JTIF | Jurnal INOVATIF WIRA WACANA Vol. 01 No.03 Desember 2022, 187-196 p**ISSN (**2961-7316**)**
eISSN (2962-5998**)**

Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp Snooping Dan Switch Port Security

(*Implementation Analysis of Network Security Systems Using the DHCP Snooping and Switch Port Security Methods*)

Yandrianus Christianto Dara[1],Fajar Hariadi[2], Pingky Alfa Ray Leo Lede[3]

[1, 2, 3] Program Studi Teknik Informatika, Universitas Kristen Wira Wacana Sumba

E-mail: christiandara28018@gmail.com, fajar@unkriswina.ac.id, pingky.leo.lede@unkriswina.ac.id

KEYWORDS:
DHCP, DHCP Rogue, DHCP Snooping, Port Security

ABSTRACT

In an institution, of course, it really needs a network, and of course it cannot be separated from network security. On a switch there are several ports that can be accessed by anyone, in this case what is meant is the DHCP Rogue attack. For the sake of security, we need a security method that only allows computers that have the right to access a port to connect to the network by recording the IP address and Mac address of the client that may be registered in the Mac address table of a switch. Security is also very much needed to overcome attacks when requesting and giving IP addresses to clients, because of this, DHCP Snooping is carried out which works by distinguishing ports that can be trusted and ports that cannot be trusted in terms of distributing IP addresses. With the DHCP Snooping and Switch Port Security methods, an agency's network security will be safer to use.

KATA KUNCI:
DHCP, DHCPRogue, DHCPSnooping, PortSecurity

ABSTRAK

Dalam suatu instansi tentu sangat membutuhkan suatu jaringan, dan tentunya tidak lepas dari suatu keamanan jaringan. Pada suatu switch terdapat beberapa port yang bisa diakses oleh siapa saja, dalam hal ini yang dimaksudkan adalah serangan DHCP Rogue. Demi keamanan maka perlunya suatu metode pengamanan yang hanya memperbolehkan komputer yang memiliki hak saja yang boleh mengakses suatu port untuk terhubung dalam jaringan tersebut dengan cara mencatat IP address dan MAC address dari klien yang boleh terdaftar dalam MAC address table sebuah switch. Pengamanan juga sangat di perlukan untuk menanggulangi adanya serangan saat permintaan dan pemberian IP address pada klient, karena hal tersebut maka dilakukanlah pengamanan DHCP Snooping yang bekerja dengan cara membedakan port yang bisa di percaya dan port yang tidak bisa di percaya dalam hal mendistribusikan IP address.Berdasarkan hasil penelitian DHCP Snooping berhasil mencegah Client mendapatkan IP Address, Gateway dan DNS dari DHCP Rogue Sedangkan dengan adanya Port Security berhasil mengatasi pengguna asing yang mencoba masuk dalam jaringan menggunakan port milik user yang diizinkan.

PENDAHULUAN

Kumpulan dari banyak komputer yang kemudian saling terkoneksi atara satu dengan yang lain disebut juga dengan Jaringan komputer, yang bisa membuat pengguna saling bertukar data berupa video,suara dan informasimelalui jaringan sama. Kebutuhkan internet dalam sebuah jaringan komputer juga sangat membantu untuk mencari informasi, lokasi,sarana transportasi,berita, bisnis transaksi *dan* perbankantransaksi secara *online*[1].

Secara tidak langsung, jaringan internet sangat penting bagi suatu instansi karena sangat mendukung proses kerjanya. Contohnya pada Universitas Kristen Wira Wacana Sumba sangat membutuhkan jaringan internet untuk kelancaran proses belajar-mengajar khususnya dalam masa pandemi Covid-19. Dalam proses tersebut, tentunya membutuhkan suatu layanan jaringan untuk mendapatkan *Internet Protocol (IP) Address*. Pembagian *IP Address* secara manual akan banyak membuang waktu dan tenaga karena setiap komputer harus di*setting IP Address*nya satu persatu, sehingga dibutuhkan *settingan* secara otomatis[2]. Protokol jaringan yang disebut *Dynamik Host Confguration Protocol* (DHCP). Protocol ini dapat membuat perangkat jaringan berbagi konfigurasi *IP address* kepada komputer yang membutuhkannya. Hal utama yang dibutuhkan untuk mengakses internet yaitu konfigurasi *IP address* itu sendiri, *subner mask, DNS server*dan *default gateway*. DHCP server merupakan perangkat yang akan membagi IP *address*, sedangkan DHCP *user*merupakan komputer yang menerima konfigurasi dari server[3].

Port pemindai dan DoS (*Denial of Service*)yaitu metode penyeranganjaringan komputer yang paling sering digunakan. Attackermemakai*Port pemindai*untukmenemui*port* terbuka, yang mengungkapkelemahan dari sistem dalam jaringan. Dan metode serangan selanjutnya adalah DoS, yaitu penyerang berulangkali mengirimkan permintaan ke server dengan tujuan untuk membuat server sibuksampai hangus atau putus.Penyerang kemudian dapat dengan gampang mencuri atau menghancurkan data dalam jaringan[4].

Dengan semakin berkembangnya penggunaan jaringan komputer, para *attacker* mulai memikirkan cara bagaimana mendapatkan informasi penting melalui jaringan komputer. Kerentanan terdapat pada *packet broadcast* yang dikirim oleh *client*saat pertama kali terhubung ke jaringan yaitu proses awal permintaan *IPaddress* pada DHCP server. Hal ini bisa menjadi cela keamanan karena komputer lain akan mengetahui bahwa ada permintaan *IPaddress* oleh klienyang baru sehingga diperlukan protokol keamanan untuk mengantisipasi hal tersebut [5].

Penggunaan DHCP *Rogue*merupakan cara peretasan yang paling sederhana dimana *attacker* membuat DHCP palsu yang terhubung dengan jaringan intimembuat peretas dapat mengatur DHCP server palsu dengan akses penuh untuk mendistribusikan IP a*ddress* ke klien, dan bukan hanya *IPaddress* saja, *attacker* juga mengganti *IPGateway* dan *IP Domain Name Server* (DNS) asli dengan *IPGateway* dan IP DNS yang dibuat sendiri untuk kemudian didistribusikan kepada klien yang melakukan permintaan *IP address* ke *DHCP Server*.

Pada proses ini, apa bila klien mendapat *IPGateway* dari DHCP Palsu maka *attacker* dapat membaca lalu lintas data yang dikirim oleh klien, selain itu apabila klien mendapatkan IP DNS dari DHCP Palsu, maka *attacker* dapat melakukan serangan yang dinamakan *phising* dengan mengirimkan *web* palsu, sehingga komputer klien mengisi data yang sebenarnya, kemudian data yang di-*input*-kan akan direkam untuk digunakan oleh *attacker*.Akses internet pada jaringansering mengalami kesulitan yang disebabkan oleh serangan kepada Server yang jalankan oleh *user* yang tidak sah karena kurang baiknya keamanan dalam jaringan. Beberapa kasus peretasan yang pernah terjadi akan dilampirkan pada tabel di bawah:

Table 1 Kasus Peretasan yang pernah terjadi

No	Kasus	Tahun	Keterangan
1	BPJS Kesehatan	2021	Situs milik Badan Penyelenggara Jaminan Sosial, yaitu bpjs-kesehatan.go.id diretas pada bulan Mei Tahun 2021 yang berdampak pada 279 juta data penduduk Indonesia diketahui dan dijual .
2	Asuransi BRI *Life*	2021	Asuransi BRI *Life*jadi korban peretasan pada bulan Juli tahun 2021 dan berdampak pada 2 juta data nasabah dalam format file PDF dan sekitar 463 ribu dokumen lainnya diketahui dan dijual.
3.	e-HAC Kemenkes	2021	Aplikasi *Electronic Health* (e-HAC) buatan Kementrian Kesehatan

			(Kemenkes) diretas pada bulan Juli 2021 yang berdampak pada kebocoran data 1,3 juta penduduk Indonesia yang tersimpan dalam aplikasi tersebut dan pihak Kemenkes membenarkan kejadian tersebut dilakukan oleh mitra kerja yang lama.

Tujuan utama dari keamanan komputer yaitu melindungi perangkat komputer dalam suatu jaringan dengan cara mengamankan informasi yang berada dalam jaringan tersebut[6]

Untuk menjawab masalah keamanan dalam jaringan dan juga internet diharapkan metode *DHCP snooping* dapat membantu, dimana *DHCP Snooping* akan membedakan mana *port* yang dapat dipercaya (*Trusted Port*) dan *port* yang tidak dapat dipercaya (*Untrusted Port*) dalam meneruskan paket yang berisi *FlagDHCP* (*DHCPOffer* dan *DHCPAcknowledge*).

Terdapat *hardware* khusus dalam implementasi jaringan komputer, yang berfungsi menghubungkan beberapa komputer sekaligus dengan sumber jaringan, perangkat tersebut adalah *Switch. Switch* terbagi menjadi dua jenis, yaitu:

a. Switch Unmanageable

Switch yang mampu mendistribusikan paket antara beberapa komputer yang terhubung ke suatu jaringan sama dan mengenal topologi jaringan dibanyak lapisan, memungkinkanpaketdidistribusilangsung sampai ke tujuan dengan cepat. Saat terhubung dengan sever dan *device* jaringan lain,perangkat ini akan bekerja secara otomatis. *Switch* ini memiliki kelemahan yaitu tidak bisa melakukan *setting*an konfigurasi dan hanya bisa bekerja dengan menggunakan konfigurasi yang terdapat dari pabrikan [7].

b. *Switch Manageable*

Jenis *swutch* ini memiliki kesamaan fungsi dengan *switch unmanageable*tetapisudah mampu melakukan pengaturan konfigurasi pada saat memakai dan memiliki fitur tambahan. Fitur*Quality of Service*, seperti pengaturan *banwidth*yang mengutamakan data dikirim terlebih dahulu. Kemudianmemiliki fitur pemantauan kerja jaringan yang biasa disebut*Simple Network Management Protocol* (SNMP). Dan juga terdapat *Virtual Lokal Area Network* (VLAN)yang paling banyak dipakai. Dalam peningkatan keamanan,*switch* inilah yang dipakai dalammenjalankan konfigurasi *Switch Port Security*, dengan cara melakukan pemeriksaan akses dari masing-masing*device* yang terhubung dalam suatu jaringan [8].

Switch Port Security merupakan metode yang bisa dilakukan pada *switch* agar dapat memberikan akses hanya kepada klien yang *Mac* a*ddress*-nya sudah tercatat dalam *Mac* a*ddress table* sebuah *switch*, sehingga *host* lain yang tidak bertanggung jawab tidak akan mudah terhubung ke dalam jaringan menggunakan setiap *port* yang berada di*switch*[9].*Switch Port Security* juga bisa dikatakan sebagai metode yang akan memperbolehkan user tertentu yang bisa mengakses jaringan melewati port yang disediakan di *switch* untuk mengamankan jaringan LAN (*Local Area Network*)[10]

Tujuan dari penelitian ini dapat merancang sebuah jaringan yang memiliki sistem keamanan yang mampu mencegah terjadinya serangan DHCP *Rogue* dan mencegah perangkat yang tidak dikenal untuk terhubung ke dalam jaringan.

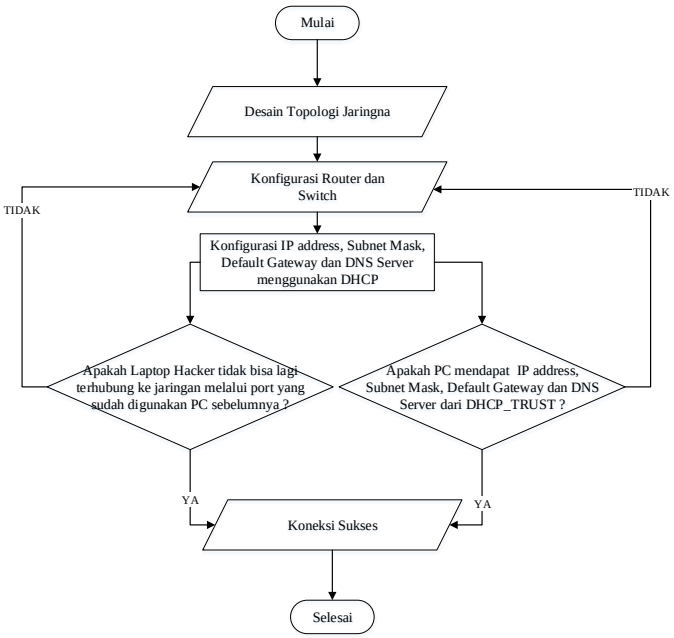
METODE PENELITIAN

Penelitian ini memakaiaplikasi simulasi Cisco Packet Tracer 8.1.1. dengan metode yang dipakaiadalah metode*DHCP Snooping* dan metode *Switch Port Security*. Adapun rancangan pada topologi yang akan dibuat dalam penelitian ini menggunakan 2 buah *router* yang berfungsi sebagai server asli dan server palsu dalam pengujian DHCP *Snooping*. Dengan menggunakan 3 buah *switch* untuk membagi VLAN.

Kemudian 18 buah PC yang menjadi klien yang diizinkan terkoneksi dalam jaringan dan 6 buah laptop yang menjadi klien yang tidak diizinkan terkoneksi dalam jaringan untuk pengujian *Switch Port Security*.

Berikut langkah-langkah pengujian yang akan dilakukan:

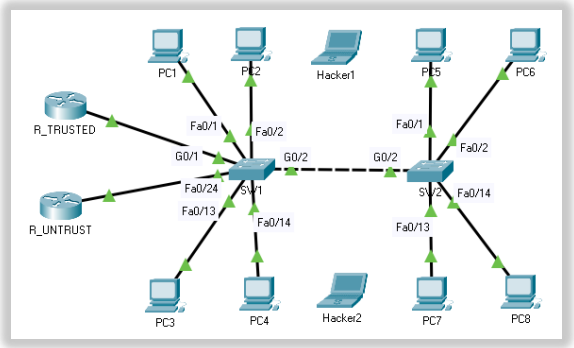
a. Merancang topologi dengan menggunakan *software* simulasi Cisco Packet Tracer
b. Melakukan *settingIP Address*, *Default Gateway*, dan *Domain Name Server*pada router
c. Melakukan konfigurasi antara *device* seperti PC, Laptop, Router dan Switch
d. Analisis perbandingan fungsi *DHCP Snoopingdan Switch Port Security*, sebelum dan sesudah penggunaan 2 metode keamanan jaringan tersebut
e. Pengujian konektivitas jaringan digambarkan menggunakan*Flowchart* Penelitian yang ditunjukkan oleh gambar berikut:



Gambar 1. *Flowchart* Simulasi

HASIL DAN PEMBAHASAN

Perancangan topologi jaringan ditampilkan pada gambar dibawah:



Gambar 2.RancanganTopologi Jaringan

Pada topologi di atas *Switch* akan dikonfigurasikan menggunakan 2 VLAN tanpa *DHCP Snooping* dan *Switch Port Security*, dan juga terdapat 2 Laptop *Hacker* yang berguna saat pengujian *Switch Port Security*. Berikut konfigurasi VLAN pada SW1 dan SW2:

Tabel 1. Konfigurasi VLAN

SW1	**SW2**
SW1>ENABLE	SW2>ENABLE
SW1#CONF T	SW2#CONF T
SW1(config)#VLAN 10	SW2(config)#VLAN 10
SW1(config-vlan)#NAME RUANG1	SW2(config-vlan)#NAME RUANG1
SW1(config-vlan)#VLAN 20	SW2(config-vlan)#VLAN 20
SW1(config-vlan)#NAME RUANG2	SW2(config-vlan)#NAME RUANG2
SW1(config-vlan)#EXIT	SW2(config-vlan)#EXIT
SW1(config)#INT RANGE FA0/1-12	SW2(config)#INT RANGE FA0/1-12
SW1(config-if-range)#SWITCHPORT ACCESS VLAN 10	SW2(config-if-range)#SWITCHPORT ACCESS VLAN 10
SW1(config-if-range)#SWITCHPORT MODE ACCESS	SW2(config-if-range)#SWITCHPORT MODE ACCESS
SW1(config-if-range)#INT RANGE FA0/13-23	SW2(config-if-range)#INT RANGE FA0/13-24
SW1(config-if-range)#SWITCHPORT ACCESS VLAN 20	SW2(config-if-range)#SWITCHPORT ACCESS VLAN 20
SW1(config-if-range)#SWITCHPORT MODE ACCESS	SW2(config-if-range)#SWITCHPORT MODE ACCESS
SW1(config-if-range)#INT RANGE G0/1-2	SW2(config-if-range)#INT RANGE G0/1-2
SW1(config-if-range)#SWITCHPORT MODE TRUNK	SW2(config-if-range)#SWITCHPORT MODE TRUNK
SW1(config-if-range)#EXIT	SW2(config-if-range)#EXIT
SW1(config)#INT FA0/24	SW2(config)#EXIT
SW1(config-if)#SW MODE TRUNK	SW2#
SW1(config-if)#EXIT	
SW1(config)#EXIT	

Pada tabel konfigurasi di atas dibuat 2 VLAN pada masing-masing *Switch*, yang pertama *VLAN* dengan ID 10 menggunakan *VLAN Name* RUANG1 dan VLAN dengan ID 20 menggunakan *VLAN Name* Ruang2. Untuk pembagian Port pada SW1, VLAN 10 masuk dalam rentang *port* Fa0/1 sampai Fa0/12 dan *VLAN* 20 masuk dalam rentang *port* Fa0/13 sampai Fa0/23. Port Fa0/24 tidak masuk dalam pembagian *VLAN* karena *port* tersebut akan digunakan untuk menghubungkan SW1 dengan R_Untrust sebagai *DHCP* yang tidak dapat dipercaya. Untuk pembagian *port* pada SW2, *VLAN* 10 masuk dalam rentang *port* Fa0/1 sampai Fa0/12 dan VLAN 20 masuk dalam rentang *port* Fa0/13 sampai Fa0/24.
Konfigurasi *DHCP Trusted* dan *DHCP Untrust* pada Router sebagai berikut:

Tabel 2. Konfigurasi *DHCP Trusted* dan *DHCP Untrust*

DHCP Trusted	***DHCP Untrust***
R_Trusted>ENABLE	R_Untrust>ENABLE
R_Trusted#CONF T	R_Untrust#CONF T
R_Trusted(config)#INT G0/0	R_Untrust(config)#INT G0/0
R_Trusted(config-if)#NO SHUTDOWN	R_Untrust(config-if)#NO SHUTDOWN
R_Trusted(config-if)#EXIT	R_Untrust(config-if)#EXIT
R_Trusted(config)#INT G0/0.10	R_Untrust(config)#INT G0/0.10
R_Trusted(config-subif)#ENCAPSULATION DOT1Q 10	R_Untrust(config-subif)#ENCAPSULATION DOT1Q 10
R_Trusted(config-subif)#IP ADD 192.168.10.1 255.255.255.0	R_Untrust(config-subif)#IP ADD 210.0.10.1 255.255.255.0
R_Trusted(config-subif)#EXIT	R_Untrust(config-subif)#EXIT
R_Trusted(config)#INT G0/0.20	R_Untrust(config)#INT G0/0.20
R_Trusted(config-subif)#ENCAPSULATION DOT1Q 20	R_Untrust(config-subif)#ENCAPSULATION DOT1Q 20
R_Trusted(config-subif)#IP ADD 192.168.20.1 255.255.255.0	R_Untrust (config-subif)#IP ADD 210.0.20.1 255.255.255.0
R_Trusted(config-subif)#EXIT	R_Untrust(config-subif)#EXIT
R_Trusted(config)#IP DHCP POOL RUANG1	R_Untrust(config)#IP DHCP POOL RUANG1
R_Trusted(dhcp-config)#NETWORK 192.168.10.0	R_Untrust(dhcp-config)#NETWORK 210.0.10.0

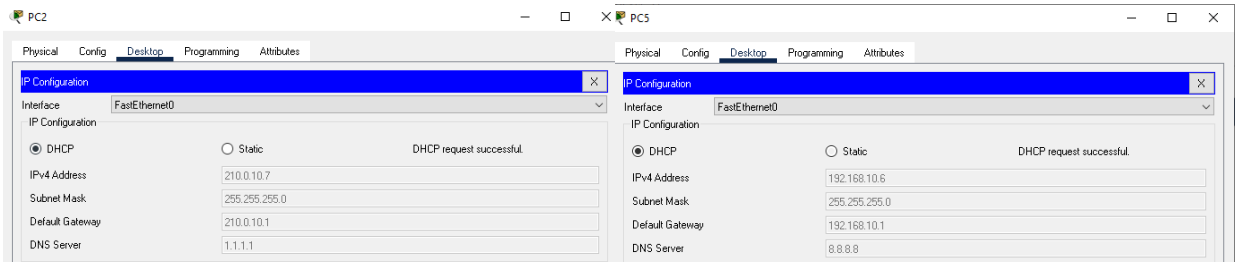
```
255.255.255.0                                   255.255.255.0
R_Trusted(dhcp-config)#DEFAULT-ROUTER           R_Untrust(dhcp-config)#DEFAULT-ROUTER
192.168.10.1                                    210.0.10.1
R_Trusted(dhcp-config)#DNS-SERVER 8.8.8.8       R_Untrust(dhcp-config)#DNS-SERVER 1.1.1.1
R_Trusted(dhcp-config)#EXIT                     R_Untrust(dhcp-config)#EXIT
R_Trusted(config)#IP DHCP POOL RUANG2           R_Untrust(config)#IP DHCP POOL RUANG2
R_Trusted(dhcp-config)#NETWORK 192.168.20.0     R_Untrust(dhcp-config)#NETWORK 210.0.20.0
255.255.255.0                                   255.255.255.0
R_Trusted(dhcp-config)#DEFAULT-ROUTER           R_Untrust(dhcp-config)#DEFAULT-ROUTER
192.168.20.1                                    210.0.20.1
R_Trusted(dhcp-config)#DNS-SERVER 8.8.8.8       R_Untrust(dhcp-config)#DNS-SERVER 1.1.1.1
R_Trusted(dhcp-config)#EXIT                     R_Untrust(dhcp-config)#EXIT
R_Trusted(config)#                              R_Untrust(config)#
```

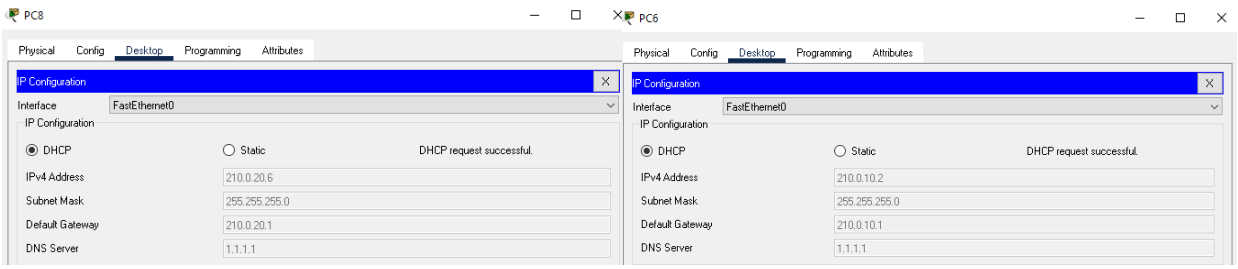
IP Address dari PC1hingga PC8 di-*setting* memakai DHCP dan *IP-address* yang didapat oleh beberapa PC tersebut akan berbeda sehingga ada beberapa PC yang mendapat IP dari *DHCP Trusted* dan ada juga yang mendapat IP dari *DHCP Untrust*.

Tabel 3. Konfigurasi *IP-Address* Sebelum Memakai*DHCP-Snooping*

Device	VLAN Id	IP Address	Subnetmask	Gateway	DNS
R_Trusted	10	192.168.10.1	255.255.255.0	192.168.10.1	8.8.8.8
	20	192.168.20.1	255.255.255.0	192.168.20.1	8.8.8.8
R_Untrust	10	210.0.10.1	255.255.255.0	210.0.10.1	1.1.1.1
	20	210.0.20.1	255.255.255.0	210.0.20.1	1.1.1.1
PC1	10	192.168.10.3	255.255.255.0	192.168.10.1	8.8.8.8
PC2	10	210.0.20.7	255.255.255.0	210.0.20.1	1.1.1.1
PC3	20	192.168.20.7	255.255.255.0	192.168.20.1	8.8.8.8
PC4	20	192.168.20.3	255.255.255.0	192.168.20.1	8.8.8.8
PC5	10	192.168.10.6	255.255.255.0	192.168.10.1	8.8.8.8
PC6	10	210.0.10.2	255.255.255.0	210.0.10.1	1.1.1.1
PC7	20	192.168.20.3	255.255.255.0	192.168.20.1	8.8.8.8
PC8	20	210.0.20.6	255.255.255.0	210.0.20.1	1.1.1.1

Pada tabel konfigurasi di atas dapat dilihat ada beberapa PC diantaranya PC1, PC3, PC4, PC5 dan PC7 mendapat *IPAddress*, *Gateway* dan *Domain Name Server* dari *DHCP Trusted* sedangkan beberapa PC mendapat *IP Address*, *Gateway* dan *Domain Name Server* dari *DHCP Untrust*.





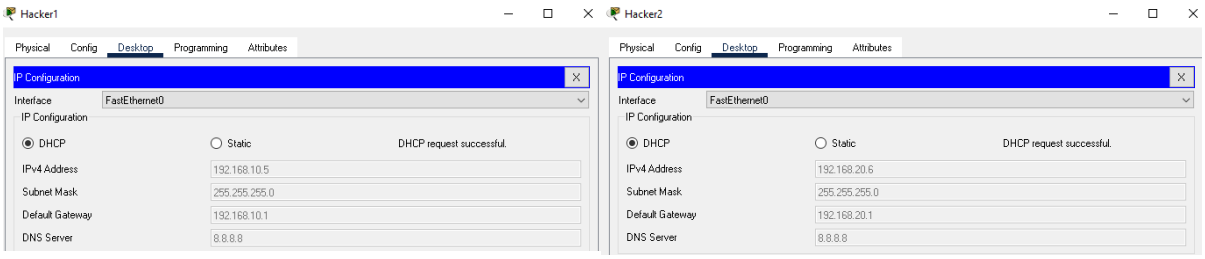
Gambar 3. Pengujian PC tanpa *DHCP Snooping*

Konfigurasi *IP Address* sebelum menggunakan *Switch Port Security* akan dipaparkan dalam tabel berikut:

Tabel 4. Konfigurasi*IP Address*Sebelum Menggunakan *Switch Port Security*

Device	MAC Address	IP Address	Port	Status
PC1	0040.0b3a.d624	192.168.10.4	Fa0/1	Dikenali
PC2	0060.47cd.e597	210.0.20.7	Fa0/2	Dikenali
PC3	000a.41b2.8d40	192.168.20.7	Fa0/13	Dikenali
PC4	000a.f396.4d3d	192.168.20.2	Fa0/14	Dikenali
PC5	0002.4ab0.8892	192.168.10.6	Fa0/1	Dikenali
PC6	0001.6409.e056	210.0.10.2	Fa0/2	Dikenali
PC7	0001.96bb.9ea9	192.168.20.3	Fa0/13	Dikenali
PC8	0003.e4c0.4b30	210.0.20.6	Fa0/14	Dikenali
Hacker1	0004.9a15.6d51	192.168.10.5	Fa0/2	Tidak Dikenali
Hacker2	00d0.bca5.0956	192.168.20.6	Fa0/13	Tidak Dikenali

Pada tabel permintaan*IP address* oleh Laptop *Hacker* di atas, terlihat bahwa para *Hacker* berhasil mendapat *IP address* dari *DHCP server* menggunakan port Fa0/2 milik PC2 pada SW1 dan port Fa0/13 milik PC7 pada SW2.



Gambar 4. Pengujian Laptop *Hacker* tanpa *Switch Port Security*

Hasil perancangan simulasi jaringan komputer dengan mengonfigurasi*Switch* menggunakan *DHCP Snooping*.

Berikut konfigurasi *DHCP Snooping* pada SW1:

```
SW1>ENABLE
SW1#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#IP DHCP SNOOPING VLAN 10,20
SW1(config)#NO IP DHCP SNOOPING INFORMATION OPTION
SW1(config)#IP DHCP SNOOPING
SW1(config)#INT G0/1
SW1(config-if)#DESCRIPTION "DHCP TRUSTED"
```

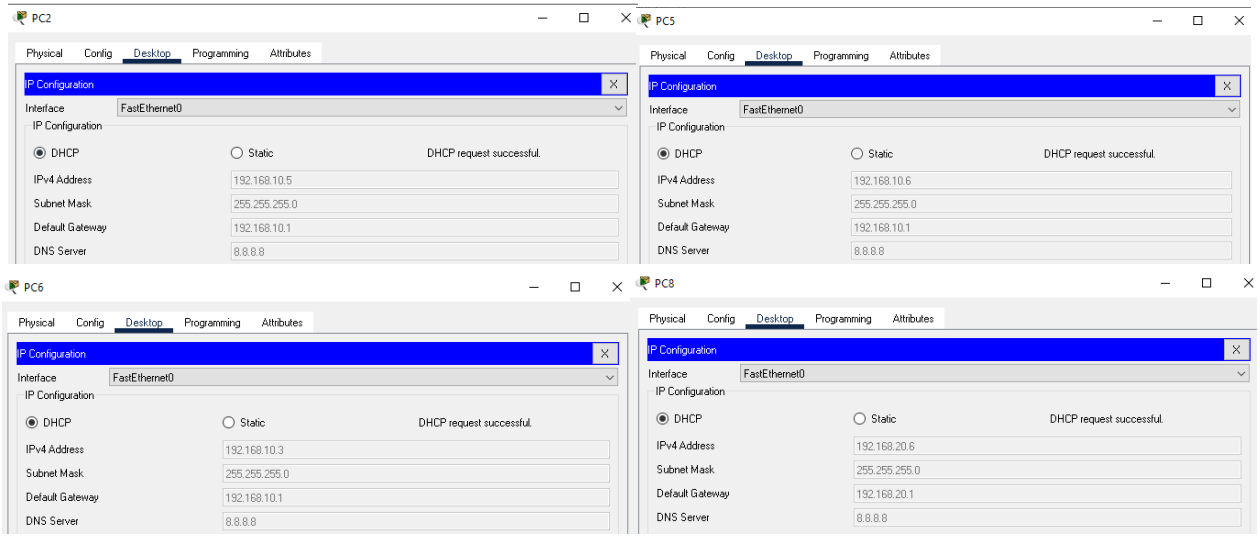
```
SW1(config-if)#IP DHCP SNOOPING
SW1(config)#INT G0/1
SW1(config-if)#IP DHCP SNOOPING TRUST
SW1(config-if)#EXIT
SW1(config)#
```

Pada konfigurasi di atas, perintah *IP DHCP Snooping* mengaktifkan metode keamanan *DHCPSnooping* dan hanya *port* G0/1 yang dapat dipercaya sebagai *DHCP server* dengan deskripsi *DHCP TRUSTED.*

Hasil dari konfigurasi ditampilkan pada tabel di bawah:

Tabel 5. Konfigurasi *IP-Address* Sesudah Menggunakan *DHCP-Snooping*

Device	VLAN ID	IP Address	Subnetmask	Gateway	DNS
R_Trusted	10	192.168.10.1	255.255.255.0	192.168.10.1	8.8.8.8
	20	192.168.20.1	255.255.255.0	192.168.20.1	8.8.8.8
R_Untrust	10	210.0.10.1	255.255.255.0	210.0.10.1	1.1.1.1
	20	210.0.20.1	255.255.255.0	210.0.20.1	1.1.1.1
PC1	10	192.168.10.4	255.255.255.0	192.168.10.1	8.8.8.8
PC2	10	192.168.10.5	255.255.255.0	192.168.10.1	8.8.8.8
PC3	20	192.168.20.7	255.255.255.0	192.168.20.1	8.8.8.8
PC4	20	192.168.20.2	255.255.255.0	192.168.20.1	8.8.8.8
PC5	10	192.168.10.6	255.255.255.0	192.168.10.1	8.8.8.8
PC6	10	192.168.10.3	255.255.255.0	192.168.10.1	8.8.8.8
PC7	20	192.168.20.3	255.255.255.0	192.168.20.1	8.8.8.8
PC8	20	192.168.20.6	255.255.255.0	192.168.20.1	8.8.8.8



Gambar 5. Pengujian PC setelah menggunakan *DHCP Snooping*

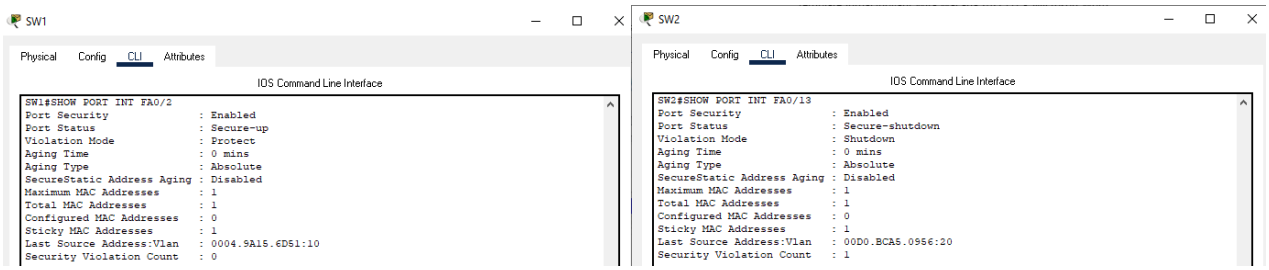
Berdasarkan hasil konfigurasi *DHCP Snooping* di atas, dapat dilihat bahwa semua PC berhasil mendapat *IP Address*,*DNS server*dan*Gateway*dari *DHCPTrusted* atau *Server* yang dipercaya, kemudian PC2, PC6 dan PC8 tidak lagi mendapat *IP Address*,*DNS server*dan*Gateway* dari *DHCP Untrusted* atau *Server* yang tidak dipercaya.

Untuk implementasi *Switch Port Security* pada SW1 dan SW2ditampilkan pada tabel di bawah:

Tabel 6. konfigurasi *Switch Port Security*

SW1	SW2
SW1>ENABLE	SW2>ENABLE
SW1#CONF T	SW2#CONF T
SW1(config)#INT RANGE FA0/1-12	SW2(config)#INT RANGE FA0/1-12
SW1(config-if-range)#SWICHPORT PORT-SECURITY	SW2(config-if-range)#SWICHPORT PORT-SECURITY
SW1(config-if-range)#SWICHPORT PORT-SECURITY MAC-ADD STICKY	SW2(config-if-range)#SWICHPORT PORT-SECURITY MAC-ADD STICKY
SW1(config-if-range)#SWICHPORT PORT-SECURITY MAX 1	SW2(config-if-range)#SWICHPORT PORT-SECURITY MAX 1
SW1(config-if-range)#SWICHPORT PORT-SECURITY VIOLATION PROTECT	SW2(config-if-range)#SWICHPORT PORT-SECURITY VIOLATION RESTRICT
SW1(config-if-range)#EXIT	SW2(config-if-range)#EXIT
SW1(config)#INT RANGE FA0/13-23	SW2(config)#INT RANGE FA0/12-24
SW1(config-if-range)#SWICHPORT PORT-SECURITY	SW2(config-if-range)#SWICHPORT PORT-SECURITY
SW1(config-if-range)#SWICHPORT PORT-SECURITY MAC-ADD STICKY	SW2(config-if-range)#SWICHPORT PORT-SECURITY MAC-ADD STICKY
SW1(config-if-range)#SWICHPORT PORT-SECURITY MAX 1	SW2(config-if-range)#SWICHPORT PORT-SECURITY MAX 1
SW1(config-if-range)#SWICHPORT PORT-SECURITY VIOLATION RESTRICK	SW2(config-if-range)#SWICHPORT PORT-SECURITY VIOLATION SHUTDOWN
SW1(config-if-range)#EXIT	SW2(config-if-range)#EXIT
SW1(config)#	SW2(config)#

Pada konfigurasi di atas, masing-masing *switch* dibagi 2 *violation*, pada SW1 VLAN10 menggunakan *violation Protect* dan VLAN20 menggunakan *violation Restrict*, kemudian pada SW2 VLAN10 menggunakan *violation Restrict* dan VLAN20 menggunakan *violation Shutdown*. Untuk *mac-address* dibaca denganotomatis bagi perangkat yang tersambung pertama kali dengan *port*pada *switch*menggunakan metode *Sticky*. kemudian perintah *SwitchportPort-Security* Max 1 berarti membatasi jumlah *mac address* yang boleh menggunakan setiap *port* yang ada, dalam hal ini hanya boleh 1 *mac address* saja yang boleh tersambung menggunakan setiap *port*. Berdasarkan konfigurasi setelah penggunaan *Switch Port Security*, hasil konfigurasi ditampilkan pada gambar di bawah:



Gambar 6. Hasil Konfigurasi Laptop *Hacker* setelah menggunakan *Switch Port-Security*

Terlihat *port interface* Fa0/2 pada*switch* SW1 memilikijumlah maksimum *mac address* sesuai dengan yang sdah diatur dan *violatian*-nya adalah *protect*. *Violation*ini tidak memutuskan koneksi tetapi data akan tetap di drop dan pelanggaran tidak di hitung, berbeda dengan *port* Fa0/13 pada SW2, *violation shutdown* akan otomatis memutuskan koneksi dan menghitung pelanggaran yang terjadi.

KESIMPULAN

Berdasarkan hasil pengujian dalam rancangansimulasi maka dapat disimpulkan:

a. Penggunaan metode keamanan *DHCP Snooping* dapat mengatasi masalah *DHCP Untrusted* atau *DHCP Server* yang tidak dapat dipercaya dengan cara menentukan *port* yang bisa dipercaya dengan hasil

pengujian bahwa setiap PC yang ada pada simulasi jaringan tidak lagi mendapat *IP Address, DNS server*, dan *Gateway* dari *DHCP Untrusted* atau *Server* yang tidak dipercayadengan hasil persentase pengujian sebelum adanya *DHCP Snooping* sebesar 62,5% PC yang mendapat *IP Address*, *Gateway* dan *DNS server* dari *DHCP Trusted* dan 32,5% PC yang mendapat *IP Address*, *Gateway* dan *DNS server* dari *DHCP Untrusted* atau *Server* yang tidak dipercaya, Kemudian setelah adanya *DHCP Snooping,* hasil persentase jumlah PC yang mendapat *IP Address*, *Gateway* dan *DNS server* dari *DHCP Trust* adalah 100%.

b. Penggunaan metode *Switch Port Security* dapat mengatasi *user* asing yang ingin masuk dalam sebuah jaringan menggunakan *port* yang sudah digunakan oleh PC yang *macaddress*-nya sudah tercatat dalam *macaddress* tabel sebuah *switch*dengan cara membatasi jumlah maksimal *mac address* yang boleh terkoneksi pada setiap port dan menggunakan *violation* atau penanganan jika terjadi pelanggaran. Hasil persentase pengujian jumlah laptop *Hacker* yang berhasil terkoneksi ke jaringan sebelum adanya *Switch Port Security*adalah 100% dan hasil persentase pengujian setelah adanya *Switch Port Security*, jumlah laptop *Hacker* yang berhasil terkoneksi kedalam jaringan adalah 0%.

DAFTAR PUSTAKA

[1] Z. Miftah, "Simulasi Keamanan Jaringan Dengan Metode DHCP Snooping Dan VLAN," *Fakt. Exacta*, vol. 11, no. 2, p. 167, 2018, doi: 10.30998/faktorexacta.v11i2.2456.

[2] D. Kurnia, "Analisis Serangan DHCP Starvation Attack pada Router OS Mikrotik," *J. Ilm. Core IT Community Res. Inf. Technol.*, vol. 8, no. 5, pp. 12–17, 2020.

[3] N. Sarip and A. Setyanto, "Filter Paket Berdasarkan Differentiated Services Code Point untuk Pencegahan Serangan DHCP Starvation Packet," *J. Pekommas*, vol. 4, no. 2, p. 137, 2019, doi: 10.30818/jpkm.2019.2040204.

[4] I. Anugrah and R. H. Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 5, no. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.

[5] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *Tek. Inform. dan Sist. Inf.*, vol. 2, pp. 302–307, 2021.

[6] M. S. Hasibuan, "Keylogger Pada Aspek Keamanan Komputer," vol. 03, pp. 8–15, 2016.

[7] O. K. Sulaiman, "Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security," *Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 9–14, 2016.

[8] S. Sudaryanto, "Implementation Port Security for Security Systems Network at the Computing Laboratory of Adisutjipto College of Technology," *Conf. Senat. STT Adisutjipto Yogyakarta*, vol. 4, 2018, doi: 10.28989/senatik.v4i0.239.

[9] T. Ariyadi, "Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN)," *Jusikom*, vol. 2, no. 1, pp. 28–29, 2017.

[10] S. S. Zara, A. M. Elhanafi, and ..., "Permodelan Jaringan Wan Dengan Teknologi Frame Relay Dengan Memanfaatkan Switch Port Security Sebagai Sistem Keamanan Jaringan," *Semin. Nas. Teknol. Inf. Komun. Ke-7*, 2020, [Online]. Available: http://prosiding.snastikom.com/index.php/SNASTIKOM2020/article/view/66