter Rules** lalu klik tanda + yang berfungsi untuk menambahkan daftar block nya. Maka akan didapat tampilan seperti gambar dibawah:

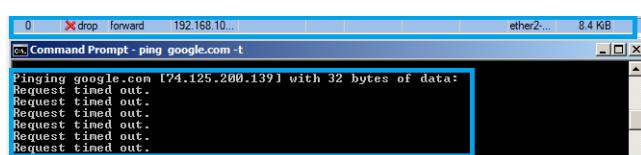


Pada bagian chain diisikan forward, yang mana digunakan untuk proses paket data yang melewati router. Untuk out interface, disini kami menggunakan Ether 2, ini bisa diganti sesuai dengan ethernet mana yang digunakan untuk terhubung ke jaringan luar.

6. Lalu klik **action** , pilih **drop** yang berarti seluruh paket yang dikirim oleh PC client dengan IP yang telah didaftarkan akan di drop atau ditolak.

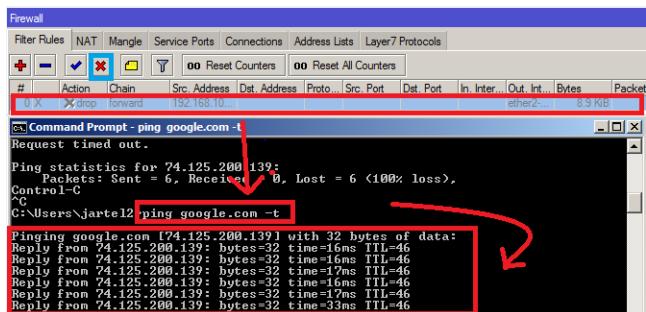


Dapat dibuktikan dengan tes PING ke ip yang diblock tersebut.

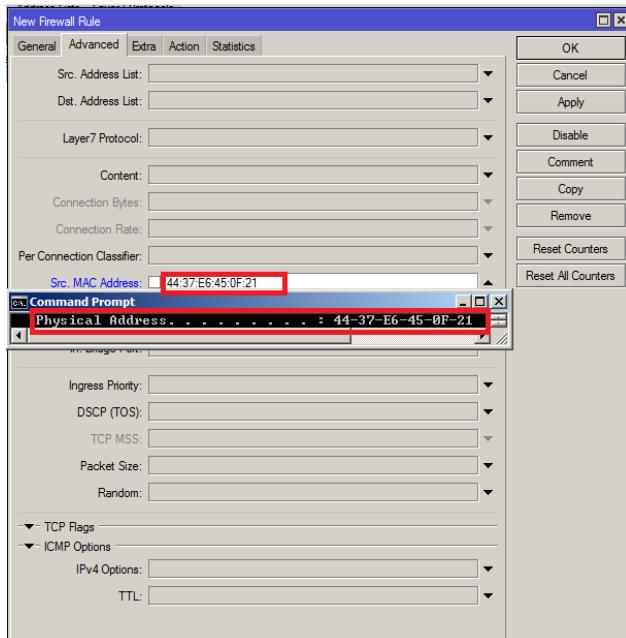


Apabila kita ingin menghapus block nya, kita cukup meng-klik tanda silang. contohnya sperti berikut





7. Selanjutnya, kita juga dapat memblok mac address dengan menggunakan mikrotik .Karna IP dapat berubah-ubah, akan tetapi mac address akan tetap, sehingga pengguna dapat di blok. Pada bagian ini, dibagian **advanced**, **src.MAC address** diisi dengan mac address yang ingin diblock, Seperti terlihat pada gambar dibawah ini:



Untuk action, tetap pilih **drop**

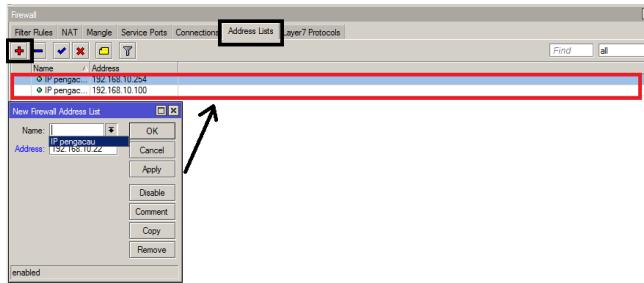
Pada konfigurasi firewall mikrotik ada beberapa pilihan Action, diantaranya :

- Accept** : paket diterima dan tidak melanjutkan membaca baris berikutnya
- Drop** : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
- Reject** : menolak paket dan mengirimkan pesan penolakan ICMP
- Jump** : melompat ke chain lain yang ditentukan oleh nilai parameter jump-target
- Tarpit** : menolak, tetapi tetap menjaga TCP connection yang masuk (membalas dengan SYN/ACK untuk paket TCP SYN yang masuk)
- Passthrough** : mengabaikan rule ini dan menuju ke rule selanjutnya
- log** : menambahkan informasi paket data ke log

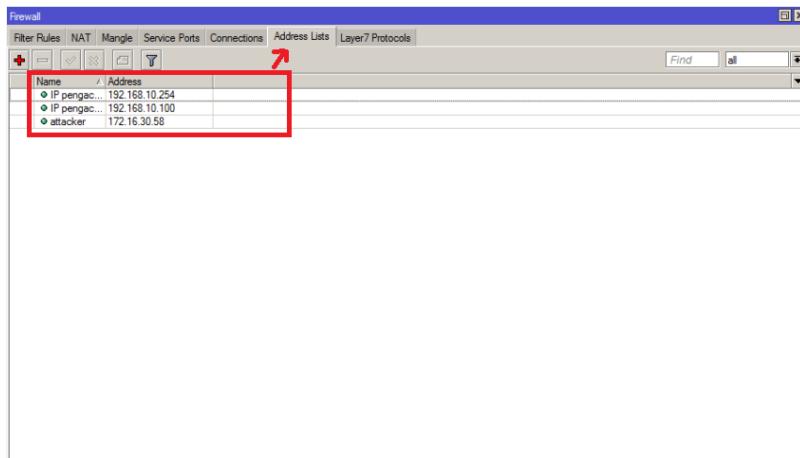




8. Apabila kita ingin mem-block beberapa IP, maka kita bisa mengelompokkan ip tersebut dalam suatu list. caranya : **IP->Firewall** , Lalu pilih **Address list**. Pada bagian ini akan ditambahkan sebuah grup, dimisalkan diberi nama " IP Pengacau"



9. Untuk menambahkan IP yang ingin dimasukkan ke list " IPpengacau" , dapat ditambahkan pada bagian **Source address list** dari menu *advanced*.





Firewall

| Filter Rules | | | | | | | | | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols | |
|----------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|--|---------------|-------------|---------------|------------------|--|
| <input type="button" value="+"/> | <input checked="" type="checkbox"/> | <input type="button" value="00 Reset Counters"/> | <input type="button" value="00 Reset All Counters"/> | | | | | |
| # | Action | Chain | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Inter... | Out. Int... | Bytes | | | | | |
| 0 X | drop | Forward | 192.168.10... | | | | | | | 8.9 | | | | | |
| 1 X | drop | forward | | | | | | | | 454 | | | | | |
| 2 | drop | forward | | | | | | | | 6 | | | | | |

```
Command Prompt - ping google.com -t
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=55ms TTL=54
Reply from 173.194.117.36: bytes=32 time=27ms TTL=54
Reply from 173.194.117.36: bytes=32 time=25ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=21ms TTL=54
Reply from 173.194.117.36: bytes=32 time=19ms TTL=54
Reply from 173.194.117.36: bytes=32 time=19ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=56ms TTL=54
Reply from 173.194.117.36: bytes=32 time=41ms TTL=54
Reply from 173.194.117.36: bytes=32 time=70ms TTL=54
Reply from 173.194.117.36: bytes=32 time=19ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=31ms TTL=54
Reply from 173.194.117.36: bytes=32 time=18ms TTL=54
Reply from 173.194.117.36: bytes=32 time=19ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=22ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=18ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=36ms TTL=54
Reply from 173.194.117.36: bytes=32 time=17ms TTL=54
Reply from 173.194.117.36: bytes=32 time=16ms TTL=54
Reply from 173.194.117.36: bytes=32 time=42ms TTL=54
Reply from 173.194.117.36: bytes=32 time=18ms TTL=54
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

10. Selanjutnya, dari menu firewall yang ada pada mikrotik ini, kita juga dapat memblock situs atau IP tujuan yang kita anggap sebagai situs yang tidak baik.

klik **Filter Rules** lalu isi pada bagian **Dst.Addresses** (IP tujuan yang akan diblock). Dan untuk actionnya pilih **Drop**.

New Firewall Rule

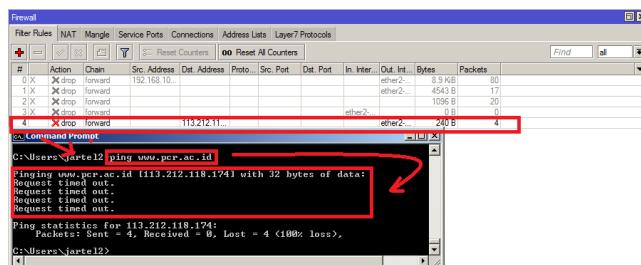
| General | | Advanced | | Extra | | Action | | Statistics | |
|-------------------|--|--|--|-------|--|--------|--|------------|--|
| Chain: | | forward | | | | | | | |
| Src. Address: | | | | | | | | | |
| Dst. Address: | | <input type="text" value="113.212.118.174"/> | | | | | | | |
| Protocol: | | | | | | | | | |
| Src. Port: | | | | | | | | | |
| Dst. Port: | | | | | | | | | |
| Any. Port: | | | | | | | | | |
| P2P: | | | | | | | | | |
| In. Interface: | | | | | | | | | |
| Out. Interface: | | <input type="text" value="ether2-WAN"/> | | | | | | | |
| Packet Mark: | | | | | | | | | |
| Connection Mark: | | | | | | | | | |
| Routing Mark: | | | | | | | | | |
| Routing Table: | | | | | | | | | |
| Connection Type: | | | | | | | | | |
| Connection State: | | | | | | | | | |
| enabled | | | | | | | | | |



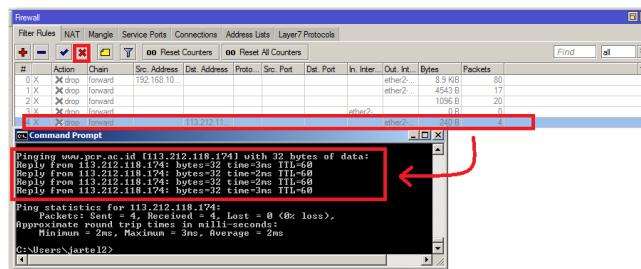
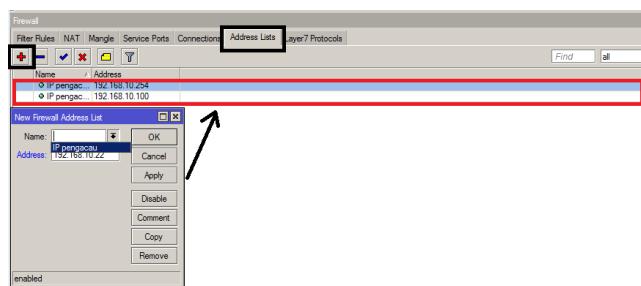


Disini kami mencoba memblock situs atau IP dari kampus Politeknik Caltex Riau.

Lalu kembali kita tes dengan melakukan PING ke IP situs Politeknik Caltex Riau



Dan jika ingin menghapus block atau membatalkan block, dapat memberikan tanda silang pada konfigurasi tadi.



11. Selanjutnya, kita juga dapat memblock jaringan yang berasal dari luar, misalkan jaringan ini dicurigai sebagai aktifitas hacker.

Caranya kita tambahkan IP jaringan yang berasal dari luar mikrotik. Lalu untuk actionnya dipilih **Drop**.

Disini kami menamai "attacker"



SIJA -- Idiarso



New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List: ▾
Dst. Address List: ▾

Layer7 Protocol: ▾

Content: ▾

Connection Bytes: ▾

Connection Rate: ▾

Per Connection Classifier: ▾

Src. MAC Address: ▾

Out. Bridge Port: ▾

In. Bridge Port: ▾

Ingress Priority: ▾

DSCP (TOS): ▾

TCP MSS: ▾

Packet Size: ▾

Random: ▾

▼ TCP Flags

▼ ICMP Options

IPv4 Options: ▾

TTL: ▾

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters





JOB SHEET/ LEMBAR KERJA PESERTA DIDIK
SMK NEGERI 1 KEMUSU
MATA PELAJARAN : ADMINISTRASI INFRASTRUKTUR JARINGAN (AIJ)
KOMPETENSI KEAHLIAN : TEKNIK KOMPUTER DAN JARINGAN (TKJ)

Judul Kegiatan : Instalasi dan Konfigurasi Perangkat Jaringan Komputer

Soal:

Dalam kegiatan ini anda bertindak sebagai seolah-olah menjadi teknisi Jaringan. Tugas anda sebagai seorang teknisi Jaringan adalah merancang bangun dan mengkonfigurasi sebuah *Wifi Router* berfungsi sebagai Gateway Internet, DHCP Server dan Firewall, kemudian internet tersebut *diskonek* ke client melalui jalur kabel dan wireless. Jumlah Client direncanakan: 10 client.

a. Konfigurasi Wifi Router

- | | |
|--|--|
| 1. Sistem operasi | = RouterOS |
| 2. DNS | = Sesuai dengan DNS yang diberikan ISP |
| 3. NTP | = Yes |
| <i>Ether1:</i> | |
| 4. IP Ether1 | = Sesuai dengan Network yang diberikan ISP |
| 5. Gateway | = Sesuai dengan IP yang diberikan oleh ISP |
| <i>Ether2:</i> | |
| 6. Terhubung dengan kabel ke switch dan PC | |
| 7. IP Ether2 | = 192.168.100.1/24 |
| 8. DHCP Pool | = 192.168.100.2-192.168.100.100 |
| 9. Buat firewall agar IP 192.168.100.2-192.168.100.50 tidak dapat ping ke router | |

WLAN 1 (WLAN Interface):

- | | |
|---------------|---------------------------------|
| 10. IP WLAN 1 | = 192.168.200.1/24 |
| 11. SSID | = nama_peserta |
| 12. DHCP Pool | = 192.168.200.2-192.168.200.100 |

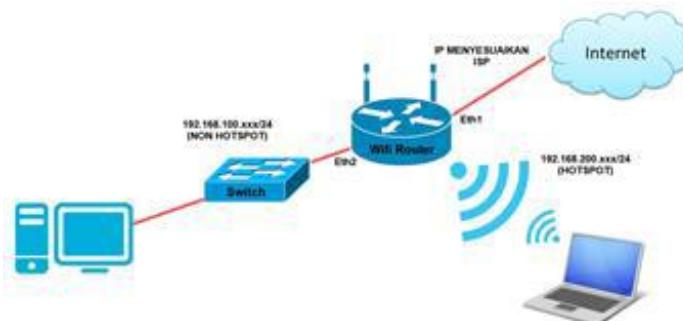
b. Konfigurasi PC/Laptop Client (Yang tergabung Ether2 melalui Switch)

- | | |
|-------------------|-------------------|
| 1. IP LAN | = Dinamis |
| 2. Sistem operasi | = Windows / Linux |

c. Konfigurasi PC/Laptop Client (Yang tergabung WLAN1 melalui wireless)

- | | |
|-------------------|-------------------|
| 1. IP WLAN | = Dinamis |
| 2. Sistem operasi | = Windows / Linux |

d. Gambar kerja





Prosedur yang harus diselesaikan:

1. Menerapkan prosedur kesehatan, keselamatan kerja dan keamanan kerja yang diperlukan

2. Melakukan pemasangan kabel UTP

3. Melakukan pemasangan non managable switch

4. Melakukan pemasangan dan konfigurasi jaringan lokal (LAN)

5. Melakukan pemasangan dan konfigurasi jaringan internet (WAN)

6. Melakukan pemasangan dan konfigurasi jaringan nirkabel (WLAN)

7. Melakukan instalasi dan konfigurasi Server/Router (Hotspot)

8. Melakukan instalasi dan konfigurasi DHCP Server (melalui WLAN 1)

9. Melakukan instalasi dan konfigurasi gateway internet





10. Melakukan konfigurasi TCP/IP Statis pada PC Client/Laptop yang terhubung ether2 melalui switch

11. Melakukan konfigurasi TCP/IP Dinamis pada PC Client/Laptop yang terhubung melalui wireless

12. Melakukan pengujian pada sistem.

Pengujian dari PC Client yang terhubung kabel :

- a. Koneksi internet

Pengujian dari Laptop Client yang terhubung wireless :

- a. Tampilan halaman hotspot

Penguji

Peserta didik

.....

.....



**Penilaian Sikap****a. Indikator Penilaian Sikap**

- 1) Menyapaikan materi/presentasi dengan baik
- 2) Memperhatikan ketika diterangkan materi

b. Instrumen Penilaian sikap**LEMBAR PENILAIAN SIKAP**

Kelas/Semester : /

Waktu Penilaian :

Penilai :

| Aspek Penilaian | Penilaian | | | |
|---|-----------|--------|---------------|--------------|
| | Selalu | Sering | Kadang-kadang | Tidak pernah |
| 1. Peserta bertanya kepada teman ketika mengerjakan tugas individu | | | | |
| 2. Peserta didik meniru/menyontek pekerjaan teman pada saat ulangan | | | | |
| 3. Peserta didik mengeluh ketika menyelesaikan tugas individu atau kelompok | | | | |
| 4. Peserta didik menuntaskan tugas yang diberikan | | | | |
| 5. Peserta didik bertanya kepada teman ketika proses pembelajaran berlangsung | | | | |
| 6. Peserta didik mengumpulkan tugas tepat waktu | | | | |

Tulis masing-masing huruf (4/3/2/1) sesuai dengan pendapatmu jika:

- Selalu skor 4
- Sering skor 3
- Kadang-kadang skor 2
- Tidak pernah skor 1

Skor Perolehan

$$\text{Nilai} = \frac{\text{Skor Maksimum}}{\text{Skor Maksimum}} \times 100$$

Mengetahui,
Guru Mata Pelajaran,

to





Rekap Penilaian Sikap

Lembar Penilaian Sikap

Catatan Jurnal Perkembangan Sikap Spiritual dan Sosial

1. Kelas : X
 2. Hari, Tanggal :
 3. Pertemuan ke :
 4. Materi Pokok :

Mengetahui,
Guru Mata Pelajaran,

to



Penilaian Diri

Nama Siswa :
Hari/Tgl Pengisian :

Petunjuk

Berdasarkan perilaku kalian selama ini, nilailah diri kalian sendiri dengan memberikan tanda centang (✓) pada kolom skor 4, 3, 2, atau 1 pada Lembar Penilaian Diri dengan ketentuan sebagai berikut.

Skor 4 apabila **selalu** melakukan perilaku yang dinyatakan

Skor 3 apabila **sering** melakukan perilaku yang dinyatakan

Skor 2 apabila **kadang-kadang** melakukan perilaku yang dinyatakan

Skor 1 apabila **jarang** melakukan perilaku yang dinyatakan

Indikator Sikap:

- | | | |
|--------------|-------------------|-----------------|
| 1. Keimanan | 4. Santun | 7. Peduli |
| 2. Ketaqwaan | 5. Disiplin | 8. Percaya diri |
| 3. Kejujuran | 6. Tanggung jawab | |

| N | Pernyataan | Skor | | | | Ketera
n |
|---|---|------|---|---|---|-------------|
| | | 1 | 2 | 3 | 4 | |
| 1 | Saya berdoa sebelum dan sesudah menjalankan setiap perbuatan, ikhlas menerima pemberian dan keputusan Tuhan YME, suka berikhтир, dan | | | | | |
| 2 | Saya menjalankan ibadah sesuai ajaran agama yang saya anut, mengikuti ibadah bersama di sekolah, dan mengucapkan kalimat puji bagi | | | | | |
| 3 | Saya jujur dalam perkataan dan perbuatan, mengakui kesalahan yang diperbuat, mengakui kekurangan yang dimiliki, tidak menyontek dalam | | | | | |
| 4 | Saya hadir dan pulang sekolah tepat waktu, berpakaian rapi sesuai ketentuan, patuh pada tata tertib sekolah (mengenakan helm saat membonceng) | | | | | |
| 5 | Saya melaksanakan setiap pekerjaan yang menjadi tanggungjawabnya, mengakui dan | | | | | |
| 6 | Saya membantu orang yang membutuhkan, memelihara lingkungan, mematikan lampu dan keran air jika tidak | | | | | |
| 7 | Saya menerima kesepakatan meskipun berbeda dengan pendapat saya, menerima kekurangan orang lain, memaafkan kesalahan orang lain, | | | | | |





| | | | | | |
|--------------------|--|--|--|--|--|
| 8 | Saya terlibat aktif dalam kegiatan membersihkan kelas/sekolah, kerja kelompok, mendahulukan kepentingan bersama, dan membantu orang lain tanpa mengharap imbalan | | | | |
| 9 | Saya menghormati orang yang lebih tua, tidak berkata-kata kotor, kasar, dan tidak menyakitkan, mengucapkan terima kasih, meminta ijin ketika menggunakan barang orang lain, melakukan pembiasaan 3S (Senyum, Sapa, Salam). | | | | |
| 10 | Saya berpendapat/bertindak tanpa ragu-ragu, berani berpendapat, bertanya atau menjawab, presentasi di depan kelas, dan membuat keputusan dengan cepat. | | | | |
| Jumlah Skor | | | | | |

Mengetahui,
Guru Mata Pelajaran,

to





2. Penilaian Pengetahuan

Dengan Tes Tertulis

Kisi-Kisi Soal

| Kompetensi | IPK | Indikator Soal | Jenis tes | Nom So |
|--|---|--|----------------------------|-------------------|
| 3.12
Mengevaluasi firewall jaringan | 1. Menjelaskan konsep <i>firewall</i> pada jaringan.
2. Mengklasifikasikan jenis <i>firewall</i> pada jaringan. | 1. Siswa dapat menjelaskan definis konsep <i>firewall</i> jaringan dengan baik dan benar. | Uraian | 1 |
| 4.12
Konfigurasi firewall jaringan | 3. Menentukan cara konfigurasi <i>firewall</i> pada jaringan.
4. Melakukan konfigurasi <i>firewall</i> pada jaringan.
5. Menguji hasil konfigurasi <i>firewall</i> pada jaringan. | 2. Siswa dapat menjelaskan jenis – jenis <i>firewall</i> jaringan dengan baik dan benar.
3. Siswa dapat menerapkan konfigurasi <i>firewall</i> jaringan.
4. Siswa dapat menganalisis hasil pengujian konfigurasi <i>firewall</i> jaringan. | uraian
Uraian
Uraian | 2
3
4 dan 5 |

Soal dan Norma Penilaian

| N | Naskah Soal | Kriteria nilai |
|---|---|--|
| 1 | Setelah mempelajari materi firewall jaringan, uraikan dengan
<u>Bahasamu sendiri apakah yang dimaksud firewall jaringan?</u> | Sempuna: 10
Sedang: 8
salah: 4
tidak jawab: 0 |
| 2 | Setelah mempelajari materi firewall jaringan, uraikan dengan
<u>Bahasamu sendiri apakah fungsi firewall jaringan?</u> | Sempuna:
10
Sedang:
8 salah:
8 |
| 3 | Lakukan analisis bagaimanakah cara kerja firewall jaringan? | Sempuna:
10
Sedang:
8 salah:
8 |
| 4 | Dari materi yang dipelajari, coba terangkan Kembali manfaat penggunaan firewall jaringan menurut analismu! | Sempuna:
10
Sedang:
8 salah:
8 |
| 5 | Dari materi yang sudah dipelajari bahwa firewall jaringan memiliki beberapa kriteria, apa sajakah kriteria firewall dalam melewati paket data! Uraikan dengan bahasamu sendiri. | Sempuna:
10
Sedang:
8 salah:
4 |

$$\frac{\text{Skor Perolehan}}{\text{Skor}} \times 100$$



Kunci Jawaban

| No | Kunci Jawaban |
|----|---|
| 1 | Sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa |
| 2 | Untuk melindungi sumber daya dari jaringan pribadi dari pengguna dari jaringan lain |
| 3 | Sistem firewall bekerja dengan cara menganalisis paket data yang keluar dan masuk ke dalam lingkungan aman yang dilindungi oleh sistem firewall tersebut. Paket data yang tidak lolos analisis akan ditolak untuk masuk ataupun keluar jaringan atau komputer yang dilindungi. Penyaring atau filter firewall akan bekerja melakukan pemeriksaan sumber dari paket data yang masuk dengan kebijakan yang dibuat untuk mengontrol paket dari mana saja yang boleh masuk. Sistem juga dapat melakukan pemblokiran pada jenis jaringan tertentu serta melakukan pencatatan pada lalu lintas paket data yang mencurigakan |
| 4 | Menjaga informasi rahasia dan berharga yang menyelinap keluar tanpa sepengetahuan. Sebagai filter yang digunakan untuk mencegah lalu lintas tertentu mengalir ke subnet jaringan. Memodifikasi paket data yang data di firewall, proses tersebut <i>Network Address Translation (NAT)</i> .
Sebagai Alurasi data seperti informasi kuantan spesifikasi produk barang produk dll |
| 5 | Alamat IP dari komputer sumber Port TCP/UDP sumber dari sumber.
Alamat IP dari komputer tujuan.
Port TCP/UDP tujuan data pada komputer tujuan
Informasi dari header yang disimpan dalam paket |

Interval Nilai Kualitatif

| | |
|------------|---------------|
| 81 – 100 A | (Sangat Baik) |
| 70 – 80 B | (Baik) |
| 50 – 69 C | (Cukup) |
| < 60 K | (Kurang) |





Form Penilaian Aspek Keterampilan

Nama :
Kelas :

| No | Komponen/Sub Komponen | Kompeten | | | | | |
|----------------------|--|----------|----|---|---|---|---|
| | | Belum | Ya | | | | |
| | | | 0 | 1 | 2 | 3 | |
| 1. | | 2 | 3 | 4 | 5 | 6 | 7 |
| I Persiapan | | | | | | | |
| 1.1 | Melakukan survei teknis | | | | | | |
| 1.2 | Membuat daftar kebutuhan teknis | | | | | | |
| 1.3 | Mempersiapkan peralatan dan bahan yang diperlukan | | | | | | |
| 1.4 | Merencanakan pengkabelan | | | | | | |
| 1.5 | Mempersiapkan peralatan dan | | | | | | |
| 1.6 | Mengumpulkan informasi mengenai perangkat jaringan | | | | | | |
| 1.7 | Menentukan kebutuhan pengguna secara | | | | | | |
| 1.8 | Menetapkan persyaratan perangkat jaringan dari pengguna | | | | | | |
| 1.9 | Menyiapkan perangkat jaringan | | | | | | |
| 1.10 | Menentukan data penting yang harus di- | | | | | | |
| | Rerata capaian kompetensi komponen | | | | | | |
| I Pelaksanaan | | | | | | | |
| 2.1 | Membuat daftar teknologi dan perangkat | | | | | | |
| 2.2 | Membuat daftar teknologi yang dapat memperbaiki kinerja jaringan | | | | | | |
| 2.3 | Memasang konektor pada kabel | | | | | | |
| 2.4 | Menginstalasi pengkabelan | | | | | | |
| 2.5 | Menuliskan spesifikasi perangkat jaringan | | | | | | |
| 2.6 | Menentukan spesifikasi perangkat | | | | | | |
| 2.7 | Menginstalasi perangkat | | | | | | |
| 2.8 | Membuat spesifikasi topologi | | | | | | |
| 2.9 | Mengidentifikasi sistem operasi pada | | | | | | |
| 2.10 | Membagi alamat jaringan pada perangkat jaringan | | | | | | |
| 2.11 | Menentukan spesifikasi switch | | | | | | |
| 2.12 | Memilih switch yang tepat | | | | | | |
| 2.13 | Memasang switch | | | | | | |
| 2.14 | Meng-install perangkat keras | | | | | | |
| 2.15 | Mengkonfigurasi router pada perangkat | | | | | | |





| No | Komponen/Sub Komponen | Kompeten | | | | Catatan | |
|----------|--|----------|-------|------|-------------|---------|--|
| | | Belum | Ya | | | | |
| | | | Cukup | Baik | Sangat Baik | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
| 2.16 | Melakukan <i>restore</i> konfigurasi perangkat | | | | | | |
| | Rerata capaian kompetensi komponen | | | | | | |
| I | Hasil | | | | | | |
| 3.1 | Menguji koneksi kabel | | | | | | |
| 3.2 | Membuat dokumentasi pengkabelan terstruktur horizontal | | | | | | |
| 3.3 | Menguji perangkat | | | | | | |
| 3.4 | Mendokumentasikan pengalaman jaringan. | | | | | | |
| 3.5 | Menguji switch pada jaringan | | | | | | |
| 3.6 | Menyediakan dukungan untuk produk- | | | | | | |
| 3.7 | Menguji routing pada perangkat | | | | | | |
| 3.8 | Mendokumentasikan konfigurasi | | | | | | |
| 3.9 | Mengembangkan prosedur <i>backup</i> dan | | | | | | |
| | Rerata capaian kompetensi komponen | | | | | | |

Keterangan :

- Capaian kompetensi peserta uji per Sub Komponen dituliskan dalam bentuk ceklis (✓)
- Rerata Capaian kompetensi peserta uji per Komponen dituliskan dalam bentuk ceklis (✓)
- Jika peserta uji dinilai Belum baik pada salah satu komponen, maka peserta uji diberi kesempatan untuk mengulang
- Catatan diberikan sebagai keterangan tambahan unjuk kerja
- **Catatan positif** diberikan kepada peserta uji yang mampu menunjukkan inovasi, efisiensi kerja, dan pemecahan masalah secara kreatif.
- **Catatan negatif** diberikan kepada peserta uji yang mengulangi proses atau unjuk kerja lainnya yang bertentangan dengan kriteria unjuk kerja





KRITERIA/RUBRIK PENILAIAN

Rubrik Penilaian Aspek Keterampilan

| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian |
|-----|---|--|--|
| 1 | 2 | 3 | 4 |
| I | Persiapan | | |
| | 1.1 Melakukan survei teknis | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Daftar kebutuhan pengguna telah ditentukan. • Informasi yang dibutuhkan ditentukan. menampilkan 3 kriteria unjuk kerja
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja | Sangat Baik
Baik
Cukup Baik
Belum |
| | 1.2 Membuat daftar kebutuhan teknis pengguna jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Tabel untuk merangkum hasil survei teknis telah dipersiapkan. • Kebutuhan teknis pengguna yang menggunakan jaringan dibuat. • Daftar jumlah kebutuhan pengguna dibuat. menampilkan 3 kriteria unjuk kerja
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja | Sangat Baik
Baik
Cukup Baik
Belum |
| | 1.3 Mempersiapkan peralatan dan bahan yang diperlukan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Spesifikasi jaringan diidentifikasi. • Bahan-bahan yang diperlukan disiapkan sesuai spesifikasi. • Peralatan yang sesuai disiapkan. • Alat ukur untuk pengujian disiapkan. menampilkan 4 kriteria unjuk kerja
menampilkan 3 kriteria unjuk kerja
menampilkan 2 kriteria unjuk kerja
menampilkan <2 kriteria unjuk kerja | Sangat Baik
Baik
Cukup Baik
Belum |
| | 1.4 Merencanakan pengkabelan horizontal. | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Prosedur instalasi jaringan yang aman baik dari segi elektris maupun konstruksi disiapkan. • Diagram jalur perkabelan dibuat. • Jadwal dan urutan penyelesaian pekerjaan ditentukan. menampilkan 3 kriteria unjuk kerja
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja | Sangat Baik
Baik
Cukup Baik
Belum |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian |
|-----|--|---|-------------|
| 1 | 2 | 3 | 4 |
| | 1.5 Mempersiapkan peralatan dan bahan/materi yang diperlukan. | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> ● Topologi jaringan yang membutuhkan perangkat baru ditentukan. ● Daftar perangkat jaringan dan rancangan kapasitasnya dibuat. <p>menampilkan 3 kriteria unjuk kerja</p> <p>menampilkan 2 kriteria unjuk kerja</p> <p>menampilkan 1 kriteria unjuk kerja</p> <p>tidak menampilkan kriteria unjuk kerja</p> | |
| | | menampilkan 3 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| | 1.6 Mengumpulkan informasi mengenai perangkat jaringan yang ada di pasaran | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> ● Daftar perangkat jaringan yang dapat memenuhi kebutuhan dari berbagai vendor dibuat. ● Rentang kapasitas yang mencakup perangkat jaringan yang ada di pasaran dituliskan. ● Nilai kanasitas yang dapat dinenuhi oleh <p>menampilkan 3 kriteria unjuk kerja</p> <p>menampilkan 2 kriteria unjuk kerja</p> <p>menampilkan 1 kriteria unjuk kerja</p> <p>tidak menampilkan kriteria unjuk kerja</p> | |
| | | menampilkan 3 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| | 1.7 Menentukan kebutuhan pengguna secara keseluruhan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> ● Ruang lingkup jaringan diidentifikasi sesuai dengan usulan. ● Besarnya kapasitas jaringan dihitung berdasarkan kebutuhan bisnis. ● Spesifikasi kelas IP address ditentukan sesuai kebutuhan <p>menampilkan 3 kriteria unjuk kerja</p> <p>menampilkan 2 kriteria unjuk kerja</p> <p>menampilkan 1 kriteria unjuk kerja</p> <p>tidak menampilkan kriteria unjuk kerja</p> | |
| | | menampilkan 3 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| | 1.8 Menetapkan persyaratan perangkat jaringan dari pengguna | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> ● Perangkat jaringan diidentifikasi sesuai dengan kebutuhan jaringan. ● Persyaratan dianalisis sesuai kebutuhan teknis dan pengguna. ● Persyaratan pengguna dievaluasi sesuai pedoman organisasi. <p>menampilkan 3 kriteria unjuk kerja</p> <p>menampilkan 2 kriteria unjuk kerja</p> <p>menampilkan 1 kriteria unjuk kerja</p> <p>tidak menampilkan kriteria unjuk kerja</p> | |
| | | menampilkan 3 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian |
|-----|---|--|---------|
| 1 | 2 | 3 | 4 |
| | 1.9 Menyiapkan perangkat jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Perangkat jaringan dipilih sesuai dengan kebutuhan. • Perangkat jaringan dievaluasi sesuai dengan kebutuhan. <p>menampilkan 4 kriteria unjuk kerja
menampilkan 3 kriteria unjuk kerja
menampilkan 2 kriteria unjuk kerja
menampilkan <2 kriteria unjuk kerja</p> | |
| | 1.10 Menentukan data penting yang harus di-backup | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Konfigurasi jaringan yang meliputi akses dan keamanan diidentifikasi. • Konfigurasi perangkat jaringan yang berjalan di-backup. <p>menampilkan 2 kriteria unjuk kerja dengan tepat
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja</p> | |
| II | Pelaksanaan | | |
| | 2.1 Membuat daftar teknologi dan perangkat jaringan saat ini (existing) | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Daftar teknologi yang saat ini dipakai disusun. <p>menampilkan 2 kriteria unjuk kerja dengan
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja</p> | |
| | 2.2 Membuat daftar teknologi yang dapat memperbaiki kinerja jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Perkembangan yang ada dari semua teknologi yang dipakai dirangkum. • Teknologi yang berpotensi meningkatkan kinerja jaringan ditentukan. <p>menampilkan 2 kriteria unjuk kerja dengan
menampilkan 2 kriteria unjuk kerja
menampilkan 1 kriteria unjuk kerja
tidak menampilkan kriteria unjuk kerja</p> | |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian Kompetensi |
|-----|---|---|--------------------|
| 1 | 2 | 3 | 4 |
| 1 | 2.3 Memasang konektor pada kabel jaringan | Kriteria unjuk kerja: <ul style="list-style-type: none"> • Kabel dipotong sesuai keperluan dengan mempertimbangkan standar batasan panjang maksimum kabel. • Kabel dikupas sesuai dengan ukuran konektor. • Konektor dipasang pada kabel sesuai dengan standar urutan warna. • Urutan warna kabel (jika ada warna) dipastikan sudah sesuai standar. | |
| | | menampilkan 4-5kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2-3 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| 2 | 2.4 Menginstalasi pengkabelan horizontal | Kriteria unjuk kerja: <ul style="list-style-type: none"> • Soket RJ-45 dipasang pada dinding di wiring closet. • Perangkat dalam wiring closet dipasang. • Terminal utama (main distribution frame) atau terminal cabang (intermediate distribution frame) dipasang jika diperlukan. | |
| | | menampilkan 4-5kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2-3 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| 3 | 2.5 Menuliskan spesifikasi perangkat jaringan untuk keperluan pengguna. | Kriteria unjuk kerja: <ul style="list-style-type: none"> • Dokumen spesifikasi perangkat jaringan dibuat. • Spesifikasi yang sesuai dengan pasar dan kebutuhan dikumpulkan. | |
| | | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| 4 | 2.6 Menentukan spesifikasi perangkat | Kriteria unjuk kerja: <ul style="list-style-type: none"> • Kebutuhan detail dari perangkat ditetapkan sesuai dengan kebutuhan jaringan saat ini dan masa yang akan datang. • Kapasitas jaringan saat ini dan masa yang akan datang ditetapkan sesuai dengan kebutuhan jumlah pengguna saat ini dan masa yang akan datang. • Kebutuhan keamanan dan manajemen jaringan ditetapkan sesuai dengan kebutuhan | |
| | | Menampilkan 3 kriteria unjuk kerja | Sangat Baik |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian |
|-----|---|---|-------------|
| 1 | 2 | 3 | 4 |
| | | menampilkan 2 kriteria unjuk kerja | Bai |
| | | menampilkan 1 kriteria unjuk kerja | Cukup |
| | | tidak menampilkan kriteria unjuk kerja | Belu |
| | 2.7 Menginstalasi perangkat | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Perangkat dengan fitur yang tepat dipilih berdasarkan kebutuhan teknis. Perangkat dipasang sesuai dengan kebutuhan teknis. | |
| | | menampilkan 3 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |
| | 2.8 Membuat spesifikasi topologi jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Besaran bandwidth setiap segmen telah ditentukan. Topologi lokasi penempatan perangkat jaringan telah dipilih dengan mempertimbangkan jarak dan jumlah pengguna. Fitur-fitur fisik dipertimbangkan sebagai hasil dari desain jaringan. Peta jaringan sesuai dengan keadaan gedung/lapangan dibuat. Rancangan kebutuhan perkabelan disusun. Biaya keseluruhan diperhitungkan. Analisis proyeksi pengembangan jaringan dibuat. | |
| | | menampilkan 6-7 kriteria unjuk kerja | Sangat Baik |
| | | menampilkan 4-5 kriteria unjuk kerja | Baik |
| | | menampilkan 2-3 kriteria unjuk kerja | Cukup Baik |
| | | menampilkan <2 kriteria unjuk kerja | Belum |
| | 2.9 Mengidentifikasi sistem operasi pada jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Sistem operasi yang berjalan di jaringan diidentifikasi. Informasi cara menginstal dan konfigurasi jaringan pada sistem operasi yang dipakai | |
| | | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik |
| | | menampilkan 2 kriteria unjuk kerja | Baik |
| | | menampilkan 1 kriteria unjuk kerja | Cukup Baik |
| | | tidak menampilkan kriteria unjuk kerja | Belum |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian | | | | | | | | |
|---|--|--|---|-------------|------------------------------------|------|------------------------------------|------------|--|-------|--|
| 1 | 2 | 3 | 4 | | | | | | | | |
| | 2.1
0 Membagi alamat jaringan pada perangkat jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Jumlah node (host) jaringan ditentukan berdasarkan kebutuhan pengguna. • Kelas atau segmen alamat jaringan ditentukan berdasarkan besarnya jumlah node (host) jaringan. <table border="1"> <tr> <td>menampilkan 3 kriteria unjuk kerja</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 3 kriteria unjuk kerja | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 3 kriteria unjuk kerja | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| | 2.1
1 Menentukan spesifikasi switch | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Kapasitas jaringan disesuaikan berdasarkan dokumentasi kebutuhan bisnis saat ini. • Tipe dan jumlah switch ditetapkan <table border="1"> <tr> <td>menampilkan 2 kriteria unjuk kerja dengan</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| | 2.1
2 Memilih switch yang tepat | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Switch dengan fitur yang cocok dipilih sesuai kebutuhan. • Jumlah port disesuaikan dengan kebutuhan jaringan. <table border="1"> <tr> <td>menampilkan 2 kriteria unjuk kerja dengan</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| | 2.1
3 Memasang switch | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> • Switch dan perangkat pendukungnya dipasang berdasarkan kebutuhan jaringan. • Hubungan antar switch atau perangkat jaringan dibuat dengan menyambungkan kabel jaringan. • Switch dikonfigurasi berdasarkan kebutuhan <table border="1"> <tr> <td>menampilkan 3-4 kriteria unjuk kerja</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian | | | | | | | | |
|---|---|---|---|-------------|--|------|--|------------|--|-------|--|
| 1 | 2 | 3 | 4 | | | | | | | | |
| | 2.1
4
Meng-install perangkat keras jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Instalasi diatur agar Belum ada gangguan pada operasional jaringan. Perangkat keras dipasang sesuai dengan prosedur instalasi. Instalasi dikonfigurasi sesuai kebutuhan pengguna. <table> <tr> <td>menampilkan 3-4 kriteria unjuk kerja</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| | 2.1
5
Mengkonfigurasi router pada perangkat jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Interface pada router dikonfigurasi. Hubungan antar router dikonfigurasi. Routing diaktifkan pada router. <table> <tr> <td>menampilkan 3-4 kriteria unjuk kerja</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 3-4 kriteria unjuk kerja | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| | 2.1
6
Melakukan <i>restore</i> konfigurasi perangkat jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> Media atau dokumentasi backup dari konfigurasi perangkat jaringan yang terakhir disiapkan. Konfigurasi yang ada di media atau dokumentasi backup terakhir di- <table> <tr> <td>menampilkan 2 kriteria unjuk kerja dengan</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |
| III | Hasil | | | | | | | | | | |
| | 3.1
Menguji koneksi kabel | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> Konektivitas antar pin pada kedua konektor yang berada di ujung kabel diuji dengan menggunakan alat ukur. Hubungan antar perangkat jaringan diuji untuk memastikan konektivitas <table> <tr> <td>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk hasil kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk hasil kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk hasil kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk hasil kerja dengan tepat | Sangat Baik | menampilkan 2 kriteria unjuk hasil kerja | Baik | menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | tidak menampilkan kriteria unjuk hasil kerja | Belum | |
| menampilkan 2 kriteria unjuk hasil kerja dengan tepat | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk hasil kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk hasil kerja | Belum | | | | | | | | | | |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian |
|-----|---|--|--|
| 1 | 2 | 3 | 4 |
| | 3.2 Membuat dokumentasi pengkabelan terstruktur horizontal | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Topologi fisik jaringan digambarkan. ● Topologi logis jaringan digambarkan. <p>menampilkan 3-4 kriteria unjuk hasil kerja</p> <p>menampilkan 2 kriteria unjuk hasil kerja</p> <p>menampilkan 1 kriteria unjuk hasil kerja</p> <p>tidak menampilkan kriteria unjuk hasil kerja</p> | Sangat Baik
Baik
Cukup Baik
Belum |
| | 3.3 Menguji perangkat | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Rencana pengujian ditetapkan berdasarkan standar pengujian yang berlaku. <p>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</p> <p>menampilkan 2 kriteria unjuk hasil kerja</p> <p>menampilkan 1 kriteria unjuk hasil kerja</p> <p>tidak menampilkan kriteria unjuk hasil kerja</p> | Sangat Baik
Baik
Cukup Baik
Belum |
| | 3.4 Mendokumentasikan pengalamanan jaringan. | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Alamat masing-masing node atau perangkat jaringan dicatat. ● Dokumentasi pengalamanan jaringan dibuat. <p>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</p> <p>menampilkan 2 kriteria unjuk hasil kerja</p> <p>menampilkan 1 kriteria unjuk hasil kerja</p> <p>tidak menampilkan kriteria unjuk hasil kerja</p> | Sangat Baik
Baik
Cukup Baik
Belum |
| | 3.5 Menguji switch pada jaringan | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Perangkat switch diuji berdasarkan petunjuk pengujian. ● Perangkat switch dipastikan terhubung dengan perangkat jaringan yang lain. <p>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</p> <p>menampilkan 2 kriteria unjuk hasil kerja</p> <p>menampilkan 1 kriteria unjuk hasil kerja</p> <p>tidak menampilkan kriteria unjuk hasil kerja</p> | Sangat Baik
Baik
Cukup Baik
Belum |
| | 3.6 Menyediakan dukungan untuk produk-produk yang diinstall | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Dokumentasi petunjuk pengoperasian dibuat untuk pengguna. ● Instruksi secara individu pada pengguna. <p>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</p> <p>menampilkan 2 kriteria unjuk hasil kerja</p> <p>menampilkan 1 kriteria unjuk hasil kerja</p> <p>tidak menampilkan kriteria unjuk hasil kerja</p> | Sangat Baik
Baik
Cukup Baik
Belum |





| No. | Komponen/Sub Komponen | Indikator Penilaian | Capaian | | | | | | | | |
|---|--|--|---|-------------|--|------|--|------------|--|-------|--|
| 1 | 2 | 3 | 4 | | | | | | | | |
| | 3.7 Menguji routing pada perangkat jaringan | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Koneksi antar perangkat yang terhubung ke jaringan dibangun. ● Koneksi perangkat yang terhubung ke jaringan dengan perangkat lain di luar jaringan yang telah valid dicoba melalui <u>default routing</u>. <table border="1"> <tr> <td>menampilkan 3 kriteria unjuk hasil kerja</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk hasil kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk hasil kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk hasil kerja</td> <td>Belum</td> </tr> </table> | menampilkan 3 kriteria unjuk hasil kerja | Sangat Baik | menampilkan 2 kriteria unjuk hasil kerja | Baik | menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | tidak menampilkan kriteria unjuk hasil kerja | Belum | |
| menampilkan 3 kriteria unjuk hasil kerja | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk hasil kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk hasil kerja | Belum | | | | | | | | | | |
| | 3.8 Mendokumentasikan konfigurasi routing | <p>Kriteria unjuk hasil kerja:</p> <ul style="list-style-type: none"> ● Konfigurasi routing disimpan. ● <u>Dokumentasi konfigurasi routing dibuat.</u> <table border="1"> <tr> <td>menampilkan 2 kriteria unjuk hasil kerja dengan tepat</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk hasil kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk hasil kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk hasil kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk hasil kerja dengan tepat | Sangat Baik | menampilkan 2 kriteria unjuk hasil kerja | Baik | menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | tidak menampilkan kriteria unjuk hasil kerja | Belum | |
| menampilkan 2 kriteria unjuk hasil kerja dengan tepat | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk hasil kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk hasil kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk hasil kerja | Belum | | | | | | | | | | |
| | 3.9 Mengembangkan prosedur backup dan restore konfigurasi jaringan | <p>Kriteria unjuk kerja:</p> <ul style="list-style-type: none"> ● Prosedur backup dan restore yang telah ada dievaluasi. ● Prosedur backup dan restore diperbarui. <table border="1"> <tr> <td>menampilkan 2 kriteria unjuk kerja dengan</td> <td>Sangat Baik</td> </tr> <tr> <td>menampilkan 2 kriteria unjuk kerja</td> <td>Baik</td> </tr> <tr> <td>menampilkan 1 kriteria unjuk kerja</td> <td>Cukup Baik</td> </tr> <tr> <td>tidak menampilkan kriteria unjuk kerja</td> <td>Belum</td> </tr> </table> | menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | menampilkan 2 kriteria unjuk kerja | Baik | menampilkan 1 kriteria unjuk kerja | Cukup Baik | tidak menampilkan kriteria unjuk kerja | Belum | |
| menampilkan 2 kriteria unjuk kerja dengan | Sangat Baik | | | | | | | | | | |
| menampilkan 2 kriteria unjuk kerja | Baik | | | | | | | | | | |
| menampilkan 1 kriteria unjuk kerja | Cukup Baik | | | | | | | | | | |
| tidak menampilkan kriteria unjuk kerja | Belum | | | | | | | | | | |



**LEMBAR PENILAIAN SIKAP**

Nama :

Kelas/Semester : /

Waktu Penilaian :

| Aspek Penilaian | Penilaian | | | |
|-----------------|-----------|------|------------|--------|
| | Sangat | Baik | Cukup Baik | Kurang |
| Ketelitian | | | | |
| Kecermatan | | | | |
| Kerapihan | | | | |
| Kecekatan | | | | |

Mengetahui,
Guru Mata Pelajaran,

to





Rubrik Penilaian Aspek Sikap

| No. | Komponen/Sub Komponen | Indikator Penilaian | Tingk |
|-----|-----------------------|--|--------|
| 1 | 2 | 3 | 4 |
| 1 | Ketelitian | Kriteria unjuk sikap kerja:
<ul style="list-style-type: none"> ● Mengerjakan tugas dengan teliti <ul style="list-style-type: none"> ● Berhati-hati dalam menyelesaikan tugas dan menggunakan peralatan ● Mampu menyelesaikan pekerjaan sesuai dengan | |
| | | menampilkan 3-4 kriteria unjuk sikap kerja | Sangat |
| | | menampilkan 2 kriteria unjuk sikap kerja | Baik |
| | | menampilkan 1 kriteria unjuk sikap kerja | Cukup |
| | | tidak menampilkan kriteria unjuk sikap kerja | Kurang |
| 2 | Kecermatan | Kriteria unjuk sikap kerja:
<ul style="list-style-type: none"> ● Kerja dilaksanakan dengan aman sehubungan sesuai prosedur. <ul style="list-style-type: none"> ● Perlengkapan pelindung diri dipakai dan disimpan sesuai dengan prosedur ● Semua perlengkapan dan alat-alat keselamatan digunakan sesuai dengan kegunaannya. ● Tanda-tanda/simbol keselamatan dikenali | |
| | | menampilkan 4-5 kriteria unjuk sikap kerja | Sangat |
| | | menampilkan 2-3 kriteria unjuk sikap kerja | Baik |
| | | menampilkan 1 kriteria unjuk sikap kerja | Cukup |
| | | tidak menampilkan kriteria unjuk sikap kerja | Kurang |
| 3 | Kerapihan | Kriteria unjuk sikap kerja:
<ul style="list-style-type: none"> ● Peralatan disimpan pada tempatnya ● Kabel ditata dengan rapih <ul style="list-style-type: none"> ● Sisa bahan yang Kurang berguna dibuang pada | |
| | | menampilkan 3 kriteria unjuk sikap kerja | Sangat |
| | | menampilkan 2 kriteria unjuk sikap kerja | Baik |
| | | menampilkan 1 kriteria unjuk sikap kerja | Cukup |
| | | tidak menampilkan kriteria unjuk sikap kerja | Kurang |
| 4 | Kecepatan | Kriteria unjuk sikap kerja:
<ul style="list-style-type: none"> ● Instruksi dikerjakan dengan cepat dan tepat ● Cepat dan tepat dalam memasang dan mengkonfigurasi alat | |
| | | menampilkan 3 kriteria unjuk sikap kerja | Sangat |
| | | menampilkan 2 kriteria unjuk sikap kerja | Baik |
| | | menampilkan 1 kriteria unjuk sikap kerja | Cukup |
| | | tidak menampilkan kriteria unjuk sikap kerja | Kurang |

LEMBAR KERJA PESERTA DIDIK (LKPD)

LEMBAR KERJA PESERTA DIDIK 1

1. Berkelompoklah menjadi 8 (delapan) kemudian tulis nama dan nomor absen peserta didik di kelompokmu
2. Carilah materi di internet tentang pengertian pengertian, jenis, tipe, macam-macam, fungsi, prinsip dasar kebijakan, celah / lubang ancaman, jenis-jenis metode penyerangan dan sistem proteksi pada keamanan jaringan.
3. Diskusikan Bersama kelompokmu tema kejahatan bidang keamanan jaringan sebagai berikut (satu kelompok satu tema)
 - a. Serangan malware
 - b. Serangan phishing
 - c. Serangan DDoS
 - d. Serangan Man-in-the-Middle
 - e. Serangan Brute Force
 - f. Serangan Ransomware
 - g. Serangan Zero-day
 - h. Serangan Perusakan (Sabotage)
4. Sebutkan jenis pelaku kejahatan keamanan jaringan:
 - a) Hacker
 - b) Cracker
 - c) Script Kiddie
 - d) Insiders
 - e) Spammer
 - f) Scammer
 - g) Cyber Criminal Organizations
 - h) Nation-state Actors
 - i) Activists atau Hacktivists
 - j) Penyelidik Keamanan (Security Researchers)
5. Tuangkan Hasil Diskusimu dalam bentuk file presentasi,lakukanlah pencarian dari internet menggunakan perangkat yang ada dan Jangan lupa mencantumkan sumber materi dalam menyusun laporannya.
6. Susun laporan hasil diskusi, tuliskan semua tanggapan yang diberikan oleh kelompok lain, bisa dalam bentuk deskripsi, PPT, ataupun Video dan sertakan foto-foto pendukung karya hasil diskusimu.
7. Presentasikan di depan kelas secara bergiliran.
8. Simpan hasil karyamu sebagai portofolio.

LEMBAR KEGIATAN PESERTA DIDIK 2

1. Apa itu Wireshark dan bagaimana fungsinya dalam analisis jaringan?
2. Bagaimana cara menginstal dan mengkonfigurasi Wireshark pada sistem operasi yang berbeda?
3. Apa perbedaan antara Capture Filter dan Display Filter dalam Wireshark?
4. Bagaimana cara menggunakan Wireshark untuk menangkap paket data dalam jaringan?
5. Apa kegunaan kolom-kolom yang tersedia dalam tampilan paket Wireshark?
6. Bagaimana cara menerapkan filter pada data tangkapan paket menggunakan Wireshark?
7. Apa langkah-langkah yang perlu diambil untuk menganalisis protokol tertentu, misalnya HTTP atau DNS, menggunakan Wireshark?
8. Bagaimana Wireshark dapat membantu dalam mendekripsi dan menangani serangan jaringan, seperti serangan DDoS atau serangan brute force?
9. Apa saja ekstensi atau plugin yang tersedia untuk Wireshark dan bagaimana cara menggunakannya untuk analisis yang lebih canggih?
10. Bagaimana Wireshark dapat digunakan dalam pemecahan masalah jaringan, termasuk mengidentifikasi penyebab kegagalan jaringan atau masalah kinerja?

LEMBAR KEGIATAN PESERTA DIDIK 3

4. Tulislah jenis-jenis serangan jaringan dengan metode yang digunakan yang pernah terjadi baik di dalam negeri maupun diluar negeri.
5. Analisis pemindaian Port dari kategori sbb:
 - A. Protokol Jaringan Dasar
 1. Analisis protokol IP (Internet Protocol)
 2. Analisis protokol TCP (Transmission Control Protocol)
 3. Analisis protokol UDP (User Datagram Protocol)
 - B. Protokol Aplikasi
 1. Analisis protokol HTTP (Hypertext Transfer Protocol)
 2. Analisis protokol DNS (Domain Name System)
 3. Analisis protokol FTP (File Transfer Protocol)
 4. Analisis protokol SMTP (Simple Mail Transfer Protocol)
 5. Analisis protokol SSH (Secure Shell)
 6. Analisis protokol SSL/TLS (Secure Sockets Layer/Transport Layer Security)
 7. Analisis protokol VoIP (Voice over Internet Protocol)
6. Jelaskan salah satu metode penggunaan celah keamanan port yang kalian gunakan.
7. Observasilah dan berikan saran serta langkah-langkah praktis untuk memanfaatkan tools keamanan jaringan dengan efektif

LAMPIRAN

RUBRIK PENILAIAN

Asesmen Proses

| No | Kelompok | Keterbacaan Materi | | Karya berupa Peta Konsep | | Kreativitas | | Laporan Diskusi | | Presentasi | |
|----|----------|--------------------|-----|--------------------------|-----|-------------|-----|-----------------|-----|------------|-----|
| | | Ya | Tdk | Ya | Tdk | Ya | Tdk | Ya | Tdk | Ya | Tdk |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

Asesmen Akhir : (Nama)

| Nama Siswa: | | | | | | |
|-------------|--|--|---|---------------------|--------------------|--------------|
| No | Kreteria Ketuntasan | | | KETERCAPAIAN | | |
| | | | | Kurang kompeten (1) | Cukup Kompeten (2) | Kompeten (3) |
| 1 | Memuat judul sistem keamanan jaringan | | | | v | |
| 2 | Mengidentifikasi Konsep dasar tentang jaringan komputer dan perangkat jaringan yang umum digunakan | | | | | v |
| 3 | Mengidentifikasi Etika dan kebijakan pengguna jaringan. | | | | v | |
| 4 | Mengidentifikasi tujuan, aspek prinsip dan manfaat dari sistem keamanan jaringan. | | | | v | |
| 5 | Mengidentifikasi jenis-jenis metode penyerangan sistem keamanan jaringan. | | v | | | |
| 6 | Mengidentifikasi jenis-jenis sistem proteksi pada keamanan jaringan. | | | | v | |
| 7 | Mengidentifikasi Tools keamanan jaringan yang digunakan | | | v | | |
| 8 | Mengidentifikasi kelebihan dan kekurangan Tools keamanan jaringan yang digunakan. | | | v | | |

KKTP:

| | |
|-----------|--|
| 0 – 40 % | Belum tuntas, remidi pada seluruh materi |
| 41 – 60 % | Belum tuntas, remidi pada materi yang belum dikuasai |
| 61 – 80 % | Sudah tuntas, tetapi tanpa pengayaan |
| 81 – 100% | Sudah tuntas, perlu pengayaan atau tantangan lebih |