STUDY KASUS UJI IMPLEMENTASI CELAH KEAMANAN DHCP SERVER

Disusun oleh :

Yoghi Pratama Soedharsono (2009 81 038)

LATAR BELAKANG

- Dalam teknologi komputer telah berkembang , perkembangan yang sama juga dialami oleh perangkat lunak. Perkembangan teknologi memang menjadi hidup manusia menjadi sangat mudah. Dan sebuah jaringan internet juga sekarang makin berkembang dalam sebuah keamanan subuah jaringan internet agar lebih aman dan melinding sebuah data karena banyak orang yang tidak bertanggung jawab untuk mendapatkan sebuah file melalu sebuah internet

MASALAH-MASALAH YANG SERING TERJADI PADA DHCP SERVER

1. Masuk sebuah client yang tidak bertanggung jawab
2. Adanya gangguan terhadap DHCP server

Maka perlu adanya sebuah pengamanan terhadap DHCP server

IDENTIFIKASI MASALAH

- Mengetauhi celah kelemahan pada jaringan DHCP *server*
- Bagaimana menggamankan jaringan komputer disebuah DHCP *server*

TUJUAN PENELITIAN

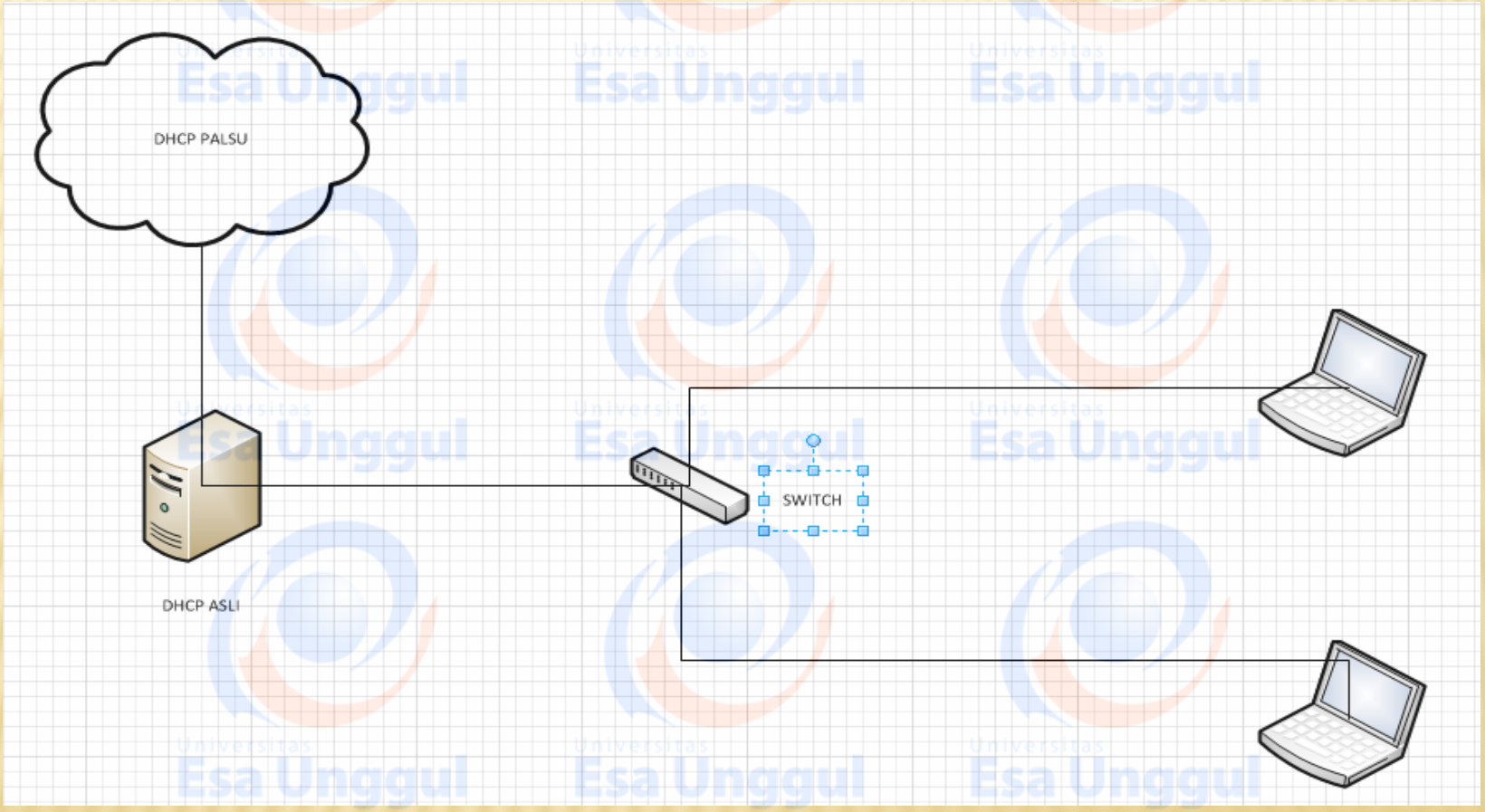
1. Membuat DHCP server
2. Mempelajari *software* yang digunakan
3. Mencari tahu langkah – langkah *heacker* menyerang DHCP
4. Mengatasi pengamanan DHCP *server*

LANDASAN TEORI

METODE ANALISIS

1. Mempelajari tentang DHCP *server*
2. Mempelajari apa yang digunakan untuk melumpuhkan DHCP *server*
3. Hadirnya client yang bukan seharusnya dilayani *server*
4. Adanya gangguan terhadap DHCP *server*

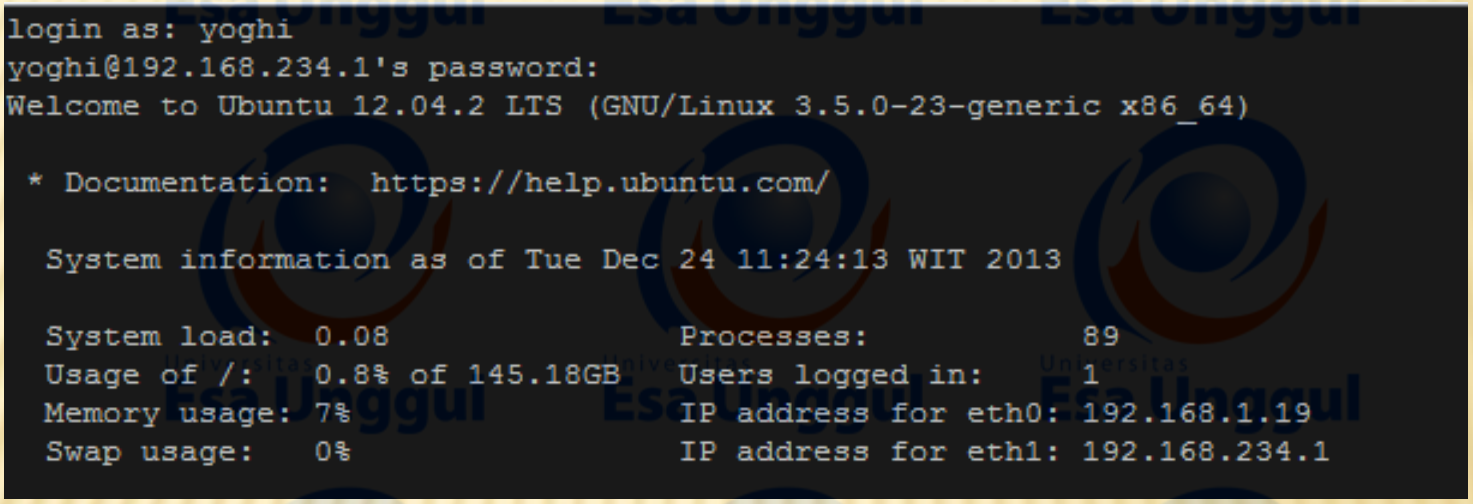
IMPLEMENTASI DAN UJI COBA



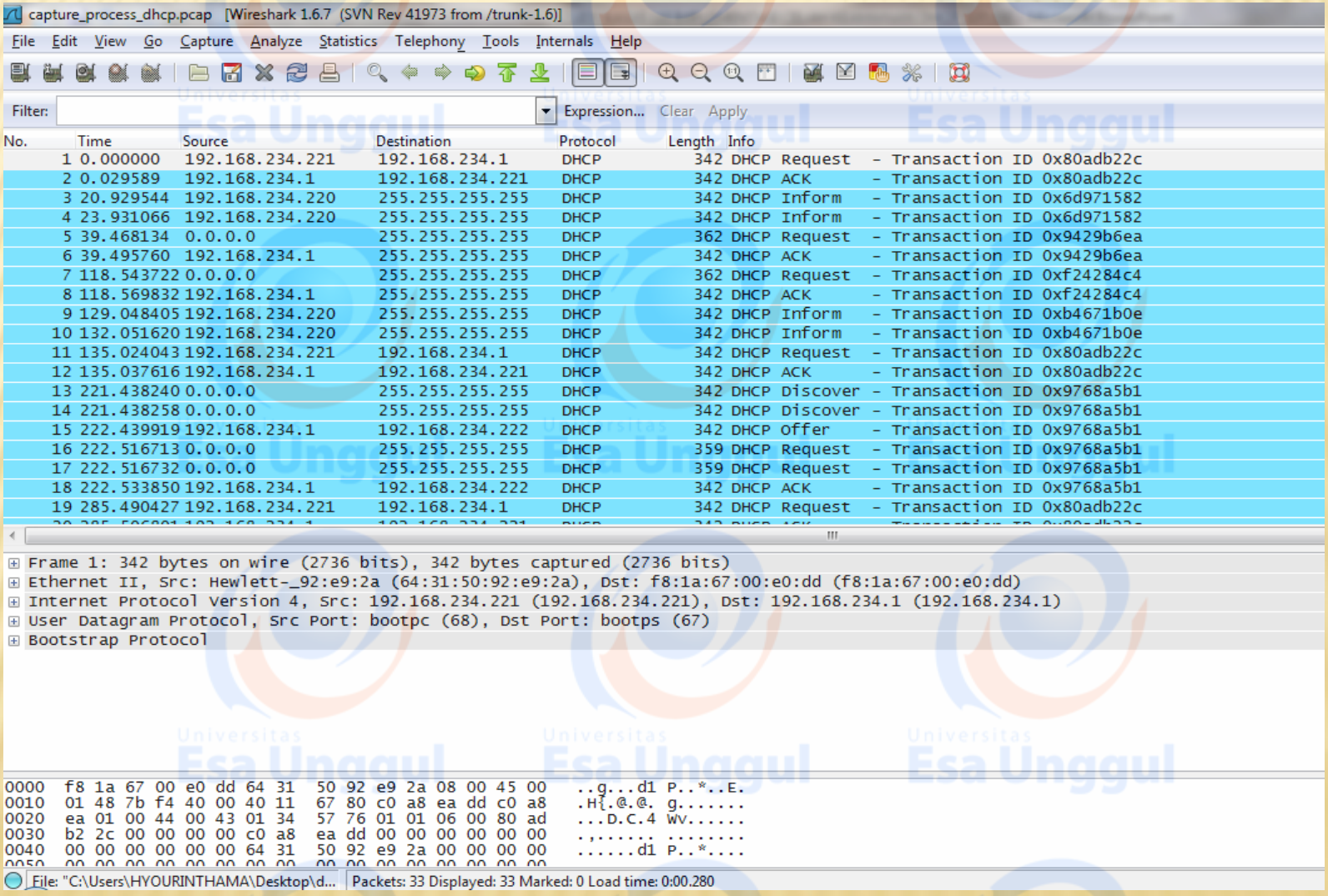
KONFIGURASI DHCP

```
  GNU nano 2.2.6               File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.1.19
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.18.255
        gateway 192.168.1.18
        # dns-* options are implemented by the resolvconf package, if installed
        dns-nameservers 8.8.8.8. 8.8.4.4
        dns-search localdomain

auto eth1
iface eth1 inet static
        address 192.168.234.1
        netmask 255.255.255.0
        network 192.168.234.0
        broadcast 192.168.234.255
```

PROSES LOGIN ADMIN



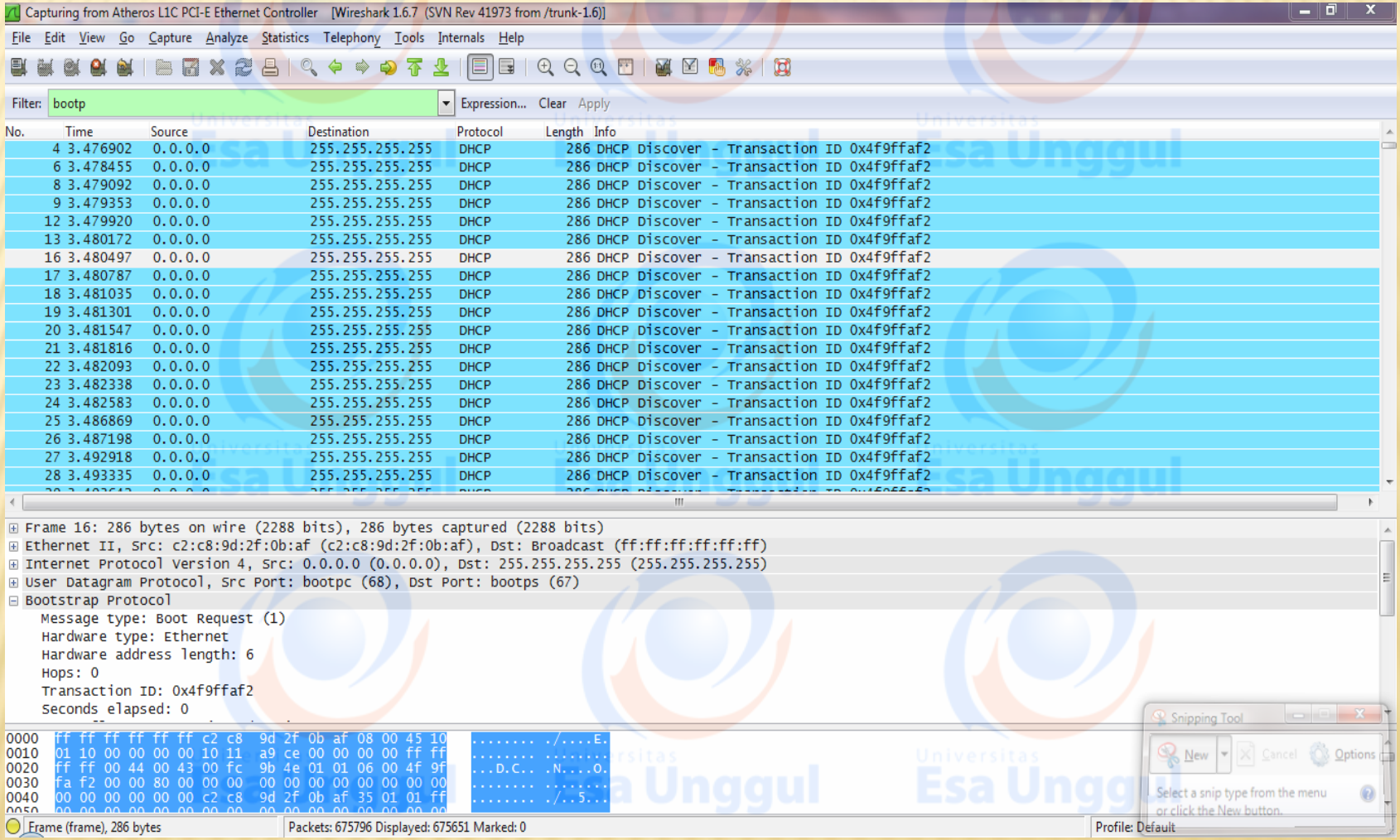
PROSES SEBUAH CLIENT MASUK KE DHCP SERVER



MASALAH YANG DIHADAPI

- Banyak yang melakukan pencurian data
- Membuat sebuah server menjadi terganggu
- Kurang maximalnya keamanan

JENIS SERANGAN TERHADAP DHCP



PROSES PENGAMANAN PADA DHCP SERVER

```
### Mulai Konfigurasi Global
###authoritative;ddns-update-style none;
log-facility local7;
ignore client-updates;

### Akhir Konfigirasi Global ###
### Deklarasi Shared Network untuk LAN dgn nama instance LAN_Interface ###
shared-network LAN_Interface {
### Deklarasi Subnet DHCP untuk Client yang dikenal
subnet  192.168.234.0  netmask 255.255.255.0 {
option broadcast-address 192.168.234.255;
option routers 192.168.234.1;
option subnet-mask 255.255.255.0;
#option netbios-name-servers 192.168.69.19, 192.168.234.1;
#option domain-name " ";
#option domain-search " ";
# Deklarasi Pool untuk Client yang dikenal

        pool {
                option domain-name-servers 8.8.8.8, 8.8.4.4;
                option time-servers 202.154.57.165, 203.89.24.34;
                max-lease-time 600;
                default-lease-time 120;
                range 192.168.234.220 192.168.234.225;
## Deklarasi hostname, MAC-Address dan IP-Adress Client yang dikenal

                host leptop04 {
                hardware ethernet 00:e0:18:ed:ab:a8;
                fixed-address 192.168.234.220;
                }

                host bokap {
                hardware ethernet 68:ed:43:d0:6f:34;
                fixed-address 192.168.234.221;
                }

                host david {
                hardware ethernet 64:31:50:92:e9:2a;
                fixed-address 192.168.234.222;
                }

                host leptop02 {
                hardware ethernet 00:e0:18:ed:ab:a7;
                fixed-address 192.168.234.223;
                }

                host leptop03 {
                hardware ethernet 00:e0:18:ed:ab:a8;
                fixed-address 192.168.234.224;
                }
```

```
                host yoghi {
                hardware ethernet 00:26:22:80:40:7b;
                fixed-address 192.168.234.225;
                }

### Deklarasi untuk menolak / blocking Client yang tidak dikenal
        deny unknown-clients;
        }
}

### Deklarasi Subnet DHCP untuk Client yang tidak dikenal
                subnet  192.168.224.0  netmask 255.255.255.0 {
                option broadcast-address 192.168.224.255;
                option routers 192.168.224.150;
                option subnet-mask 255.255.255.0;
#option netbios-name-servers 192.168.69.19, 192.168.234.1;
#option domain-name " ";
#option domain-search " ";
### Deklarasi Pool untuk Client yang tidak dikenal

                pool {
                option domain-name-servers 8.8.8.8, 8.8.4.4;
                option time-servers 202.154.57.165, 203.89.24.34;
                max-lease-time 600;
                default-lease-time 120;
                range 192.168.224.160 192.168.224.165;

### Deklarasi untuk membolehkan Client tidak dikenal untuk dilayani oleh subnet / pool ini
                allow unknown-clients;
                }
        }
}
```

PROSES PENGAMANAN DHCP SERVER DI CISCO

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address ?
  H.H.H   48 bit mac address
  sticky  Configure dynamic secure addresses as sticky

Switch(config-if)#switchport port-security mac-address 000A.000B.000C
Switch(config-if)#end
Switch#
00:22:48: %SYS-5-CONFIG_I: Configured from console by console
Switch#write memory
Building configuration...
[OK]
```

MELIHAT STATUS PORT-SECURITY PADA INTERFACES TERTENTU

```
Switch#show port-security ?
  address    Show secure address
  interface  Show secure interface
  |          Output modifiers
  <cr>

Switch#show port-security interface FastEthernet 0/8
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address        : 0000.0000.0000
Security Violation Count   : 0
```

melihat status port-security berdasarkan MAC-address

```
Switch#show port-security address
          Secure Mac Address Table
-----------------------------------------------------------------
Vlan    Mac Address       Type             Ports    Remaining Age
                                                     (mins)
----    -----------       ----             -----    -------------
   1    000a.000b.000c    SecureConfigured Fa0/8        -
   1    0026.2280.407b    SecureConfigured Fa0/9        -
   1    0026.2280.407a    SecureConfigured Fa0/10       -
-----------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

TERIMA KASIH