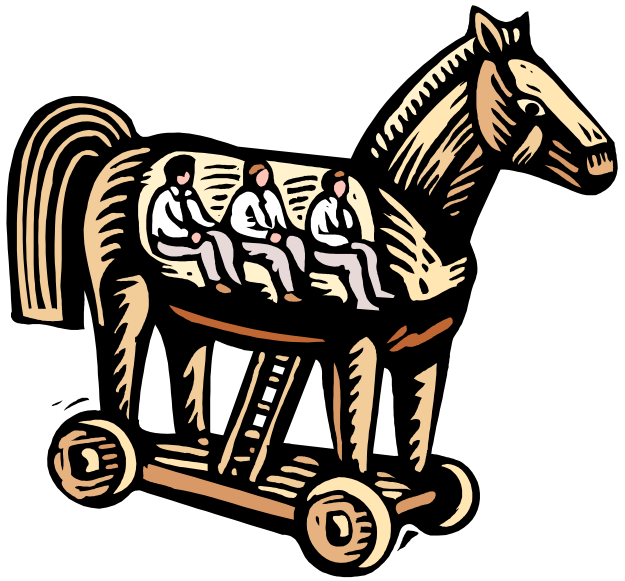
Intrusion Detection System (IDS)

Budi Rahardjo

2023

Apa itu IDS?

- Sistem untuk mendeteksi adanya "*intrusion*" yang dilakukan oleh "*intruder*"
- Mirip seperti alarm/camera
- Kejadian (intrusion) sudah terjadi
- Bekerjasama dengan (komplemen dari) firewall untuk mengatasi intrusion



Apa itu “intrusion”?

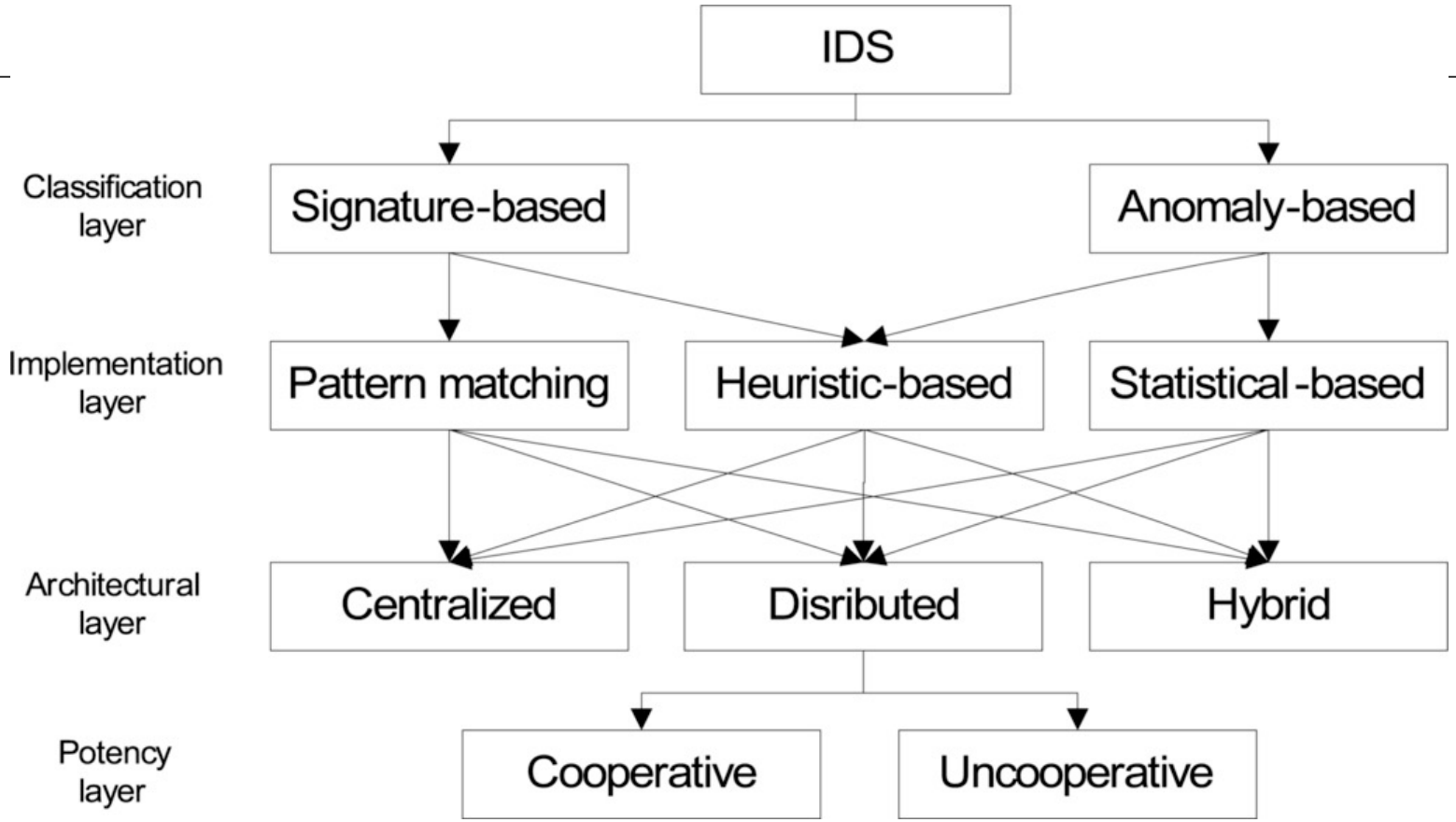
- Didefinisikan sebagai kegiatan yang bersifat *anomaly*, *incorrect*, *inappropriate* yang terjadi di jaringan atau di host
- Apa yang didefinisikan sebagai intrusion kemudian dikodekan menjadi “rules” dalam IDS
  Contoh rules:
  - Mendeteksi port scanning
  - Akses ke situs terlarang

Jenis IDS

- **Network**-based
  memantau anomali di **jaringan**,
  misal melihat adanya network scanning
  Contoh: snort, suricata, tcpblock
- **Host**-based
  memantau anomali di **host**,
  misal memonitor logfile, process, file owenership, mode
  Contoh: portsentry

Anomali

- *Traffic* / aktivitas yang tidak sesuai dgn policy:
  - akses dari/ke host yang terlarang
  - memiliki content terlarang (virus)
  - menjalankan program terlarang
    (web directory traversal:
    `GET ../..;`
    `cmd.exe`)
    - ...



http://www.mdpi.com/1424-8220/9/8/5989

IDS yang populer

- snort (open source)
  http://www.snort.org
- Sourcefire (versi komersial)
  http://www.sourcefire.com
- Suricata (open source)
  http://suricata-ids.org
- Tripwire, swatch, dll.
- OSSEC – host-based IDS (open source)
  http://www.ossec.net/
- BRO
  http://www.bro.org

snort

SNORT

- Open source IDS
  host-based
  network-based
  packet sniffer
  implementasi di UNIX & Windows
- Beroperasi berdasarkan “rules”
- Informasi lebih lengkap
  http://www.snort.org

INDOCISC

Snort Rules

- Terbagi menjadi dua (2) bagian:
  - Rule header
  - Rule option
- Contoh snort rules

```
alert tcp any any -> 202.138.228.0/24 111 (content:"|00 01 86
a5|";\ msg: "mountd access";)
```

Tulisan yang diberi garis bawah adalah “rule header”, sedangkan selebihnya adalah “rule option”

Menangkap sesi FTP

- Buat rule snort di dalam berkas "`ftp.conf`", dengan isi:

```
log tcp any any -> 192.168.1.0/24 21
```

- Perhatikan: rule header saja
- Buat direktori bernama "`coba`", kemudian jalankan perintah berikut:

```
unix# snort -d -l coba -c ftp.conf
```

Lanjutan sesi FTP

- Jalankan sesi FTP yang menuju ke sebuah host di jaringan 192.168.1.0

```
unix$ ftp 192.168.1.101
Connected to 192.168.1.101.
220 FTP server ready.
Name: anonymous
331 Guest login ok, send your complete e-mail address as
  password.
Password: guest@hotmail.com
ftp> quit
```

Lanjutan …

- Hentikan sesi snort dengan ^c (ctrl c), kemudian pindah ke direktori “coba”
- Perhatikan bahwa ada direktori yang namanya merupakan nomor IP dari komputer yang menyerang (dalam hal ini yang melakukan FTP); misalnya 192.168.1.5
- Pindah ke direktori ini. Akan ditemukan sebuah berkas yang namanya kira-kira sebagai berikut:

  ```
  TCP:35724-21
  ```

- Kemudian amatilah isi berkas ini.

Mengamati sesi TELNET

- Buat rule snort di dalam berkas telnet.conf, dengan isi:

```
var HOME_NET [192.168.1.0/24]
log tcp any any <> $HOME_NET 23 (session: printable;)
```

[Baris kedua ini harus ditulis dalam satu baris panjang. Perhatikan sudah ada rule option]

- Kemudian jalankan perintah berikut:

```
snort -d -l coba -c telnet.conf
```

Sesi TELNET [lanjutan]

- Jalankan sesi telnet yang menuju ke sebuah host di jaringan 192.168.1.0

```
unix$ telnet 192.168.1.101
Trying 192.168.1.101...
Connected to 192.168.1.101.
Escape character is '^]'.
Debian GNU/Linux 3.0 hurd
hurd login: user01
Password: user01
Unix% ls
Unix% exit
```

Sesi TELNET [lanjutan]

- Tahap selanjutnya sama seperti pada bagian Pengamatan Sesi FTP.
- Berkas yang dihasilkan oleh program snort kira-kira bernama

  `SESSION:35733-23`
- Amatilah berkas ini. Anda akan dapatkan isi sesi telnet anda

Rules yang lebih kompleks

- Rules yang lebih kompleks dapat dilihat pada distribusi snort di direktori /etc/snort
  - Mendeteksi virus
  - Mendeteksi akses daerah (file) terlarang di web server
  - Paket yang memiliki isi aneh
  - Paket yang memiliki sifat aneh (flag tidak lazim)
  - Adanya portscanning
  - dan lain-lain

Contoh log snort


```
The log begins from: Mar 9 09:11:05
The log ends     at: Mar 9 12:22:24
Total events: 161
Signatures recorded: 6
Source IP recorded: 12
Destination IP recorded: 44

 # of attacks  from         to         method
=========================================
   61     202.138.228.73    202.138.228.74   IDS135-CVE-1999-0265-MISC-
ICMPRedirectHost
   31     192.168.1.51      192.168.1.11      ICMP Destination Unreachable {ICMP}
   5      202.110.192.93    202.138.228.74    spp_http_decode: ISS Unicode
```

Tools tambahan snort

- ACID: database alerts, analisa dengan menggunakan web-based
- Demarc: web-based interface
- OSSIM: mengintegrasikan berbagai tools (snort, nmap, dll.)
- Aanval: web-based interface juga

ACID

- Analysis Console for Intrusion Databases
  (ACID)
- Program yang dirancang untuk mengelolah data-data security event seperti; IDS, Firewall, dan Network Monitoring Tools
- Data-data disimpan dalam database (MySQL)

Manfaat ACID

- Log-log yang tadinya susah dibaca menjadi mudah di baca
- Data-data dapat dicari (search) dan difilter sesuai dengan kriteria tertentu
- Managing Large Alert Databases (Deleting and Archiving)
- Untuk kasus-kasus tertentu dapat merujuk alert pada situs database security seperti Securityfocus, CVE, arachNIDS

Tampilan halaman muka ACID

Analysis Console for Intrusion Databases

Added 24 alert(s) to the Alert cache

Queried on : Fri November 15, 2002 16:15:21

Database: snort_log@localhost (**schema version:** 105)

Time window: [2002-07-30 11:57:57] - [2002-11-15 16:15:03]

Sensors: 1
Unique Alerts: 133 (16 categories)
Total Number of Alerts: 629348
Source IP addresses: 9019
Dest. IP addresses: 427
Unique IP links 13996

Source Ports: 4591
TCP (4533) UDP (69)
Dest. Ports: 30065
TCP (30045) UDP (35)

Traffic Profile by ProtocolTCP (13%)

UDP (< 1%)

ICMP (87%)

Portscan Traffic (0%)

Daftar Jenis Attack

ACID Alert Listing

Added 13 alert(s) to the Alert cache

Queried DB on : Fri November 15, 2002 16:32:23

Meta Criteria *any*
IP Criteria *any*
Layer 4 Criteria *none*
Payload Criteria *any*

< Signature > < Classification > < Total > Sensor # < Src. Addr. > < Dest. Addr. > < First > < Last >

- [arachNIDS] MISC Large ICMP Packet bad-unknown 17686 (3%) 1 403 5 2002-07-30 11:57:57 2002-11-15 16:31:4
- ICMP Destination Unreachable misc-activity 75 (0%) 1 5 2 2002-07-30 11:59:08 2002-07-30 13:31:33
- [CVE] DDOS mstream client to handler attempted-dos 1293 (0%) 1 128 2 2002-08-02 14:53:17 2002-11-15 15:00:59
- PORN free XXX kickass-porn 24925 (4%) 1 1996 3 2002-08-02 10:28:40 2002-11-15 16:29:38

Tampilan Individual Attack

ACID Query Results

Meta Criteria	Signature "[CVE] DDOS mstream client to handler"
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

ID < Signature > < Timestamp > < Source Address > < Dest. Address > < Layer 4 Proto >

- #0-(1-19879) [CVE] DDOS mstream client to handler 2002-08-02 14:53:17 202.53.224.41:80 202.152.6.196:12754 TCP
- #1-(1-20267) [CVE] DDOS mstream client to handler 2002-08-02 15:48:59 81.27.33.7:80 202.152.6.197:12754 TCP

...

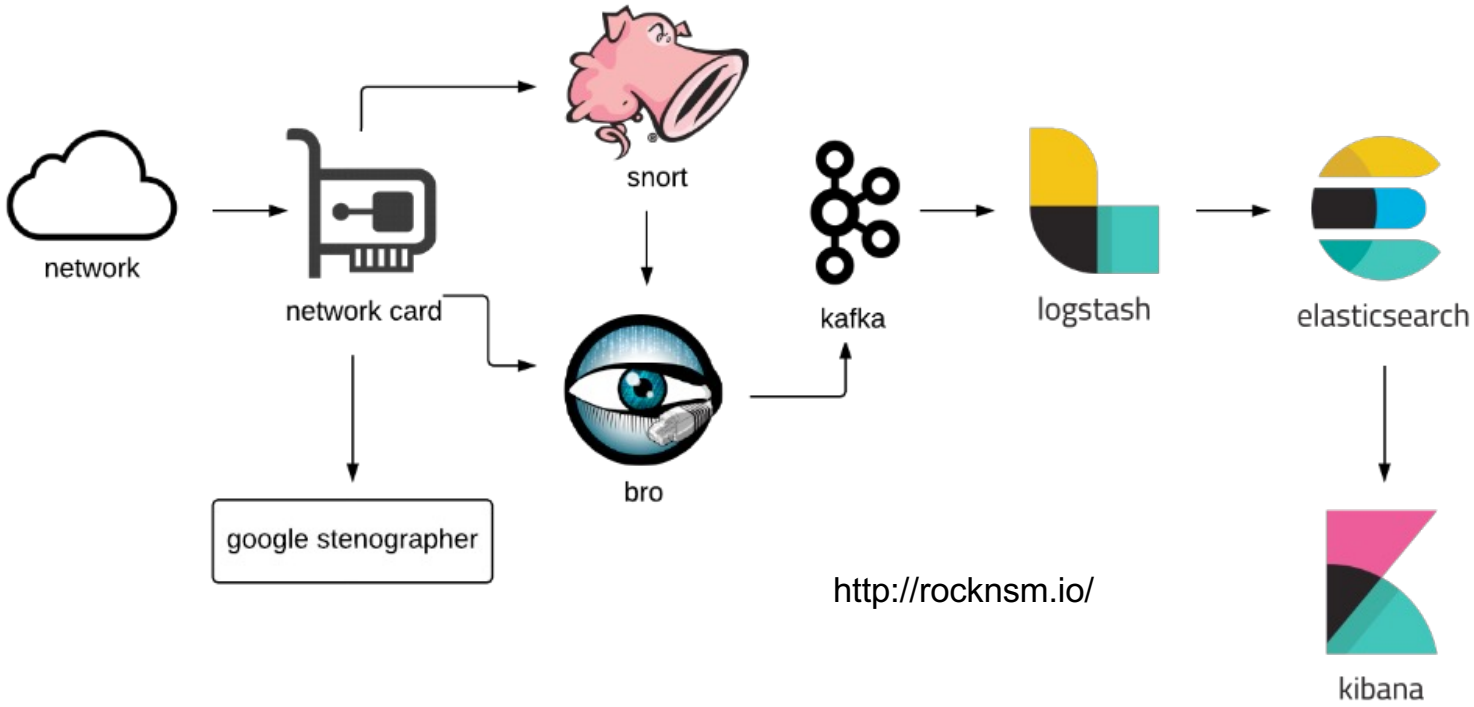
Masalah

- Serangan baru memiliki *signature* yang baru sehingga daftar *signature* harus selalu diupdate
- Network semakin cepat (gigabit) sehingga menyulitkan untuk menganalisa setiap paket. Membutuhkan hardware dengan *spec* yang bagus
- Jumlah host makin banyak: distributed IDS
- Terlalu banyak laporan (false alarm) menggangu admin

RockNSM

(Response Operation Collection Kit)

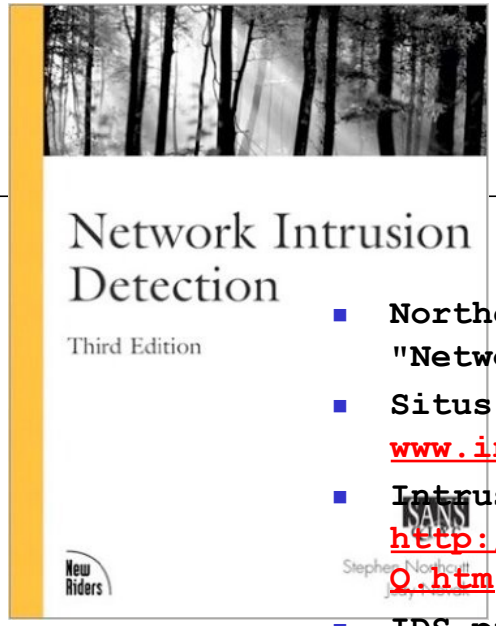
Open source Network Security Monitoring platform



http://rocknsm.io/

Penutup

- IDS merupakan sebuah komponen utama dari pengamanan sebuah jaringan (situs)
- IDS dan Firewall saling komplemen => IPS (Intrusion Prevention System)
- Ada berbagai aplikasi dari IDS untuk monitoring



Bahan Bacaan

- Northcutt, Stephen
  "Network Intrusion Detection", New Riders, 1999
- Situs incidents
  www.incidents.org
- Intrusion detection FAQ
  http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm
- IDS product query
  http://www.nwfusion.com/bg/intrude2/intrude2result.jsp?_tablename=intrude2
- Front-end untuk Snort
  - ACID: http://acidlab.sourceforge.net/
  - OSSIM: http://www.ossim.net
  - Aanval: http://www.aanval.com