

**MODUL PRAKTIKUM**

# **KEAMANAN INFORMASI**

**DISAMPAIKAN PADA  
SEMESTER GENAP  
TAHUN AKADEMIK 2023/2024**

**DEPARTEMEN TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BRAWIJAYA  
MALANG**

## **TIM PENYUSUN**

1. ADHITYA BHAWIYUGA, S.KOM, M.SC.
2. ARI KUSYANTI, S.T., M.SC.
3. DANY PRAMANITA KARTIKASARI, S.T., M.KOM.
4. FARIZ ANDRI BAKHTIAR, S.T., M.KOM.
5. M. ALI FAUZI, S.KOM., M.KOM., PH.D.

# BAB 4

## AUDIT DAN MONITORING

### 4.1. DASAR TEORI

Intrusion Detection System (IDS) adalah alat atau perangkat lunak yang memonitor aktivitas jaringan ataupun sistem untuk melihat aktivitas berbahaya maupun pelanggaran kebijakan dan melaporkannya ke bagian manajemen. Beberapa sistem dapat melakukan penghentian intrusi tetapi hal ini terkadang tidak diinginkan ataupun dibutuhkan oleh sistem monitoring itu sendiri. Fokus utama IDS adalah identifikasi kemungkinan insiden, logging informasi terkait insiden, dan melaporkan kejadian tersebut. Beberapa organisasi/korporasi menggunakan IDS untuk tujuan lain seperti identifikasi masalah dalam kebijakan keamanan, dokumentasi ancaman yang ada, dan menghalangi individu tertentu yang bermaksud melanggar kebijakan keamanan yang telah dibangun. IDS menjadi hal yang fitur penting dalam keamanan infrastruktur di setiap organisasi/korporasi.

IDS biasanya merekam informasi terkait kegiatan yang diawasi, melaporkan administrator keamanan mengenai hal tersebut, dan membuat laporan. Banyak IDS yang juga merespon ancaman dengan melakukan pencegahan, menjadi Intrusion Detection and Prevention System (IDPS). Hal ini termasuk re-konfigurasi firewall oleh IDPS, menghentikan serangan dengan kemampuan IDPS sendiri, ataupun mengubah konten yang digunakan untuk menyerang.

Secara garis besar, IDS dibagi menjadi dua yaitu Network Intrusion Detection System (NIDS) yang berfokus pada deteksi serangan pada jaringan dan Host Intrusion Detection System (HIDS) yang lebih berfokus pada sistem host. NIDS mendeteksi akses trafik, sensor diletakkan pada DMZ ataupun batas batas jaringan. Contoh NIDS adalah snort. HIDS biasanya digunakan untuk mendeteksi modifikasi file system, mencatat log aplikasi, dan kegiatan lain yang dilaksanakan di tingkat host. Contoh dari HIDS adalah Tripwire dan OSSEC.

## 4.2. TUJUAN PERCOBAAN

1. Mahasiswa mampu memahami apa yang dimaksud dengan IDS dan IPS
2. Mahasiswa mampu melakukan konfigurasi IDPS sederhana

## 4.3. ALAT DAN BAHAN

Dalam rangka melaksanakan langkah-langkah praktikum yang terdapat pada bab ini, peserta praktikum perlu menyiapkan beberapa perangkat berikut:

- Perangkat komputer Desktop/Laptop dengan kapasitas RAM minimum 8 GB
- Perangkat lunak virtualisasi (Oracle VM VirtualBox/VMWare Workstation)
- Koneksi internet
- Beberapa tools yang dibutuhkan dalam praktikum

## 4.4. PROSEDUR PERCOBAAN

### Instalasi Persiapan Lingkungan Praktikum

Berikut langkah-langkah yang perlu dilakukan dalam mempersiapkan kebutuhan praktikum:

- **Kali Linux**

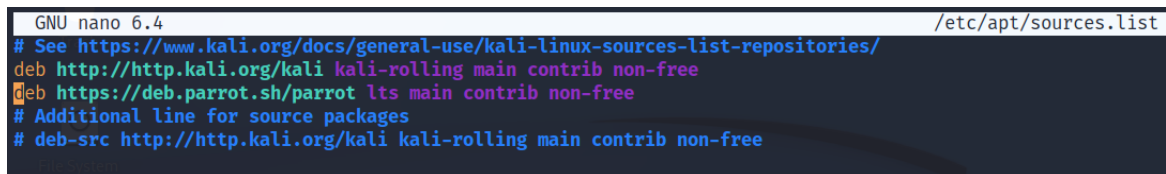
1. Jalankan command berikut pada terminal untuk masuk ke dalam daftar repository:

**sudo nano /etc/apt/sources.list**

2. Kemudian tambahkan repository parrot ke dalam daftar sumber tersebut:

**deb https://deb.parrot.sh/parrot lts main contrib non-free**

Sehingga, akan menjadi seperti berikut:



```
GNU nano 6.4 /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free
deb https://deb.parrot.sh/parrot lts main contrib non-free
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

3. Kemudian simpan dengan ctrl+x -> y -> Enter

4. Pada terminal masukkan keyring agar dapat mengakses repository dengan perintah:

**sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 823BF07CEB5C469B**

5. Berikutnya, lakukan update repository dengan perintah:

**sudo apt update**

6. Untuk langkah terakhir, lakukan instalasi tools snort dengan perintah:

**sudo apt install snort**

- **Ubuntu**

1. Lakukan instalasi tools snort dengan perintah:

**sudo apt install snort**

## Praktik Penggunaan Snort

Berikut merupakan langkah-langkah yang perlu dilakukan dalam menyelesaikan praktikum:

1. Bukalah file pada `/etc/snort/snort.conf` dengan text editor favoritmu dan perhatikan konfigurasi tersebut serta jelaskan bagian rule dan network:

*Screenshot snort.conf dan penjelasan bagian rule dan network*

2. Kembali ke terminal dan jalankan command berikut untuk sniffing menggunakan snort:  
**sudo snort -v -d -e -i <network card yang ingin di cek>**

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

*Penjelasan dari flag/param -v -d -e dan -i , screenshot dari tiap keluaran tiap flag/param. Serta penjelasan singkat mengenai screenshot tersebut.*

3. Hentikan snort dan jalankan command snort dibawah ini untuk mode packet logger:  
**sudo snort -dev -l ./log -b -i <network card yang ingin dicek>**

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address

4. Jalankan command berikut untuk menjalankan snort dengan IDS mode:

```
ubuntu@ubuntu-VirtualBox:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s8
10/16-17:24:17.903023  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68
-> 255.255.255.255:67
10/16-17:25:15.460358  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168
.56.1:35196 -> 192.168.56.10:705
10/16-17:25:15.463030  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.56.1:4
7476 -> 192.168.56.10:161
□
```

**sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i  
<network yang ingin dicek>**

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

*Penjelasan dari flag/param -A -q -u -g -c dan -i serta screenshots dan penjelasan dari outputnya*

## 4.5. KESIMPULAN

Pada bagian ini, tuliskan kesimpulan apa saja yang didapat dari hasil melaksanakan kegiatan-kegiatan pada bab ini.

## 4.6. EVALUASI

1. Apa perbedaan dan batasan-batasan antara IDS, IPS, dan Firewall?

2. Buatlah konfigurasi Snort IPS menggunakan DAQ AFPacket. Salah satu contoh konfigurasi snort IPS bisa dilihat di dokumentasi resmi berikut:

<https://snort.org/documents/snort-ips-using-daq-afpacket>