

# MODUL AJAR FASE F

# SISTEM KEAMANAN JARINGAN

1

TUJUAN  
PEMBELAJARAN



**Modul 1**

**TP : Konsep Dasar Sistem Keamanan  
Jaringan**



Idiarso, S.Kom

SISTEM INFORMASI  
JARINGAN DAN APLIKASI



**MODUL AJAR 1**  
**Konsep Dasar Sistem Keamanan 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 konsep terkait sistem keamanan jaringan

### Indikator Ketercapaian Tujuan Pembelajaran

- Memahami konsep sistem keamanan jaringan dan pentingnya perlindungan data.
- Memahami Konsep dasar tentang jaringan komputer dan perangkat jaringan yang umum digunakan
- Memahami Etika dan kebijakan pengguna jaringan.
- Memahami celah / lubang dan ancaman keamanan jaringan yang umum dihadapi.
- Memahami tujuan, aspek prinsip dan manfaat dari sistem keamanan jaringan.
- Mengidentifikasi jenis-jenis metode penyerangan sistem keamanan jaringan.
- Memahami jenis-jenis sistem proteksi pada keamanan jaringan.
- Melakukan debat argumen tentang hacker dan cracker.
- Melakukan Analisis Packet dalam jaringan
- Memahami jenis-jenis Protokol jaringan
- Memahami Implementasi Web Proxy menggunakan mikrotik
- Memahami penerapan Proxy internal dan proxy external

## 2. LANGKAH PEMBELAJARAN

### Pertemuan 1 (4x45 menit)

- Pendahuluan** : 1) Apersepsi diberikan guru kepada peserta didik melalui pertanyaan pemantik yang disampaikan guru;
- a. Apa yang kalian ketahui tentang Sistem Keamanan Jaringan ?
  - b. Mengapa jaringan perlu perlindungan keamanan ?
- 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 Sistem Keamanan Jaringan
- b. Mendeskripsikan Kebijakan dan etika menggunakan jaringan
- c. Mencari tahu bahaya apa saja yang dapat mengancam

**Inti** jaringan

- - 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 pengertian, jenis, tipe, macam-macam, fungsi, prinsip dasar kebijakan, celah / lubang ancaman, jenis-jenis metode penyerangan dan sistem proteksi pada keamanan 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 apakah menyenangkan, materi yang dibahas apakah mudah dipahami, apakah semua peserta didik paham, siapa saja yang belum
  - 6) apakah ada 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 (16x45 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 pahami tentang konsep keamanan jaringan pada pertemuan kemarin ?
  - b. Apa saja Tool atau alat yang kita gunakan untuk dapat membantu melindungi jaringan dari serangan dan ancaman ?

**Inti**

- : 1) Peserta didik diajak menonton bersama tayangan video tentang serangan pada jaringan melalui link  
[Video https://www.youtube.com/watch?v=xtoEmfaZMsU,](https://www.youtube.com/watch?v=xtoEmfaZMsU)  
kemudian Peserta Didik diminta untuk menonton video selanjutnya tentang tools atau alat-alat apa saja yang dapat digunakan untuk mendeteksi serangan melalui link  
<https://www.youtube.com/watch?v=aExLMwdxRq8> dan  
[https://www.youtube.com/watch?v=X1\\_B\\_GIwSqs](https://www.youtube.com/watch?v=X1_B_GIwSqs)  
menggunakan layar, laptop dan LCD. Peserta didik diminta menjawab kira-kira apa tipe serangan yang digunakan dan tools atau alat apa yang bisa digunakan untuk mendeteksi serangan tersebut, kemudian guru memberikan gambaran sekilas mengapa menayangkan video tersebut.
- 2) Setelah melakukan pengamatan dari hasil menonton video, Peserta didik diminta untuk mempraktikan beberapa alat yang sudah disediakan di lab komputer kemudian menginstal Aplikasi wireshark dan beberapa aplikasi pendukung lainnya.
- 3) Peserta Didik memberikan tanggapan dan mengisikannya dalam bentuk form seperti tercantum dalam LKPD 2.
- 4) Peserta didik dibagi menjadi 8 kelompok diskusi Masing-masing kelompok diberikan waktu untuk melakukan presentasi .
- 5) Peserta didik lain memberikan tanggapan dalam bentuk pertanyaan,saran, dan masukan. Pendidik melakukan observasi serta memberikan bantuan ketika ada pertanyaan yang belum bisa dijawab.

<b>Penutup (45 menit)</b>	<ul style="list-style-type: none"> <li>: 1) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.</li> <li>2) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi perkembangan alat bantu keamanan jaringan dari teknologi konvensional sampai dengan teknologi modern, adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.</li> <li>3) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam</li> </ul>
---------------------------	--

<b>Pertemuan 3 (8x45 menit)</b>	
<b>Pendahuluan</b>	<ul style="list-style-type: none"> <li>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal; <ul style="list-style-type: none"> <li>a. Apa yang kalian pahami tentang konsep pemindaian port dalam jaringan pada pertemuan kemarin?</li> <li>b. Menurut kalian bagaimana cara menentukan langkah awal yang kita gunakan untuk mengetahui anomali dalam jaringan ?</li> <li>c. Apa saja protokol yang digunakan dalam komunikasi data dalam jaringan ?</li> </ul> </li> </ul>

<b>Inti</b>	<p>: 1) Peserta didik diajak menonton bersama tayangan Video Protokol dan Pemodelan Jaringan melalui link <a href="https://www.youtube.com/watch?v=6spUGFUOokw">https://www.youtube.com/watch?v=6spUGFUOokw</a> menggunakan layar, laptop dan LCD.</p> <p>2) Peserta didik diminta menjawab kira-kira protokol apa saja yang digunakan untuk komunikasi data dalam jaringan dan bagaimana kedudukannya dalam lapisan osi layers</p> <p>3) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 3</p> <p>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 (P3 Dimensi Kreatif: Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala</p>
-------------	---

<b>Penutup (45 menit)</b>	<p>: 1) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.</p> <p>2) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.</p> <p>3) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam</p>
---------------------------	---

<b>Pertemuan 4 (12x45 menit)</b>	
<b>Pendahuluan</b>	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <p>a. Apa yang kalian pahami tentang konsep Web Proxy ?</p> <p>b. Menurut kalian bagaimana cara kerja jenis-jenis implementasi <i>Web Proxy</i> ?</p> <p>c. Bagaimana Mengaplikasikan Web Proxy Menggunakan Routerboard Mikrotik ?</p>

<b>Inti</b>	<p>: 5) Peserta didik diajak untuk mencari diinternet tentang implemenatsi Web Proxy dan sebagai bahan referensi awal Peserta didik juga diharapkan mengunjungi link <a href="https://blog.dnetprovider.id/2018/11/02/tutorial-mikrotik-membuat-web-proxy-pada-mikrotik/">https://blog.dnetprovider.id/2018/11/02/tutorial-mikrotik-membuat-web-proxy-pada-mikrotik/</a></p> <p>6) Peserta didik diminta untuk mempraktikan Web Proxy menggunakan routerboard mikrotik yang sudah disediakan</p> <p>7) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 4</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 (P3 Dimensi Kreatif: Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala</p>
-------------	--

<b>Penutup (45 menit)</b>	<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 web proxy 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>
---------------------------	---

<b>Pertemuan 5 (16x45 menit)</b>	
<b>Pendahuluan</b>	<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 Web Proxy menggunakan Mikrotik , bisakah kalian praktik menggunakan selain mikrotik ?</p> <p>b. Apa yang kalian pahami tentang Squid proxy ?</p> <p>c. Bagaimana cara kerja Squid proxy disisi server ?</p>

<b>Inti</b>	<p>: 9) Peserta didik diajak untuk mencari diinternet tentang implementasi Web Proxy menggunakan Squid proxy.</p> <p>10) Peserta didik diminta untuk mempraktikan Web Proxy External menggunakan Squid proxy pada sistem operasi Linux menggunakan mesin virtual yang nantinya akan digunakan sebagai implementasi server</p> <p>11) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 5</p> <p>12) 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 (<b>P3 Dimensi Kreatif: Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala</b></p>
<b>Penutup (45 menit)</b>	<p>: 7) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.</p> <p>8) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi web proxy external , adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.</p> <p>9) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam</p>

<b>Pertemuan 6 (24x45 menit)</b>	
<b>Pendahuluan</b>	<p>: 1) Peserta didik merespon apersepsi yang disampaikan guru dalam mengawali kegiatan pembelajaran dengan menjawab pertanyaan pemantik sekaligus asesmen awal;</p> <ul style="list-style-type: none"> <li>a. Setelah kalian dari awal kalian mengetahui tentang sistemkeamanan jaringan dari awal sampai implementasi Web Proxy, dapatkah kalian membuat konfigurasi menyeluruh secara Komperehensif ?</li> <li>b. Bisakah kalian membuat miniatur jaringan berdasarkan materi yang telah dipelajari ?</li> </ul>
<b>Inti</b>	<p>: 2) Peserta didik diajak membuat miniatur jaringan yang terdiri atas :</p> <ol style="list-style-type: none"> <li>1. Perangkat Mikrotik</li> <li>2. Switch</li> <li>3. Sitem operasi menggunakan mesin virtual</li> <li>4. Accespoint sebagai pemanclar Hotspot</li> <li>4. Kabel Lan untuk disebarluaskan melalui jaringan lokal</li> </ol> <p>13) Peserta didik diminta untuk mengumpulkan perangkat dan bahan lain penunjang lainnya yang telah disediakan di lab komputer</p> <p>14) Peserta didik dibagi menjadi 8 kelompok untuk berdiskusi sebagaimana tercantum pada LKPD 6</p> <p>15) 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 (<b>P3 Dimensi Kreatif: Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala</b></p>

<b>Penutup (45 menit)</b>	<p>: 10) Peserta didik dibimbing untuk menyimpulkan keseluruhan hasil diskusi, dan guru memberikan penguatan.</p> <p>11) Peserta didik menyampaikan refleksi dan tindak lanjut, terkait penyampaian materi apakah menyenangkan, sampai di mana pemahaman materi konfigurasi keamanan jaringan menggunakan miniatur jaringan lokal, adakah yang belum paham, belum pahamnya di bagian mana, dan berapa peserta didik yang belum paham.</p> <p>12) Peserta didik mendengarkan informasi guru terkait aktivitas selanjutnya dan pertemuan ditutup dengan doa dan salam</p>
---------------------------	---

### 3. ASESMEN

<b>Asesmen Awal</b>	<p>:</p> <ul style="list-style-type: none"> <li>a. Menjelaskan Pengertian sistem keamanan jaringan dan pentingnya perlindungan data.</li> <li>b. Menjelaskan Konsep dasar tentang jaringan komputer dan perangkat jaringan yang umum digunakan</li> <li>c. Menjelaskan Etika dan kebijakan pengguna jaringan.</li> <li>d. Menjelaskan celah / lubang dan ancaman keamanan jaringan yang umum dihadapi.</li> <li>e. Menjelaskan tujuan, aspek prinsip dan manfaat dari sistem keamanan jaringan.</li> <li>f. Mengidentifikasi jenis-jenis metode penyerangan sistem keamanan jaringan.</li> <li>g. Menjelaskan jenis-jenis sistem proteksi pada keamanan jaringan. Menjelaskan tool dalam sistem keamanan jaringan dan bagaimana tool ini dapat membantu melindungi jaringan dari serangan dan ancaman.</li> </ul>
<b>Asesmen Proses</b>	<p>:</p> <p>Observasi diskusi sesuai LKPD 1, LKPD 2, LKPD 3, LKPD 4 dan LKPD 5</p>
<b>Asesmen Akhir</b>	<p>:</p> <p>Observasi Video keamanan jaringan dan jenis-jenis serangan yang mengancam keamanan jaringan dengan celah port dan protokol yang paling rentan dipandu dengan LKPD 6</p>

## **LEMBAR KERJA PESERTA DIDIK (LKPD)**

### **LEMBAR KEGIATAN 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 (Sabotase)
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**

11. Apa itu Wireshark dan bagaimana fungsinya dalam analisis jaringan?
12. Bagaimana cara menginstal dan mengkonfigurasi Wireshark pada sistem operasi yang berbeda?
13. Apa perbedaan antara Capture Filter dan Display Filter dalam Wireshark?
14. Bagaimana cara menggunakan Wireshark untuk menangkap paket data dalam jaringan?
15. Apa kegunaan kolom-kolom yang tersedia dalam tampilan paket Wireshark?
16. Bagaimana cara menerapkan filter pada data tangkapan paket menggunakan Wireshark?
17. Apa langkah-langkah yang perlu diambil untuk menganalisis protokol tertentu, misalnya HTTP atau DNS, menggunakan Wireshark?
18. Bagaimana Wireshark dapat membantu dalam mendekripsi dan menangani serangan jaringan, seperti serangan DDoS atau serangan brute force?
19. Apa saja ekstensi atau plugin yang tersedia untuk Wireshark dan bagaimana cara menggunakannya untuk analisis yang lebih canggih?
20. Bagaimana Wireshark dapat digunakan dalam pemecahan masalah jaringan, termasuk mengidentifikasi penyebab kegagalan jaringan atau masalah kinerja?

## **LEMBAR KEGIATAN PESERTA DIDIK 3**

1. Tulislah jenis-jenis serangan jaringan dengan metode yang digunakan yang pernah terjadi baik di dalam negeri maupun diluar negeri.
2. 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)
3. Jelaskan salah satu metode penggunaan celah keamanan port yang kalian gunakan.
4. Observasilah dan berikan saran serta langkah-langkah praktis untuk memanfaatkan tools keamanan jaringan dengan efektif

## **LEMBAR KEGIATAN PESERTA DIDIK 4**

### **Soal Latihan**

Buatlah konfigurasi untuk mengatur jaringan LAN, hotspot, dan web proxy sederhana pada MikroTik RouterOS dengan mengikuti panduan sebagai berikut :

1. Mengatur IP Address pada Interface:

```
```
/ip address
add address=192.168.1.1/24 interface=ether1 comment="LAN Interface"
add address=10.0.0.1/24 interface=ether2 comment="Hotspot Interface"
```
```

2. Mengaktifkan DHCP Server untuk jaringan LAN:

```
```
/ip dhcp-server
add interface=ether1 address-pool=LAN-pool disabled=no
/ip dhcp-server network
add address=192.168.1.0/24 gateway=192.168.1.1 dns-server=8.8.8.8
comment="LAN Network"
/ip pool
add name=LAN-pool ranges=192.168.1.2-192.168.1.254
```
```

3. Mengaktifkan Hotspot:

```
```
/ip hotspot profile
add name=hotspot-profile dns-name=hotspot.domain.com hotspot-address=10.0.0.1
login-by=http-pap
/ip hotspot
add name=hotspot interface=ether2 address-pool=hotspot-pool profile=hotspot-profile
disabled=no
/ip pool
add name=hotspot-pool ranges=10.0.0.2-10.0.0.254
```
```

4. Mengatur Web Proxy:

```
```
/ip proxy
set enabled=yes
/ip proxy access
add dst-host=facebook.com action=deny
/ip proxy cache
set enabled=yes
/ip proxy cache on-disk
```
```

```
set enabled=yes
```

```
```
```

Dalam konfigurasi di atas, Anda perlu mengganti "ether1" dan "ether2" dengan nama interface yang sesuai pada perangkat MikroTik Anda. Juga, pastikan untuk mengubah alamat jaringan, nama domain, dan aturan akses web proxy sesuai dengan kebutuhan Anda.

Setelah melakukan konfigurasi di atas, Anda harus memiliki jaringan LAN yang menggunakan IP Address 192.168.1.0/24 dengan gateway 192.168.1.1. Hotspot akan menggunakan IP Address 10.0.0.0/24 dengan alamat hotspot pada 10.0.0.1. Web proxy akan diaktifkan dengan aturan yang telah ditentukan.

Harap dicatat bahwa ini adalah contoh konfigurasi dasar dan Anda mungkin perlu menyesuaikannya sesuai dengan kebutuhan dan struktur jaringan Anda. Penting untuk memahami konfigurasi yang Anda terapkan dan memastikan kompatibilitas dengan perangkat MikroTik dan versi RouterOS yang digunakan.

## LEMBAR KEGIATAN PESERTA DIDIK 5

Praktikan langkah-langkah umum untuk melakukan konfigurasi iptables:

1. Periksa status iptables saat ini:

- Gunakan perintah `iptables -L` untuk melihat aturan-aturan yang ada pada masing-masing rantai (chain) iptables.
- Gunakan perintah `iptables -S` untuk melihat aturan-aturan iptables dalam format yang lebih terstruktur.

2. Tentukan kebijakan default:

- Tentukan kebijakan default untuk setiap rantai (chain) iptables, yaitu INPUT, OUTPUT, dan FORWARD. Misalnya, Anda dapat menggunakan perintah `iptables -P <chain> <policy>` untuk menetapkan kebijakan default. Contohnya: `iptables -P INPUT DROP` akan mengatur kebijakan default INPUT menjadi DROP (menolak semua lalu lintas masuk kecuali yang diizinkan).

3. Tambahkan aturan baru:

- Gunakan perintah `iptables -A <chain> <options>` untuk menambahkan aturan baru ke dalam rantai (chain) iptables. `<chain>` adalah nama rantai yang ingin Anda tambahkan aturan, dan `<options>` adalah opsi dan parameter yang sesuai untuk aturan tersebut. Misalnya, `iptables -A INPUT -p

`tcp --dport 22 -j ACCEPT` akan menambahkan aturan yang mengizinkan koneksi SSH (port 22) masuk ke sistem.

4. Konfigurasi aturan-aturan iptables:

- Anda dapat menggunakan opsi dan parameter yang berbeda dalam perintah `iptables` untuk mengkonfigurasi aturan sesuai kebutuhan Anda. Beberapa contoh opsi yang sering digunakan antara lain: `-p` untuk menentukan protokol, `--dport` untuk menentukan port tujuan, `-s` dan `-d` untuk menentukan alamat sumber dan tujuan, dan `-j` untuk menentukan aksi yang diambil.

5. Simpan konfigurasi iptables:

- Gunakan perintah `iptables-save` untuk menyimpan konfigurasi iptables yang sudah Anda buat. Hal ini akan menyimpan konfigurasi ke dalam file yang dapat dipulihkan saat sistem di-restart.

6. Aktifkan konfigurasi iptables saat boot:

- Agar konfigurasi iptables diterapkan setiap kali sistem di-boot, pastikan Anda menjalankan skrip iptables saat inisialisasi sistem. Caranya dapat bervariasi tergantung pada distribusi Linux yang Anda gunakan. Anda dapat menambahkan entri yang sesuai dalam skrip inisialisasi sistem, seperti `/etc/rc.local` atau menggunakan mekanisme lain yang disediakan oleh sistem operasi Anda.

8. sebagai bahan referensi kalian bisa mengikuti link berikut

<https://www.niagahoster.co.id/blog/tutorial-iptables/>

Pastikan untuk memiliki pemahaman yang baik tentang cara kerja iptables dan melakukan uji coba sebelum menerapkan konfigurasi iptables pada sistem produksi. Kesalahan konfigurasi dapat menyebabkan kehilangan akses jaringan atau server yang tidak diinginkan. Juga, disarankan untuk mengacu pada dokumentasi resmi dan sumber daya yang relevan untuk informasi lebih lanjut tentang konfigurasi iptables sesuai dengan sistem operasi Linux yang Anda gunakan.

7. Tuliskan beserta hasil screenshoot gambar langkah-langkah yang kalian kerjakan

## **LEMBAR KEGIATAN PESERTA DIDIK 6**

1. Buatlah miniatur jaringan dengan implementasi keamanan menggunakan 2 Percobaan
  - a. mikrotik
  - b. Linux
2. Dokumentasikan hasil pekerjaan kedalam sebuah Video dan di upload di youtube

### **LAMPIRAN**

#### **RUBRIK PENILAIAN**

##### **Asesmen Proses**

| No | Kelompok | Keterba<br>caan<br>Materi |     | Karya<br>berupa<br>Peta<br>Konsep |     | Kreativita<br>s |     | Lapora<br>n<br>Disku<br>si |     | Presenta<br>si |     |
|----|----------|---------------------------|-----|-----------------------------------|-----|-----------------|-----|----------------------------|-----|----------------|-----|
|    |          | Ya                        | Tdk | Ya                                | Tdk | Ya              | Tdk | Ya                         | Tdk | Ya             | Tdk |
|    |          |                           |     |                                   |     |                 |     |                            |     |                |     |
|    |          |                           |     |                                   |     |                 |     |                            |     |                |     |
|    |          |                           |     |                                   |     |                 |     |                            |     |                |     |
|    |          |                           |     |                                   |     |                 |     |                            |     |                |     |

##### **Asesmen Akhir : (Nama)**

| Nama Siswa: |                                                                                                    | KETERCAPAIAN              |                          |                 |
|-------------|----------------------------------------------------------------------------------------------------|---------------------------|--------------------------|-----------------|
| No          | Kreteria<br>Ketuntasa<br>n                                                                         | Kurang<br>kompete<br>n(1) | Cukup<br>Kompete<br>n(2) | Kompete<br>n(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 %  | <i>Belum tuntas, remidi pada seluruh materi</i>             |
| 41 – 60 % | <i>Belum tuntas, remidi pada materi yang belum dikuasai</i> |
| 61 – 80 % | <i>Sudah tuntas, tetapi tanpa pengayaan</i>                 |
| 81 – 100% | <i>Sudah tuntas, perlu pengayaan atau tantangan lebih</i>   |

### Profil Pelajar Pancasila

| No | Dimensi Kreatif-Sub Elemen                                                                                                                                                                                                                                 | Terlihat maks | Terlihat sedikit | Belum terlihat |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------------|----------------|
| 1  | Mengeksplorasi dan mengekspresikan pikiran dan/atau perasaannya dalam bentuk karya dan/atau tindakan, serta mengevaluasinya dan mempertimbangkan dampak dan risikonya bagi diri dan lingkungannya                                                          |               |                  |                |
| 2  | Menghasilkan gagasan yang beragam untuk mengekspresikan pikiran dan/atau perasaannya, menilai gagasannya, serta memikirkan segala risikonya dengan mempertimbangkan banyak perspektif seperti etika dan nilai kemanusiaan ketika gagasannya direalisasikan |               |                  |                |

### **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                 | : Ujian Tulis (Uraian dan Pilihan Ganda)            |
| d. Proses                 | : Tes Lisan (Format Assessmen Kinerja Proses)       |
| e. Keterampilan           | : Praktikum (Format Assessmen Kinerja Keterampilan) |

#### **2. Instrumen penilaian**

- |                       |                                   |
|-----------------------|-----------------------------------|
| a. Lembar Penilaian 1 | : 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

Mengetahui  
Kepala SMK Negeri 1 Punggelan

Banjarnegara, 19 Juni 2023  
Guru Mata Pelajaran,

**Drs. Supriyadi**  
**NIP. 19660128 199302 1 002**

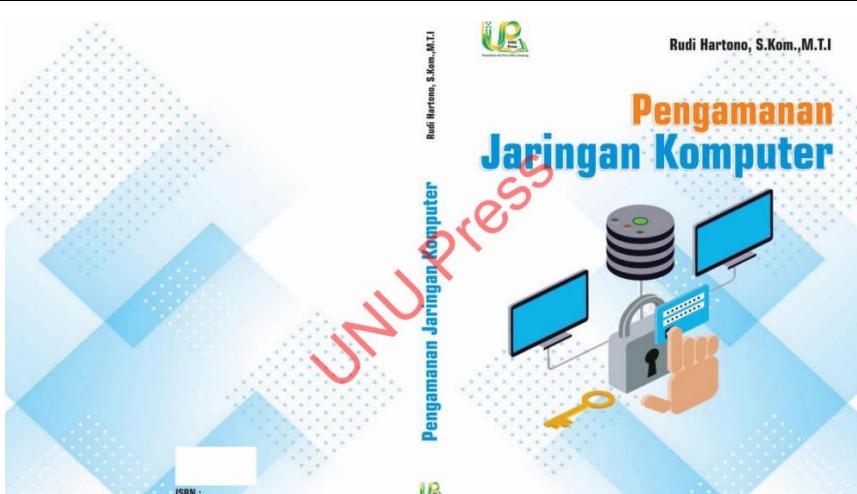
**Idiarso, S.Kom**  
**NIP.19830804 202221 1 006**

## BAHAN BACAAN

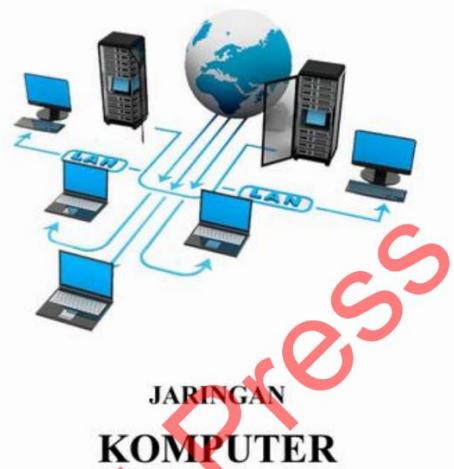
Sistem Keamanan Jaringan.

|                                                                                                                                                                                                                                                                      |                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>SISTEM INFORMATIKA JARINGAN DAN APLIKASI<br/>SMKN 1 PUNGGELAN</b></p>  <p><b>SISTEM<br/>KEAMANAN<br/>JARINGAN</b></p> <p>By : Idiarso, S.Kom</p> |                                                                                                                                                             |
| <b>LINK:</b>                                                                                                                                                                                                                                                         | <a href="https://idiuptocode.blogspot.com/2022/07/sistem-keamanan-jaringan.html">https://idiuptocode.blogspot.com/2022/07/sistem-keamanan-jaringan.html</a> |

Buku Pengamanan Jaringan Komputer

|                                                                                                                                                                                        |                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p><b>Pengamanan<br/>Jaringan Komputer</b></p> <p>Rudi Hartono, S.Kom., M.T.I</p> <p>UNUPress</p> |                                                                                                                                                                                                                                                                           |
| <b>LINK:</b>                                                                                                                                                                           | <a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a> |

## Buku Jaringan Komputer



|       |                                                                                                                                                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LINK: | <a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a> |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Ebook Desain Keamanan Jaringan

E-BOOK

DESAIN  
KEAMANAN  
JARINGAN

|       |                                                                                                                                                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LINK: | <a href="https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan">https://drive.google.com/drive/u/0/search?fbclid=IwAR3ikp4fZw-myJQH1He4bo_ay_U_i9SZ23pG2mT9SWmaiKA0wsynEfKmtQQ&amp;q=jaringan</a> |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## **Glosarium**

Serangan Distributed Denial of Service (DDoS): Serangan di mana penyerang menggunakan banyak perangkat yang terdistribusi secara geografis untuk mengirimkan lalu lintas yang sangat tinggi ke sebuah jaringan atau server, dengan tujuan menghancurkan ketersediaan layanan.

Serangan Man-in-the-Middle (MITM): Serangan di mana penyerang mengintersepsi komunikasi antara dua pihak yang sah dan dapat memanipulasi atau memonitor data yang dikirimkan.

Serangan Brute Force: Serangan di mana penyerang mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi untuk mendapatkan akses yang tidak sah.

Serangan Ransomware: Serangan di mana perangkat atau sistem dikunci oleh penyerang dan pemilik harus membayar tebusan untuk mendapatkan akses kembali.

Serangan Phishing: Serangan di mana penyerang mencoba memperoleh informasi sensitif seperti kata sandi atau data keuangan dengan menyamar sebagai entitas yang tepercaya melalui email atau situs web palsu.

Serangan Zero-day: Serangan yang mengeksplorasi kerentanan yang belum diketahui atau belum diperbaiki oleh pihak yang bertanggung jawab.

Serangan Spoofing: Serangan di mana penyerang menyamar sebagai entitas yang sah, seperti alamat IP palsu atau identitas email palsu, untuk memperoleh akses yang tidak sah atau memanipulasi data.

Serangan SQL Injection: Serangan di mana penyerang menyisipkan kode SQL berbahaya ke dalam input yang tidak divalidasi dalam aplikasi web, dengan tujuan untuk mendapatkan akses ke database atau melakukan manipulasi data.

Serangan Cross-Site Scripting (XSS): Serangan di mana penyerang menyisipkan skrip berbahaya ke dalam situs web yang dilihat oleh pengguna lain, memungkinkan penyerang untuk mencuri informasi pengguna atau mengontrol sesi pengguna.

Serangan Password Cracking: Serangan di mana penyerang mencoba memecahkan

atau menebak kata sandi dengan menggunakan metode seperti kamus serangan (dictionary attack) atau serangan brute force.

**Serangan DNS Spoofing:** Serangan di mana penyerang mengarahkan lalu lintas jaringan ke server DNS palsu dengan tujuan meretas komunikasi atau melakukan serangan phishing.

**Serangan Social Engineering:** Serangan yang melibatkan manipulasi psikologis pada individu untuk mendapatkan informasi rahasia atau menginduksi tindakan yang merugikan.

**Serangan Pharming:** Serangan di mana penyerang mengalihkan lalu lintas jaringan ke situs web palsu tanpa pengetahuan pengguna, dengan tujuan untuk mencuri informasi pribadi atau keuangan.

**Serangan Malware:** Serangan yang melibatkan penggunaan perangkat lunak berbahaya untuk menginfeksi sistem atau perangkat, termasuk virus, worm, Trojan, dan spyware.

**Serangan Trojan:** Serangan di mana penyerang menyembunyikan perangkat lunak berbahaya dalam aplikasi yang tampak sah atau berguna, dengan tujuan merusak sistem atau mencuri data.

**Serangan Worm:** Serangan berbasis jaringan yang menyebar secara otomatis ke sistem-sistem lain melalui jaringan, sering kali merusak kinerja jaringan dan merugikan sistem.

**Serangan Spyware:** Serangan yang menginstal perangkat lunak berbahaya pada sistem pengguna untuk memantau aktivitas dan mencuri informasi pribadi.

**Serangan Botnet:** Serangan di mana penyerang mengendalikan jaringan komputer yang terinfeksi (botnet) untuk melancarkan serangan terhadap target tertentu.

**Serangan Hacking:** Upaya yang tidak sah untuk mendapatkan akses tidak sah ke sistem atau perangkat untuk tujuan merusak, mencuri data, atau melakukan tindakan yang merugikan.

**Serangan Backdoor:** Serangan di mana penyerang menciptakan pintu belakang yang tidak terdeteksi ke dalam sistem atau aplikasi untuk memperoleh akses yang tidak sah di masa depan.

**Serangan Denial of Service (DoS):** Serangan yang bertujuan membuat sumber daya

sistem atau jaringan menjadi tidak tersedia untuk pengguna yang sah dengan mengirimkan lalu lintas yang berlebihan atau memanfaatkan kerentanan sistem.

**Network Access Control (NAC):** Teknologi yang digunakan untuk mengontrol akses ke jaringan berdasarkan kebijakan keamanan yang ditetapkan, termasuk verifikasi identitas, pemeriksaan status keamanan, dan pengaturan izin akses.

**Security Information and Event Management (SIEM):** Platform yang mengumpulkan, mengintegrasikan, dan menganalisis data keamanan dari berbagai sumber untuk mendeteksi dan merespons ancaman keamanan.

**Vulnerability Assessment:** Proses sistematis untuk mengidentifikasi, mengklasifikasikan, dan menganalisis kerentanan dalam infrastruktur jaringan dengan tujuan memperbaiki kelemahan tersebut sebelum dieksloitasi oleh penyerang.

**Network Segmentation:** Praktik membagi jaringan menjadi segmen-semen terpisah secara logis atau fisik untuk mengisolasi sumber daya penting dan mengurangi dampak potensial dari serangan.

**Network Traffic Monitoring:** Proses memantau dan menganalisis lalu lintas jaringan untuk mendeteksi aktivitas mencurigakan, serangan, atau pelanggaran kebijakan keamanan.

**Security Information Sharing:** Praktik berbagi informasi dan intelijen keamanan antara organisasi, lembaga pemerintah, dan penyedia layanan keamanan untuk meningkatkan pemahaman dan respons terhadap ancaman keamanan.

**Data Loss Prevention (DLP):** Strategi dan teknologi yang dirancang untuk mencegah kebocoran atau kehilangan data sensitif dari jaringan atau sistem dengan mengidentifikasi, mengawasi, dan mengendalikan aliran data.

**Network Hardening:** Proses mengamankan jaringan dengan menerapkan kebijakan, konfigurasi, dan langkah-langkah keamanan yang tepat, seperti memperbarui perangkat lunak, memblokir port yang tidak digunakan, dan menerapkan filter lalu lintas.

**Secure Socket Layer/Transport Layer Security (SSL/TLS):** Protokol keamanan yang

digunakan untuk mengenkripsi komunikasi antara klien dan server melalui internet, memberikan keamanan dalam transfer data.

**Network Behavior Analysis (NBA):** Teknik analisis yang menggunakan algoritma dan pola perilaku untuk mengidentifikasi anomali dalam lalu lintas jaringan, membantu dalam deteksi serangan baru dan tidak diketahui.

**Security Operations Center (SOC):** Pusat operasi yang mengumpulkan, menganalisis, dan merespons kejadian keamanan dalam waktu nyata, memonitor dan melindungi infrastruktur jaringan dari serangan keamanan.

**Web Application Firewall (WAF):** Firewall khusus yang melindungi aplikasi web dari serangan dengan memantau, memfilter, dan memblokir lalu lintas yang mencurigakan atau berbahaya.

**Network Authentication Protocol:** Protokol yang digunakan untuk mengotentikasi dan mengamankan akses ke jaringan, seperti Extensible Authentication Protocol (EAP) atau Remote Authentication Dial-In User Service (RADIUS).

**Security Policy:** Kumpulan aturan, pedoman, dan prosedur yang mengatur dan memandu pengelolaan keamanan jaringan, termasuk penggunaan kata sandi, akses jaringan, dan kebijakan keamanan umum.

**Network Forensics:** Proses pengumpulan, analisis, dan interpretasi bukti digital yang berkaitan dengan serangan keamanan jaringan untuk tujuan penyelidikan dan penegakan hukum.

**Two-Factor Authentication (2FA):** Metode otentikasi yang memerlukan dua faktor, seperti kombinasi kata sandi dan kode unik yang dikirim melalui perangkat seluler, untuk memberikan lapisan keamanan tambahan.

**Network Isolation:** Praktik memisahkan jaringan atau segmen jaringan yang sensitif dari jaringan umum atau tidak terpercaya untuk meminimalkan risiko dari serangan internal dan pergerakan lateral.

**Security Audit:** Pemeriksaan dan evaluasi sistem keamanan jaringan untuk mengevaluasi kepatuhan terhadap kebijakan keamanan, mengidentifikasi kerentanan, dan merekomendasikan perbaikan yang diperlukan.

**Network Access Control List (ACL):** Daftar aturan yang diterapkan pada router atau firewall untuk mengatur dan mengontrol lalu lintas jaringan berdasarkan alamat IP, protokol, atau port tujuan.

**50. Security Token:** Perangkat fisik atau aplikasi seluler yang menghasilkan kode atau kunci unik yang digunakan sebagai metode otentifikasi tambahan untuk mengamankan akses jaringan atau transaksi.