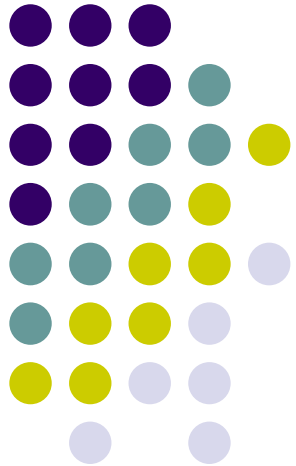
Keamanan Sistem dan Jaringan Komputer



Klafisifikasi Keamanan Sistem Informasi

menurut David Icove

Umumnya orang-orang hanya terfokus pada bagian ini

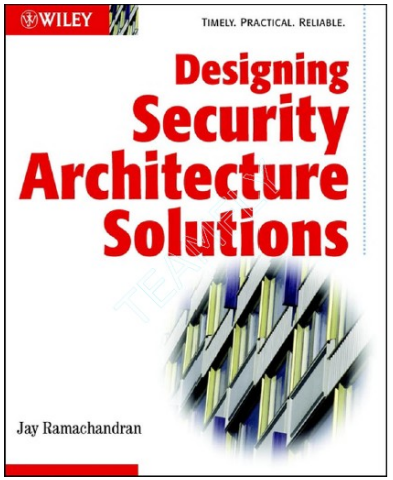
Berdasarkan Elemen System

- Network security
  - difokuskan pada saluran (media) pembawa informasi atau jalur yang dilalui.
- Application security
  - difokuskan pada aplikasinya sistem tersebut, termasuk database dan servicesnya.
- Computer security
  - difokuskan pada keamanan dari komputer pengguna (end system) yang digunakan untuk mengakses aplikasi, termasuk operating system (OS)

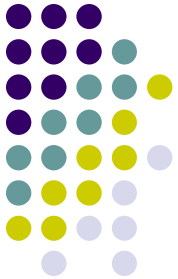
Security Principles

Menurut Jay Ramachandran pada bukunya "Designing Security Architecture Solutions"

- Authentication
- Authorization atau Access Control
- Privacy / confidentiality
- Integrity
- Availability
- Non-repudiation
- Auditing

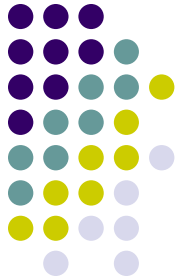


Authentication



- Menyatakan bahwa data atau informasi yang digunakan atau diberikan oleh pengguna adalah asli milik orang tersebut, begitu juga dengan server dan sistem informasi yang diakses.
- Serangan pada jaringan berupa DNS Corruption atau DNS Poison, terminal palsu (spooffing), situs aspal dan palsu, user dan password palsu.
- Countermeasure : Digital Signature misalnya teknologi SSL/TLS untuk web dan mail server.

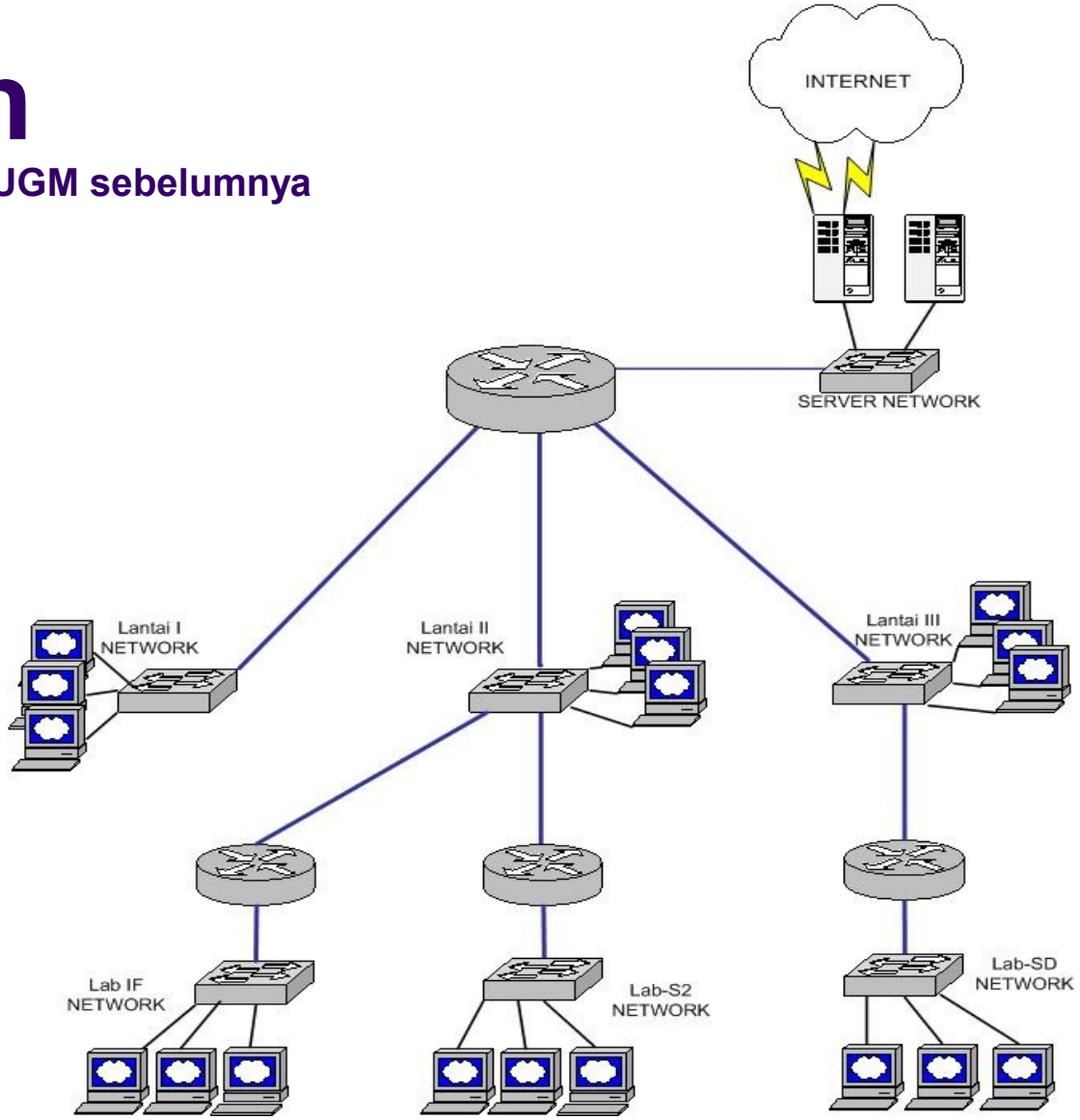
Authorization atau Access Control



- Pengaturan siapa dapat melakukan apa, atau dari mana menuju kemana. Dapat menggunakan mekanisme user/password atau mekanisme lainnya.
- Ada pembagian kelas atau tingkatan.
- Implementasi : pada “ACL” antar jaringan, pada “ACL” proxy server (mis. pembatasan bandwidth/delaypools).

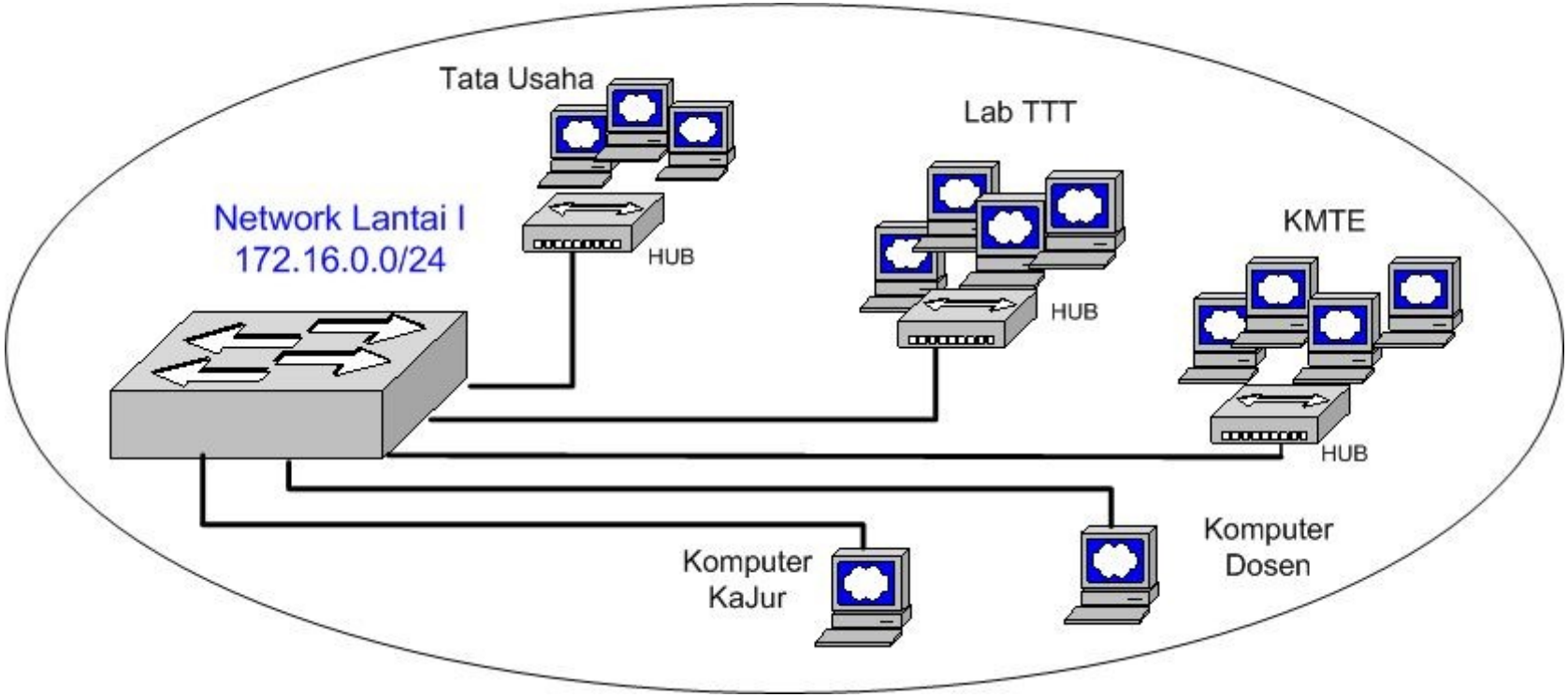
Contoh

Jaringan lokal JTE UGM sebelumnya



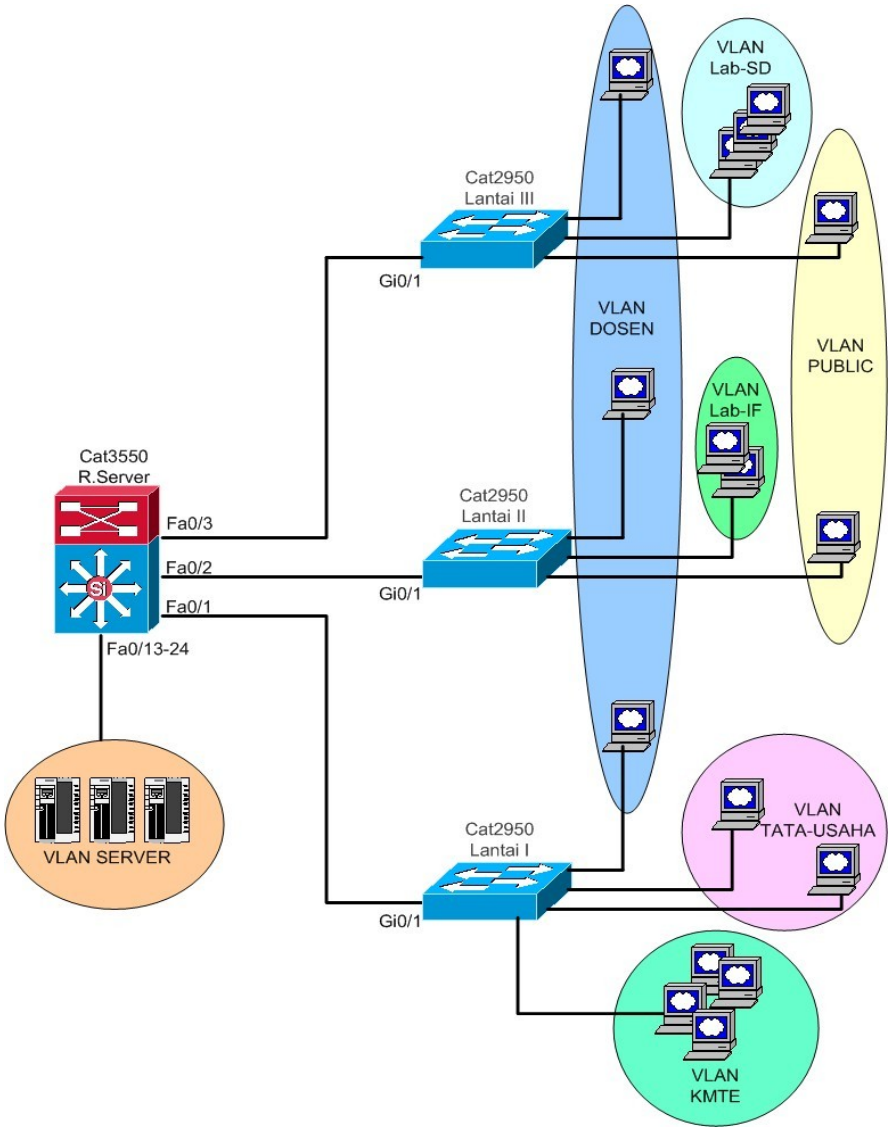
Contoh

Jaringan lantai I JTE UGM sebelumnya



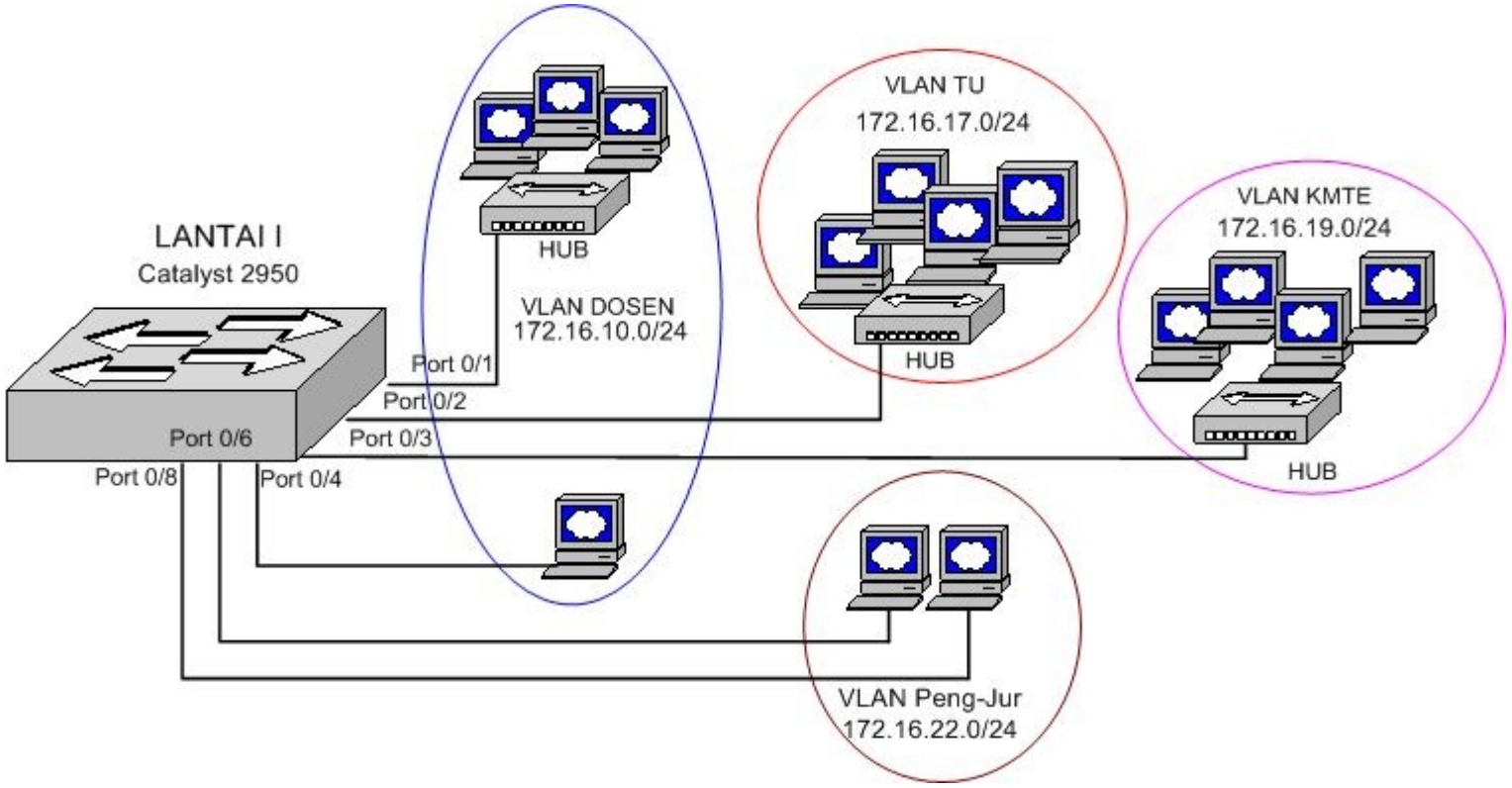
Contoh

Jaringan Lokal JTE UGM saat ini

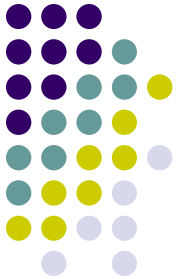


Contoh

VLAN pada switch lantai I JTE UGM

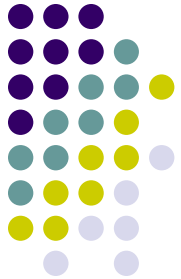


Privacy/confidentiality



- Keamanan terhadap data data pribadi, messages/pesan-pesan atau informasi lainnya yang sensitif.
- Serangan pada jaringan berupa aktifitas sniffing (menyadap) dan adanya keylogger. Umumnya terjadi karena kebijakan/policy yang kurang jelas. Admin atau ISP nakal ??
- Coutermeasure : gunakan teknologi enkripsi/kriptografi.

Integrity



- Bahwa informasi atau pesan dipastikan tidak dirubah atau berubah.
- Serangan pada jaringan dapat berupa aktifitas spoofing, mail modification, trojan horse, MITM Attack.
- Countermeasure : dengan teknologi digital signature dan Kriptografi spt PGP, 802.1x, WEP, WPA

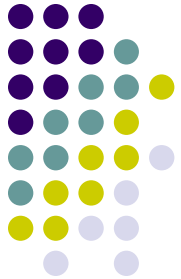
Availability

- Keamanan atas ketersediaan layanan informasi.
- Serangan pada jaringan: DoS (denial of services) baik disadari/sengaja maupun tidak. Aktifitas malware, worm, virus dan bomb mail sering memacetkan jaringan.
- Countermeasure : Firewall dan router filtering, backup dan redundancy, IDS dan IPS

Non-repudiation

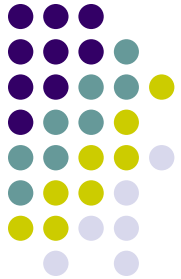
- Menjaga agar jika sudah melakukan transaksi atau aktifitas online, maka tidak dapat di sangkal.
- Umumnya digunakan untuk aktifitas e-commerce. Misalnya email yang digunakan untuk bertransaksi menggunakan digital signature.
- Pada jaringan dapat menggunakan digital signature, sertifikat dan kriptografi.
- Contoh kasus, smtp.ugm.ac.id ?? Setiap pengguna di jaringan lokal UGM dapat menggunakannya tanpa adanya authentikasi.

Auditing



- Adanya berkas semacam rekaman komunikasi data yang terjadi pada jaringan untuk keperluan audit seperti mengidentifikasi serangan serangan pada jaringan atau server.
- Implementasi : pada firewall (IDS/IPS) atau router menggunakan system logging (syslog)

Contoh file Logging dari Cisco Router/Catalyst



[root@spyder cisco]# **tail -f /var/log/cisco/log.cisco**
Feb 28 14:48:51 cat3550 111063: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.113(1027) -> 172.20.2.3(53), 14 packets
Feb 28 14:48:54 cat3550 111064: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted tcp 172.16.19.103(3219) -> 216.200.68.150(21), 1 packet
Feb 28 14:48:58 cat3550 111065: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.80.104(2782) -> 172.20.2.3(53), 1 packet
Feb 28 14:49:07 cat3550 111066: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.114(1036) -> 172.20.2.3(53), 1 packet
Feb 28 14:49:15 cat3550 111067: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.19.158(1025) -> 172.20.2.3(53), 1 packet
Feb 28 14:49:36 cat3550 111068: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.101(1434) -> 172.20.2.3(53), 1 packet
Feb 28 14:49:38 cat3550 111069: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.10.114(1026) -> 172.20.2.3(53), 1 packet
Feb 28 14:49:41 cat3550 111070: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.16.116(1031) -> 172.20.2.3(53), 3 packets
Feb 28 14:49:42 cat3550 111071: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted udp 172.16.13.102(1208) -> 172.20.2.3(53), 1 packet
Feb 28 14:50:10 cat3550 111072: 5w5d: %SEC-6-IPACCESSLOGP: list 103 permitted tcp 172.16.80.104(2787) -> 209.133.111.198(21), 1 packet

Contoh hasil audit file logging dengan script perl

```
[root@spyder cisco]# perl logscan.pl
Laporan koneksi yang ditolak (denied):
    13:   172.16.10.106  ->    172.16.10.255  udp port 137
     4:   172.16.16.101  ->    172.16.16.255  udp port 137
     3:   172.16.10.106  ->   216.152.244.84  tcp port 80
     2:   172.16.10.106  ->   221.142.186.37  tcp port 445
     2:   172.16.16.115  ->    216.49.88.118  tcp port 80
     1:   172.16.19.158  ->     213.61.6.18  tcp port 50131
     1:   172.16.16.114  ->     120.40.59.62  tcp port 445
     1:   172.16.10.106  ->     172.16.171.5  tcp port 445
     1:   172.16.16.101  ->   87.216.223.241  tcp port 445
     1:   172.16.16.113  ->   61.101.124.133  tcp port 445
     1:   172.16.10.106  ->  149.162.106.255  tcp port 445
     1:   172.16.10.106  ->   185.38.118.127  tcp port 445
     1:   172.16.16.101  ->   195.193.221.99  tcp port 445
     1:   172.16.16.113  ->  102.160.175.170  tcp port 445
     1:   172.16.16.101  ->   123.123.142.84  tcp port 445
Port port tujuan yang ditolak:
   370: tcp port 445
    18: udp port 137
     8: tcp port 80
     2: udp port 138
     1: tcp port 50131
Alamat IP Asal yang melakukan pelanggaran:
   177: 172.16.10.106
   127: 172.16.16.101
    70: 172.16.16.113
    17: 172.16.16.114
     2: 172.16.16.115
     1: 172.16.19.124
     1: 172.16.19.103
     1: 172.16.19.158
     1: 172.16.19.100
     1: 172.16.24.102
     1: 172.16.80.14
[root@spyder cisco]#
```

Praktik dan Tugas:
Penggunaan PGP dengan GnuPG pada Webmail

Buka https://mti.ugm.ac.id/pgp/
Login dengan account mail masing masing
Klik Option , Klik GPG Plugin Options
Klik Keyring Management Functions

Target :
- **Setiap peserta harus mampu membuat Public key dan Passphrase (sebagai Private key).**
- **Peserta dapat mengirimkan email bertanda tangan digital kepada orang lain (rekannya)**
- **Peserta dapat mengirimkan email terenkripsi ke pada rekan lain**
- **Peserta dapat membuka email terenkripsi yang dikirimkan menggunakan public key masing masing**