MODUL PERKULIAHAN:
KEAMANAN SIBER

Penyusun 1	Penyusun 2	Penyusun 3
Denpasar, <*Arial, 9pt>	Denpasar, <*Arial, 9pt>	Denpasar,
(Nama Dosen dan gelar) <*Arial, 9pt>	(Nama Dosen dan gelar) <*Arial, 9pt>	Nama Dosen dan gelar) <*Arial, 9pt>

INFORMASI MATA KULIAH

Jumlah SKS	**4**
Jenis Matakuliah	Teori
Kegiatan Pembelajaran	Daring
Persyaratan Sarana Peserta/Spesifikasi/ Tools/Media ajar yang akan digunakan	

CAPAIAN DAN DESKRIPSI MK

Capaian Pembelajaran Mata Kuliah (CPMK)	Deskripsi Singkat MK
• CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi. • CPMK-07-4: Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.	Keamanan siber adalah matakuliah yang mempelajari tentang konsep dan teknik untuk pengamanan aplikasi, sistem dan jaringan komputer serta data digital dari kejahatan cyber yang dapat menggangu proses bisnis dan mengakibatkan kerugian.

REFERENSI

Referensi
[1] Sadikin, R. (2012). Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam bahasa java. Yogyakarta: Andi
[2] Weidman, G. (2014). Penetration Testing A Hands-On Introduction to Hacking.
[3] Situmeang, M.S (2020). Cyber Law, Bandung: Cakra 2020

Firewall & IDS

Capaian Pembelajaran Mata Kuliah
• CPMK-06-17: Mampu menjelaskan dan menguasai teknik pengamanan sistem dan jaringan komputer untuk mengidentifikasi dan mencegah serangan cyber dengan mengimplementasikan aspek-aspek keamanan informasi. • CPMK-07-4: Mampu menjelaskan dan menguasai konsep dasar teori jaringan mahasiswa mampu memahami konsep jaringan komputer, mengetahui perangkat-perangkat jaringan, protokol jaringan, OSI dan TCP/IP model, konsep IP Address dan kelas-kelas dalam IP Address, Routing dengan media virtual seperti menggunakan packet tracer, memahami jaringan nirkabel, mengetahui serangan dalam jaringan dan mengetahui firewall.

Indikator Penilaian
1.1 Pengertian firewall dan IDS 1.2 Jenis-jenis firewall dan IDS 1.3 Menerapkan IDS dengan snort 1.4 Menurtup servis dengan firewall 1.5 Mekanisme pertahanan DDoS 1.6 Advanced Policy Firewall (APF)

Modul Ajar: Firewall dan Intrusion Detection System (IDS)

1. Tujuan Pembelajaran

- Memahami konsep dasar Firewall dan IDS.
- Mampu menjelaskan jenis-jenis firewall dan IDS beserta fungsinya.
- Mampu melakukan konfigurasi dasar firewall pada sistem operasi dan perangkat keras.
- Mengidentifikasi dan menganalisis log dari IDS untuk mendeteksi potensi serangan.

2. Definisi Firewall dan IDS

Firewall adalah sistem keamanan jaringan yang memantau dan mengontrol lalu lintas masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan. Firewall bertindak sebagai penghalang antara jaringan internal yang aman dan jaringan eksternal (seperti internet). Sedangkan **Intrusion Detection System (IDS)** adalah perangkat atau perangkat lunak yang memantau aktivitas jaringan atau sistem untuk mendeteksi tanda-tanda pelanggaran keamanan atau ancaman. IDS dapat digunakan sebagai langkah awal dalam mendeteksi serangan.

3. A. Firewall

Firewall berfungsi untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi. Firewall bisa berbentuk perangkat keras, perangkat lunak, atau kombinasi keduanya.

Jenis-Jenis Firewall:

- **Packet Filtering Firewall**
  Memeriksa paket data berdasarkan aturan-aturan dasar seperti alamat IP, port, dan protokol.
- **Stateful Inspection Firewall**
  Memeriksa koneksi dan status paket dalam jaringan.
- **Application Layer Firewall**
  Menyaring lalu lintas pada lapisan aplikasi, seperti HTTP atau FTP.
- **Proxy Firewall**
  Bertindak sebagai perantara dan melakukan inspeksi mendalam pada paket data.

Keuntungan dengan menggunakan Firewall adalah dapat membantu mencegah akses tidak sah tetapi mungkin tidak efektif untuk ancaman dari dalam jaringan atau serangan yang canggih.

B. Intrusion Detection System (IDS)

IDS memonitor jaringan untuk mendeteksi aktivitas mencurigakan atau ancaman keamanan yang bisa berbahaya bagi sistem.

Jenis-Jenis IDS antara lain :

1. **Network-based IDS (NIDS)**
   Mendeteksi ancaman di seluruh jaringan.
2. **Host-based IDS (HIDS)**
   Mendeteksi ancaman pada perangkat individu atau host.

Didalam teknik deteksi dengan menggunakan Pendekatan Deteksi yaitu :

1. **Signature-based Detection**
   Mendeteksi ancaman berdasarkan pola yang telah diketahui.
2. **Anomaly-based Detection**
   Mendeteksi ancaman berdasarkan pola lalu lintas yang tidak biasa.

Keuntungan : IDS dapat memberikan peringatan dini, namun sering menghasilkan *false positive* atau membutuhkan konfigurasi yang tepat untuk meminimalkan alarm palsu.

4. Praktik Implementasi

A. Konfigurasi Firewall

Menggunakan UFW (Uncomplicated Firewall) di Linux

1. Update Repositori Paket

Update OS linux :

```
sudo apt update
```

2. Instal UFW

UFW biasanya sudah tersedia di sebagian besar distribusi Linux modern. Untuk menginstalnya, jalankan perintah:

```
sudo apt install ufw
```

3. Cek Status UFW

Untuk memeriksa apakah UFW sudah terpasang dan statusnya, gunakan:

```
sudo ufw status
```

4. Mengatur Aturan Dasar

Sebelum mengaktifkan UFW, tentukan aturan yang diizinkan. Misalnya, untuk mengizinkan SSH (port 22) agar tetap bisa terhubung ke server:

```
sudo ufw allow ssh
```

Untuk layanan lainnya, misalnya HTTP (port 80) dan HTTPS (port 443), tambahkan aturan seperti berikut:

```
sudo ufw allow http
sudo ufw allow https
```

5. Setelah aturan dibuat, aktifkan UFW dengan perintah:

```
sudo ufw enable
```

6. Verifikasi Aturan dan Status UFW

Untuk memastikan aturan telah diterapkan, periksa kembali status UFW:

```
sudo ufw status verbose
```

Konfigurasi Iptables di Linux

1. Cek Status Iptables

Sebelum memulai konfigurasi, pastikan iptables telah terinstal dan berjalan di sistem operasi. Gunakan perintah berikut untuk memeriksa status iptables:

```
sudo iptables -L
```

2. Menambahkan Aturan Dasar

Memblokir Semua Lalu Lintas Masuk (default):

```
sudo iptables -P INPUT DROP
```

Mengizinkan Lalu Lintas yang Diperbolehkan:

Agar akses SSH (port 22) diizinkan, misalnya:

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

Agar akses HTTP (port 80) dan HTTPS (port 443) diizinkan:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

3. Menyaring Lalu Lintas Berdasarkan IP

Untuk membatasi akses hanya dari alamat IP tertentu, gunakan aturan seperti:

```
sudo iptables -A INPUT -p tcp -s 192.168.1.100 --dport 22 -j ACCEPT
```

4. Menghapus Aturan
Untuk menghapus aturan tertentu, bisa menggunakan perintah:
```
sudo iptables -D INPUT -p tcp --dport 22 -j ACCEPT
```

6. Menambahkan Aturan untuk Koneksi yang Diperbolehkan
Untuk mengizinkan lalu lintas keluar dari jaringan ke Internet, perlu memastikan aturan keluar (OUT) juga diterapkan:
```
sudo iptables -A OUTPUT -p tcp --sport 1024:65535 -d 0.0.0.0/0 -j ACCEPT
```

7. Cek dan Verifikasi Aturan
Setelah menambahkan atau mengubah aturan, verifikasi aturan yang diterapkan dengan perintah:
```
sudo iptables -L -v
```

8. Reset Iptables ke Default
Jika ingin menghapus semua aturan dan mengembalikan iptables ke pengaturan default (yang memblokir semua lalu lintas)
```
sudo iptables -F
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Contoh Aturan Firewall Iptables

- **Izinkan Semua Lalu Lintas Masuk dari IP Tertentu:**
  `sudo iptables -A INPUT -s 192.168.1.100 -j ACCEPT`
- **Blokir Semua Akses ke Port 25 (SMTP)**:
  `sudo iptables -A INPUT -p tcp --dport 25 -j REJECT`
- **Izinkan Akses dari Semua IP ke Port 80 (HTTP)**
  `sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

B. Konfigurasi IDS
Menggunakan Snort sebagai IDS:
1. Update Repositori Paket
Sebelum menginstal Snort, pastikan sistem memiliki repositori paket terbaru. Jalankan perintah:
```
sudo apt update
```
2. Instalasi Snort
Untuk menginstal Snort di sistem Linux (misalnya Ubuntu/Debian), jalankan perintah berikut:
```
sudo apt install snort
```
3. Konfigurasi Snort
Setelah instalasi selesai, perlu mengonfigurasi Snort sesuai dengan kebutuhan sistem.
Mengecek Instalasi
Verifikasi bahwa Snort terinstal dengan menjalankan perintah:
```
snort -V
```
Mengonfigurasi File Konfigurasi Snort

File konfigurasi utama untuk Snort terletak di `/etc/snort/snort.conf`.kita dapat membuka file ini untuk menyesuaikan pengaturan, seperti alamat jaringan, aturan yang diterapkan, dan jenis deteksi yang digunakan.

```
sudo nano /etc/snort/snort.conf
```

Pilih dan Sesuaikan Jaringan Lokal

Di dalam file konfigurasi, tentukan jaringan yang digunakan dengan mengatur variabel `ipvar HOME_NET:`

```
ipvar HOME_NET [192.168.0.0/24]
```

Menentukan File Aturan

Pastikan aturan yang sesuai sudah diaktifkan di dalam file `snort.conf`. juga bisa menambahkan atau mengonfigurasi file aturan tambahan sesuai kebutuhan.

4. Menambahkan Aturan Snort

Snort menggunakan aturan untuk mendeteksi dan memberi peringatan tentang ancaman keamanan. Secara default, aturan Snort disertakan dengan paket, tetapi dapat menambahkan atau memperbarui aturan dengan mengunduh dari situs web Snort atau repositori aturan lainnya.

Untuk memperbarui aturan:

```
sudo apt install snort-rules-default
```

5. Menjalankan Snort

Setelah konfigurasi selesai, dapat menjalankan Snort sebagai IDS untuk menganalisis lalu lintas jaringan. Untuk menjalankan Snort dalam mode deteksi:

```
sudo snort -A console -c /etc/snort/snort.conf -i eth0
```

- `-A console` : Menampilkan log di konsol.
- `-c /etc/snort/snort.conf` : Menggunakan file konfigurasi Snort yang telah diubah.
- `-i eth0` : Menentukan antarmuka jaringan (gantilah dengan antarmuka yang sesuai pada sistem, seperti eth0, wlan0, atau ens33)

6. Verifikasi dan Memeriksa Log

Untuk melihat log deteksi, periksa file log yang dihasilkan oleh Snort:

```
sudo tail -f /var/log/snort/alert
```

7. Konfigurasi Snort untuk Startup

Jika ingin menjalankan Snort secara otomatis saat sistem boot, dapat mengonfigurasi Snort untuk diaktifkan dengan menggunakan systemd atau sebagai layanan:

Buat file unit systemd untuk Snort:

```
sudo nano /etc/systemd/system/snort.service
Isi file dengan:
[Unit]
Description=Snort IDS
After=network.target

[Service]
```

```
ExecStart=/usr/sbin/snort -A console -c /etc/snort/snort.conf -i
eth0
Restart=on-failure
User=root

[Install]
WantedBy=multi-user.target
```

Aktifkan layanan Snort:

```
sudo systemctl enable snort
sudo systemctl start snort
```

8. Pengujian dan Pemeliharaan

Pastikan untuk menguji konfigurasi Snort secara menyeluruh dengan menghasilkan lalu lintas jaringan yang sesuai, misalnya menggunakan alat seperti nmap untuk melakukan pemindaian port dan melihat bagaimana Snort merespons.

5. Penugasan dan Evaluasi

Tugas Praktik lakukan Konfigurasi firewall dasar menggunakan UFW atau iptables pada sistem operasi Linux.