

# 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 sebuah jaringan internet agar lebih aman dan melindungi sebuah data karena banyak orang yang tidak bertanggung jawab untuk mendapatkan sebuah file melalui 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

---

- ✘ Mengetahui celah kelemahan pada jaringan DHCP *server*
- ✘ Bagaimana mengamankan 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

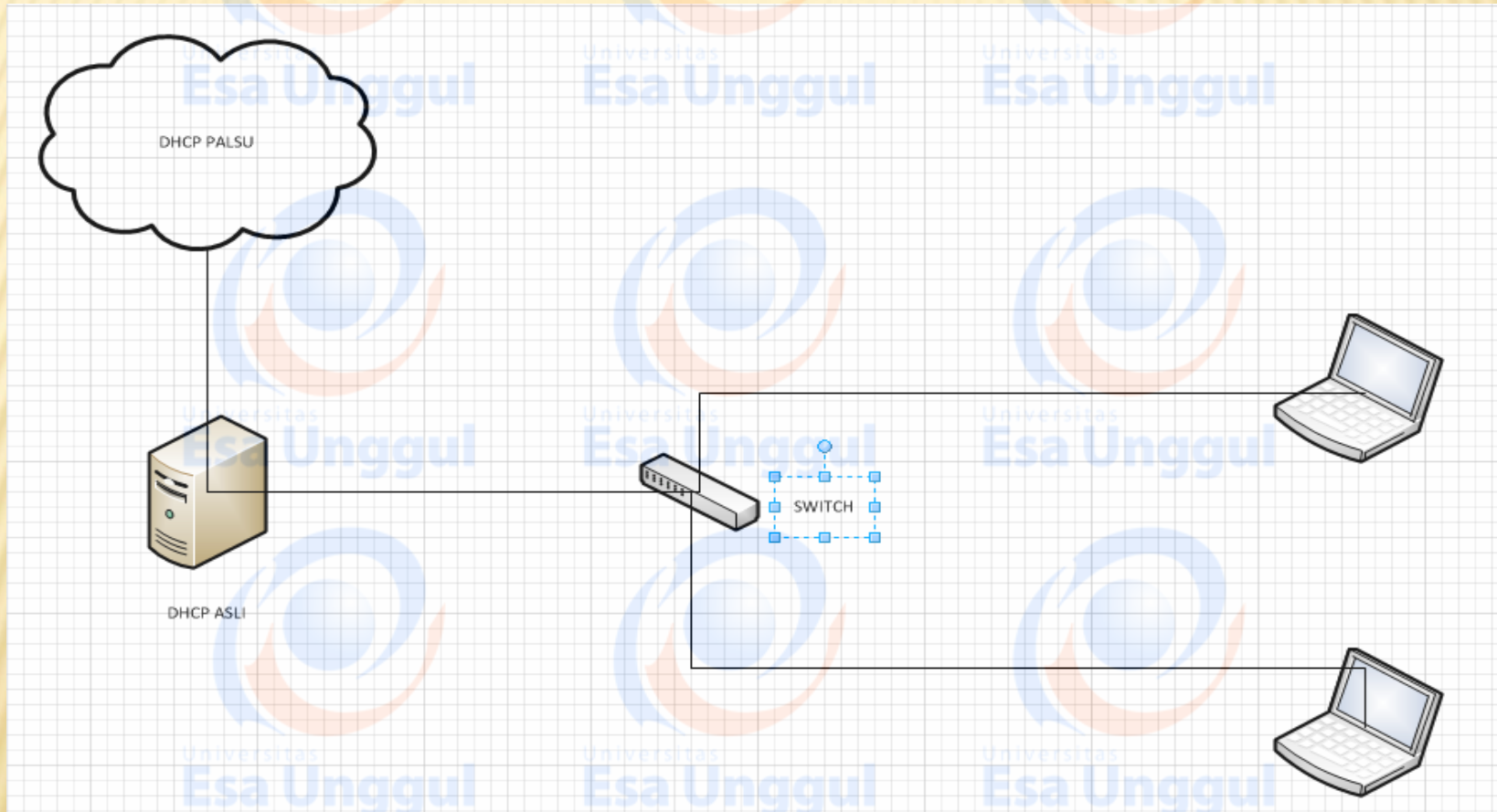


# METODE ANALISIS

---

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

```
login as: yoghi
yoghi@192.168.234.1's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic x86_64)

* Documentation:  https://help.ubuntu.com/

System information as of Tue Dec 24 11:24:13 WIT 2013

System load:  0.08          Processes:            89
Usage of /:   0.8% of 145.18GB  Users logged in:    1
Memory usage: 7%           IP address for eth0: 192.168.1.19
Swap usage:   0%           IP address for eth1: 192.168.234.1
```

# PROSES SEBUAH CLIENT MASUK KE DHCP SERVER

The image shows a Wireshark network traffic capture titled 'capture\_process\_dhcp.pcap'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter field set to 'Expression...'. The main display area shows a list of 19 DHCP packets. The selected packet (No. 1) is a DHCP Request from 192.168.234.221 to 192.168.234.1. Below the packet list, the packet details pane shows the following layers: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Bootstrap Protocol. At the bottom, the packet bytes pane shows the hexadecimal and ASCII representation of the captured data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.234.221	192.168.234.1	DHCP	342	DHCP Request - Transaction ID 0x80adb22c
2	0.029589	192.168.234.1	192.168.234.221	DHCP	342	DHCP ACK - Transaction ID 0x80adb22c
3	20.929544	192.168.234.220	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6d971582
4	23.931066	192.168.234.220	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6d971582
5	39.468134	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0x9429b6ea
6	39.495760	192.168.234.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x9429b6ea
7	118.543722	0.0.0.0	255.255.255.255	DHCP	362	DHCP Request - Transaction ID 0xf24284c4
8	118.569832	192.168.234.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xf24284c4
9	129.048405	192.168.234.220	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xb4671b0e
10	132.051620	192.168.234.220	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xb4671b0e
11	135.024043	192.168.234.221	192.168.234.1	DHCP	342	DHCP Request - Transaction ID 0x80adb22c
12	135.037616	192.168.234.1	192.168.234.221	DHCP	342	DHCP ACK - Transaction ID 0x80adb22c
13	221.438240	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9768a5b1
14	221.438258	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x9768a5b1
15	222.439919	192.168.234.1	192.168.234.222	DHCP	342	DHCP Offer - Transaction ID 0x9768a5b1
16	222.516713	0.0.0.0	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x9768a5b1
17	222.516732	0.0.0.0	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x9768a5b1
18	222.533850	192.168.234.1	192.168.234.222	DHCP	342	DHCP ACK - Transaction ID 0x9768a5b1
19	285.490427	192.168.234.221	192.168.234.1	DHCP	342	DHCP Request - Transaction ID 0x80adb22c

Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
Ethernet II, Src: Hewlett\_92:e9:2a (64:31:50:92:e9:2a), Dst: f8:1a:67:00:e0:dd (f8:1a:67:00:e0:dd)  
Internet Protocol Version 4, Src: 192.168.234.221 (192.168.234.221), Dst: 192.168.234.1 (192.168.234.1)  
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)  
Bootstrap Protocol

```
0000 f8 1a 67 00 e0 dd 64 31 50 92 e9 2a 08 00 45 00  ..g...d1 P.*...E.
0010 01 48 7b f4 40 00 40 11 67 80 c0 a8 ea dd c0 a8  .Ht.@.@.g.....
0020 ea 01 00 44 00 43 01 34 57 76 01 01 06 00 80 ad  ...D.C.4 wv.....
0030 b2 2c 00 00 00 00 c0 a8 ea dd 00 00 00 00 00 00  .....
0040 00 00 00 00 00 00 64 31 50 92 e9 2a 00 00 00 00  .....d1 P.*.....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

File: "C:\Users\HYOURINTHAMA\Desktop\d... Packets: 33 Displayed: 33 Marked: 0 Load time: 0:00.280

# MASALAH YANG DIHADAPI

---

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

# JENIS SERANGAN TERHADAP DHCP

Capturing from Atheros L1C PCI-E Ethernet Controller [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: bootp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
4	3.476902	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
6	3.478455	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
8	3.479092	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
9	3.479353	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
12	3.479920	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
13	3.480172	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
16	3.480497	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
17	3.480787	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
18	3.481035	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
19	3.481301	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
20	3.481547	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
21	3.481816	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
22	3.482093	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
23	3.482338	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
24	3.482583	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
25	3.486869	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
26	3.487198	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
27	3.492918	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2
28	3.493335	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x4f9ffaf2

Frame 16: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits)

- Ethernet II, Src: c2:c8:9d:2f:0b:af (c2:c8:9d:2f:0b:af), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol
  - Message type: Boot Request (1)
  - Hardware type: Ethernet
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0x4f9ffaf2
  - Seconds elapsed: 0

```

0000  ff ff ff ff ff ff c2 c8 9d 2f 0b af 08 00 45 10  .....E.
0010  01 10 00 00 00 00 10 11 a9 ce 00 00 00 00 ff ff  .....D.C..N...O.
0020  ff ff 00 44 00 43 00 fc 9b 4e 01 01 06 00 4f 9f  .....
0030  fa f2 00 00 80 00 00 00 00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 c2 c8 9d 2f 0b af 35 01 01 ff  .....5.
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
    
```

Frame (frame), 286 bytes      Packets: 675796 Displayed: 675651 Marked: 0      Profile: Default

Snipping Tool

New Cancel Options

Select a snip type from the menu or click the New button.

# PROSES PENGAMANAN PADA DHCP SERVER

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

### Akhir konfigurasi 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-Address 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



Universitas  
**Esa Unggul**

Universitas  
**Esa Unggul**

Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**

**TERIMA KASIH**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**



Universitas  
**Esa Unggul**

