Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

SIMULASI KEAMANAN JARINGAN DENGAN METODE DHCP SNOOPING DAN VLAN

ZAENI MIFTAH
Program Studi Teknik Informatika
Sekolah Tinggi Manajemen Informatika dan Komputer Eresha
Email : zaenimiftah02@gmail.com

Abstrak. Jaringan komputer dan *internet* merupakan kebutuhan bagi masyarakat. Banyaknya pengguna jaringan komputer dan *internet* menyebabkan keamanan pada jaringan komputer dan *internet* merupakan hal yang sangat dibutuhkan pada saat ini, khususnya di lingkungan STMIK Eresha. Banyak upaya yang dilakukan untuk memberikan pelayanan jaringan komputer dan *internet* seperti peningkatan *bandwith*, memberikan keamanan pada jaringan komputer dan *internet* seperti menggunakan *ACL, Switchport Security, Vlan* dan *DHCP Snooping. DHCP Snooping* merupakan keamanan pada jaringan komputer dan *internet* yang digunakan untuk mencegah atau memfilter adanya *server* lain yang tidak dipercaya dalam memberikan akses jaringan kepada pengguna atau komputer *client*. Peneliti akan melakukan analisis perbandingan terhadap jaringan komputer dan *internet* dengan metode *DHCP Snooping* dan tanpa *DHCP Snooping* menggunakan *software* simulasi *Cisco Packet Tracer*. Hasil perbandingan keamanan jaringan komputer dan *internet* tanpa *DHCP Snooping* yaitu beberapa komputer *client* tidak aman serta tidak dapat terhubung ke *server* sedangkan apabila menggunakan metode *DHCP Snooping* mampu melakukan filter atau penyaringan terhadap *server* yang tidak dipercaya sehingga jaringan komputer dan *internet* menjadi aman.

Kata Kunci: keamanan jaringan, VLAN, DHCP *snooping*

Abstract. *Computer and internet networks are a necessity for society. The large number of users of computer network and internet cause security in computer and internet network is very needed at this time, especially in STMIK Eresha environment. Many efforts are made to provide computer network services and the Internet such as increased bandwidth, providing security on computer networks and the Internet such as using ACL, Switchport Security, Vlan and DHCP Snooping. DHCP Snooping is a security on computer and internet networks that are used to prevent or filter the existence of other servers that are not trusted in providing network access to the user or client computer. The author will perform comparative analysis of computer network and internet with Snooping DHCP method and without DHCP Snooping using Cisco Packet Tracer simulation software. The result of comparison of computer network security and internet without DHCP Snooping that is some client computer is not secure and cannot connect to server while if using DHCP method Snooping able to filter or filtering against server that is not trusted so that computer network and internet become secure.*

Keyword: network security, VLAN, DHCP snooping

PENDAHULUAN

Jaringan *internet* merupakan kebutuhan bagi masyarakat umum dalam rangka mencari informasi berita, sarana transportasi, lokasi, transaksi bisnis *online* sampai pada transaksi perbankan secara *online*. Bagi pelajar jaringan *internet* sering digunakan untuk pembelajaran *online*, akses sistem akademik, akses perpustakaan *online* dan lain-lain. Semakin banyaknya

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

pengguna yang memanfaatkan jaringan *internet* maka keamanan jaringan komputer merupakan hal yang sangat dibutuhkan khususnya di lingkungan STMIK Eresha. Keamanan jaringan komputer melibatkan banyak aspek, mulai dari perlindungan peralatan secara fisik seperti perangkat keras, akses terhadap sumberdaya jaringan, perlindungan data serta informasi yang berada pada jaringan untuk mencegah terjadinya pencurian data.

Keamanan jaringan komputer di lingkungan STMIK Eresha masih memiliki kekurangan karena akses jaringan hanya diberikan melalui *DHCP Server*. Hal ini menyebabkan terjadinya serangan berupa *DHCP Rogue* yaitu *DHCP Server* palsu yang memberikan alamat *gateway* yang salah pada komputer *client* sehingga komputer tidak dapat terhubung pada sebuah jaringan dan *internet*. Keamanan jaringan yang belum baik menyebabkan akses *internet* pada jaringan sering terjadi masalah dikarenakan serangan terhadap *DHCP Server* yang dilakukan oleh orang yang tidak bertanggung jawab. Oleh karena itu maka metode keamanan pada jaringan komputer perlu ditingkatkan, misalnya dengan menggunakan *DHCP snooping*. Metode *DHCP snooping* diharapkan dapat membantu mengatasi masalah keamanan jaringan komputer dan internet.

Tinjauan Pustaka

Dalam jaringan komputer diperlukan beberapa komponen perangkat jaringan yang terdiri dari:

1. *Router*

   Router merupakan perangkat jaringan yang bertanggung jawab untuk meneruskan atau mengirimkan data dari satu *network* ke *network* yang berbeda. *Router* sering digunakan untuk menghubungkan *network* yang menggunakan topologi *Bus, Ring* dan *Star* (Sofana, 2009).

   Router cisco mempunyai komponen-komponen diantaranya:

   a. RAM (Random Acces Memory)

   RAM termasuk Memori *Volatile* yaitu menyimpan konfigurasi sementara selama *router* menyala seperti *Running IOS, Running* Konfigurasi *File*, *IP Routing* dan *Table ARP*

   b. ROM (Random Only Memory)

   ROM termasuk *Non-volatile* yaitu menyimpan secara permanen seperti Instruksi *Bootup, Software* Diagnostik Dasar.

   c. NVRAM (Non-volatile RAM)

   NVRAM termasuk *Non-volatile* yaitu menyimpan secara permanen seperti *startup configuration file*.

   d. Flash Memory

   Flash termasuk *Non-volatile* yaitu menyimpan secara permanen seperti *IOS image sistem operasi (cisco IOS).*

Gambar 1. Perangkat *Cisco Router*

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

2 *Switch*

Switch merupakan perangkat yang berfungsi untuk menghubungkan beberapa komputer ataupun perangkat jaringan agar dapat berbagi sumber daya. *Switch* juga merupakan perangkat keras yang memungkinkan terjadinya distribusi paket data antar komputer dalam jaringan dan mampu untuk mengenali topologi jaringan dibanyak *layer* sehingga data dapat langsung sampai ketujuan (Sulaiman, 2016).

Gambar 2. Perangkat *Switch Cisco*

3. *Wireless Access Point*

Wireless Access Point merupakan suatu perangkat yang digunakan untuk menghubungkan pengguna dengan jaringan komputer biasa. *Access Point* menerima data dari pengguna dalam bentuk gelombang berfrekuensi radio kemudian meneruskannya ke jaringan kabel. *Access Point* juga mengirimkan data dari jaringan ke pengguna dalam bentuk gelombang radio. (Prasetiono, 2010).

.

Gambar 3. Perangkat *Access Point*

4. VLAN

VLAN adalah suatu jaringan yang dibangun berdasarkan kelompok atau grup dalam satu *network* dimana beberapa komputer hanya dapat berkomunikasi sesuai dengan kelompok atau grup yang dibuat. VLAN dapat meningkatkan *performance* pada jaringan. VLAN adalah tipe baru arsitektur LAN yang menggunakan *switch* cerdas berkecepatan tinggi. Tidak seperti jenis LAN biasa yang secara fisik menghubungkan komputer ke segmen LAN, VLAN menetapkan komputer ke segmen LAN oleh perangkat lunak. VLAN telah distandarkan sebagai IEEE802.1q dan IEEE802.1p (Tarkaa, Iannah, & Iber, 2017).

Beberapa keuntungan penggunaan VLAN antara lain:

a. Keamanan pada jaringan. Keamanan pada sebuah jaringan dapat dilakukan dalam bentuk pemisahan terhadap segmentasi jaringan secara logika.
b. Penghematan anggaran. Penghematan dari penggunaan *bandwidth* yang ada dan dari *upgrade* perluasan *network* yang bisa jadi mahal.
c. Meningkatnya kemampuan jaringan. Pembagian jaringan *layer* 2 ke dalam beberapa kelompok *broadcast domain* yang lebih kecil, yang tentunya akan mengurangi lalu lintas paket yang tidak dibutuhkan dalam jaringan.
d. Memperkecil *Broadcast Domain*. Pembagian jaringan ke dalam VLAN akan mengurangi banyaknya *device* yang berpartisipasi dalam pembuatan *broadcast storm*. Hal ini terjadinya karena adanya pembatasan *broadcast domain*.

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

e. Lebih effisien dalam pengembangan dan pengelolaan teknologi jaringan. VLAN memudahkan manajemen jaringan karena pengguna yang membutuhkan sumber daya yang dibutuhkan terbagi dalam segmen yang sama.

5. *DHCP Server*

   DHCP Server adalah perangkat jaringan yang memiliki kemampuan dalam memberikan atau meminjamkan alamat IP pada Komputer *client* yang terhubung dalam sebuah jaringan sehingga Komputer dapat berkomunikasi. DHCP dapat membantu menghemat penggunaan alamat IP karena alamat IP tidak perlu lagi diberikan secara permanen pada masing-masing komputer *client*.

   DHCP Server berkerja di mana komputer *client* yang terhubung dalam sebuah jaringan melakukan permintaan *IP Address* pada komputer *server* DHCP yang memiliki persediaan alamat IP Komputer di dalam *database*-nya. Proses tersebut dikenal *DHCP DISCOVER*. Selanjutnya, *server* DHCP melakukan pengecekan pada *database* apakah masih tersedia alamat IP atau tidak. Jika alamat IP masih tersedia pada *database* maka komputer *server* DHCP memberikan informasi serta menawarkan pada komputer *client* yang minta alamat IP dan proses ini dikenal dengan *DHCP OFFER*. Proses selanjutnya komputer *client* menerima penawaran tersebut dari komputer *server* DHCP dengan meminta alamat yang ditawarkan tersebut untuk digunakan sebagai alamat IP komputernya proses ini dikenal dengan *DHCP REQUEST*. Proses terakhir adalah komputer *server* DHCP memindahkan alamat IP dari *database* komputer *server* DHCP ke komputer *client* sehingga komputer *client* diakui telah menggunakan alamat IP yang diberikan oleh komputer *server* DHCP, proses ini disebut *DHCPACK*.

6. Serangan pada Jaringan Komputer (BPPT, 2014)
   a. *Sniffer* adalah sebuah upaya yang dilakukan untuk menangkap atau mencuri data yang dikirim melalui jaringan komputer. Fungsi *sniffer* bagi pengelola bisa untuk memantau data yang sedang dikirim pada jaringan. *Packet Sniffing* adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.
   b. *Spoofing* (penyamaran) adalah upaya menyembunyikan atau memalsukan alamat komputer sehingga sistem akan kesulitan menentukan darimana komputer mentransmisikan data. *Spoofing* adalah teknik melakukan penyamaran sehingga terdeteksi sebagai identitas yang bukan sebenarnya

7. *DHCP Snooping*

   Komputer yang terhubung dalam jaringan akan mendapatkan alamat ip yang diberikan dari *server* DHCP sehingga komputer dapat berkomunikasi. DHCP *snooping* adalah fitur keamanan yang berfungsi seperti *firewall* di mana komputer yang terhubung dengan *server* DHCP akan mendapatkan alamat IP dari sumber yang terpercaya sedangkan sumber atau *server* DHCP yang tidak tepercaya tidak mendapat ijin untuk memberikan alamat IP yang dimiliki. DHCP *snooping* merupakan solusi yang tepat untuk mengatasi masalah keamanan jaringan yang lebih baik (Ariyadi, 2017).

8. *Cisco Packet Tracer*

   Cisco Packet Tracer adalah salah satu aplikasi yang dibuat oleh perusahaan Cisco yang berlokasi di San Francisco, California. Cisco didirikan pada tahun 1984. *Cisco Packet Tracer* sebagai alat simulasi yang digunakan dalam pembelajaran jaringan komputer khususnya produk Cisco. Dengan menggunakan aplikasi *cisco packet tracer*, simulasi data mengenai jaringan dapat dimanfaatkan menjadi informasi tentang keadaan koneksi suatu

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

komputer dalam suatu jaringan, apabila terjadi masalah dalam interkoneksi jaringan (Mufadhol, 2012).

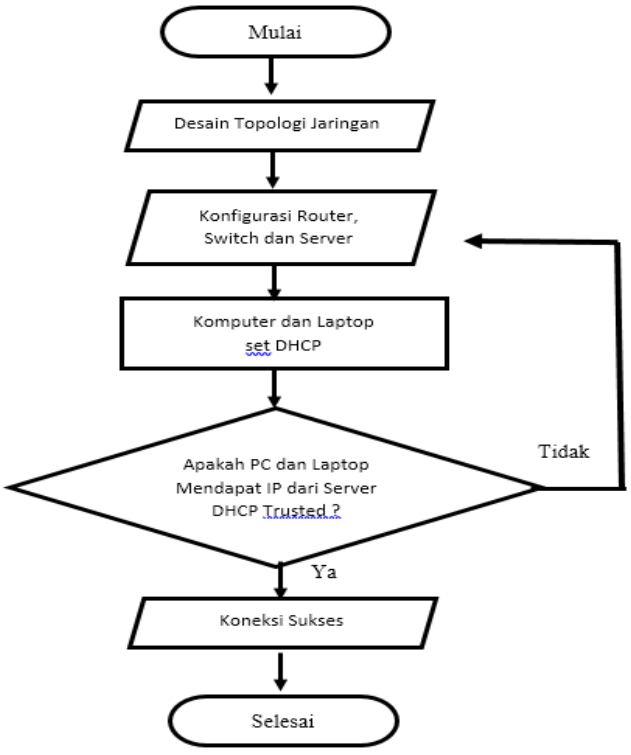
METODE

Metode penelitian yang digunakan terhadap penelitian tentang keamanan jaringan komputer dan internet dengan menggunakan *software* simulasi *Cisco Packet Tracer* 7.1. Adapun topologi yang digunakan dalam penelitian ini, peneliti akan menggunakan dua *router cisco* di mana *router* pertama sebagai *Server DHCP trusted*/yang dipercaya sedangkan yang lainnya sebagai pembanding yaitu *Server DHCP Untrusted*/tidak dipercaya, 1 unit *Access Point*, 2 unit *Server*, 4 unit PC, 9 unit Laptop dan 3 unit *Switch*.

Adapun langkah-langkah pengujian keamanan jaringan komputer menggunakan *DHCP Snooping* adalah sebagai berikut:

1. Mendesain topologi jaringan menggunakan *Software* Simulasi *Cisco Packet Tracer*.
2. Konfigurasi pada setiap *device* seperti pada *Router*, *Switch*, dan *Server*.
3. Analisis perbandingan penggunaan fungsi *DHCP Snooping* dan tanpa *DHCP Snooping*.
4. Pengujian konektifitas pada jaringan

Flowchart penelitian ditunjukkan oleh gambar berikut:

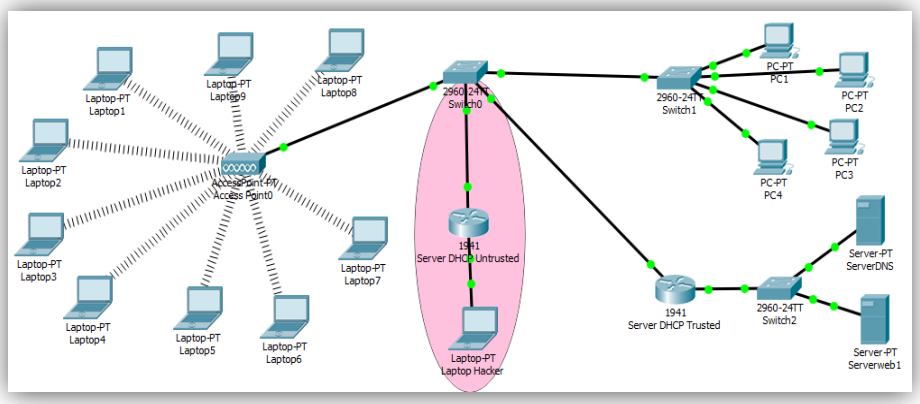


Gambar 4. *Flowchart* Penelitian

HASIL DAN PEMBAHASAN

Hasil dari perancangan jaringan komputer dapat dilihat pada Gambar 5 berikut, di mana *Switch* akan dikonfigurasi tanpa menggunakan *DHCP Snooping* dan VLAN.

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456



Gambar 5. Topologi Jaringan

Konfigurasi *Router* sebagai *Server DHCP Trusted* sebagai berikut:

Router>enable
Router#configure terminal
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface g0/1
Router(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp pool server_trusted
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#do wr

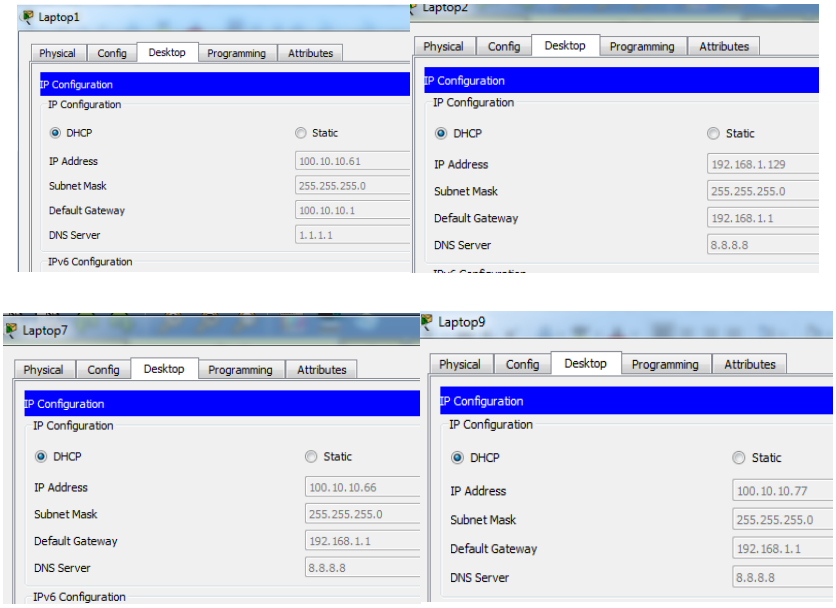
Konfigurasi *Router* sebagai *Server DHCP* Untrusted sebagai berikut:

Router>enable
Router#configure terminal
Router(config)#interface g0/0
Router(config-if)#ip address 100.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface g0/1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp pool server_untrusted
Router(dhcp-config)#network 100.10.10.0 255.255.255.0
Router(dhcp-config)#default-router 100.10.10.1
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#do wr

PC1 sampai dengan PC4 serta laptop1 sampai dengan laptop9 di-*setting IP Address* menggunakan DHCP. Hasil alamat IP pada masing-masing PC dan Laptop yang terhubung pada jaringan memiliki *IP Address* yang berbeda, sehingga ada beberapa komputer yang dapat terhubung dengan *server* dan ada beberapa yang gagal, dikarenakan adanya *Server* DHCP

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

Untrusted atau tidak dipercaya menyewakan alamat IP pada Komputer yang terhubung pada jaringan.



Gambar 6. Pengujian PC dengan DHCP *Server Untrusted*

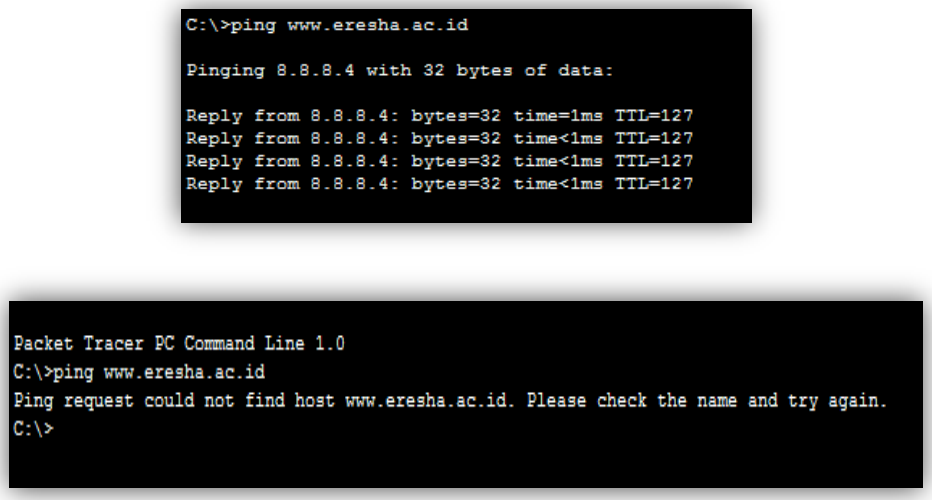
Tabel 1. *IP Address* Tanpa *DHCP Snooping*

Device	***Interface***	***IP address***	***Subnetmask***	***Gateway***	***Dns***
Server DHCP	Fa0/0	192.168.1.1	255.255.255.0		8.8.8.8
Trusted	Fa0/1	8.8.8.1	255.255.255.0		
Server DHCP	Fa0/0	100.10.10.1	255.255.255.0		1.1.1.1
Untrusted	Fa0/1	10.10.10.1	255.255.255.0		1.1.1.1
PC1		192.168.1.110	255.255.255.0	192.168.1.1	8.8.8.8
PC2		100.10.10.67	255.255.255.0	100.10.10.1	1.1.1.1
PC3		100.10.10.54	255.255.255.0	100.10.10.1	1.1.1.1
PC4		100.10.10.52	255.255.255.0	100.10.10.1	1.1.1.1
Laptop1		100.10.10.61	255.255.255.0	100.10.10.1	1.1.1.1
Laptop2		192.168.1.129	255.255.255.0	192.168.1.1	8.8.8.8
Laptop3		192.168.1.116	255.255.255.0	192.168.1.1	8.8.8.8
Laptop4		100.10.10.70	255.255.255.0	100.10.10.1	1.1.1.1
Laptop5		100.10.10.63	255.255.255.0	100.10.10.1	1.1.1.1
Laptop6		100.10.10.71	255.255.255.0	192.168.1.1	8.8.8.8
Laptop7		100.10.10.66	255.255.255.0	192.168.1.1	8.8.8.8
Laptop8		100.10.10.72	255.255.255.0	100.10.10.1	1.1.1.1
Laptop9		100.10.10.77	255.255.255.0	192.168.1.1	8.8.8.8

Pada tabel di atas tampak pada beberapa PC diantaranya PC1, Laptop 2 dan Laptop 3 mendapatkan *IP Address*, subnetmask dan *gateway* dari sumber yang terpercaya dan beberapa PC mendapatkan *IP Address*, subnetmask dan *gateway* dari sumber yang tidak dipercaya.

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

Pengujian koneksi dilakukan dari PC1 dengan hasil sukses dan PC2 dengan hasil tidak sukses.



Gambar 7. Pengujian koneksi ke *server* dengan tanpa *DHCP Snooping*

Hasil dari perancangan jaringan komputer dimana Switch akan dikonfigurasi menggunakan *DHCP Snooping* dan VLAN.

Konfigurasi Router sebagai *Server DHCP Trusted* sebagai berikut:
Router>enable
Router#configure terminal
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface g0/1
Router(config-if)#ip address 8.8.8.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp pool server_trusted
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp relay information trust-all
Router(config)#do write

Konfigurasi Router sebagai *Server DHCP Untrusted* sebagai berikut:
Router>enable
Router#configure terminal
Router(config)#interface g0/0
Router(config-if)#ip address 100.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#interface g0/1
Router(config-if)#ip address 10.10.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

Router(config)#ip dhcp pool server_untrusted
Router(dhcp-config)#network 100.10.10.0 255.255.255.0
Router(dhcp-config)#default-router 100.10.10.1
Rou (deriramdani, 2014)ter(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#do write

Konfigurasi pada *Switch*

Konfigurasi pada *Switch*0 dan *Switch*1 yaitu untuk melakukan filter terhadap *port* pada *switch* yang digunakan untuk membatasi penggunaan *server DHCP* yaitu menggunakan metode *DHCP Snooping*.

Langkah Membuat Vlan dengan id 10 dan nama *dhcp_snooping* pada *Switch*0 :

Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name dhcp_snooping
Switch(config)#int range fa0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch>enable
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#interface fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config)#int fa0/20
Switch(config-if)#ip dhcp snooping trust

Perintah di atas membuat VLAN id 10 dengan nama *dhcp_snooping* sedangkan *interface* mulai *FastEthernet*0/1-24 *mode acces* diubah menjadi VLAN 10.

Perintah IP *dhcp snooping* mengaktifkan *switch dhcp snooping* dan *interface FastEthernet*0/1 dan *FastEthernet*0/20 menjadi *port* yang dipercaya sebagai *DHCP_SERVER.*

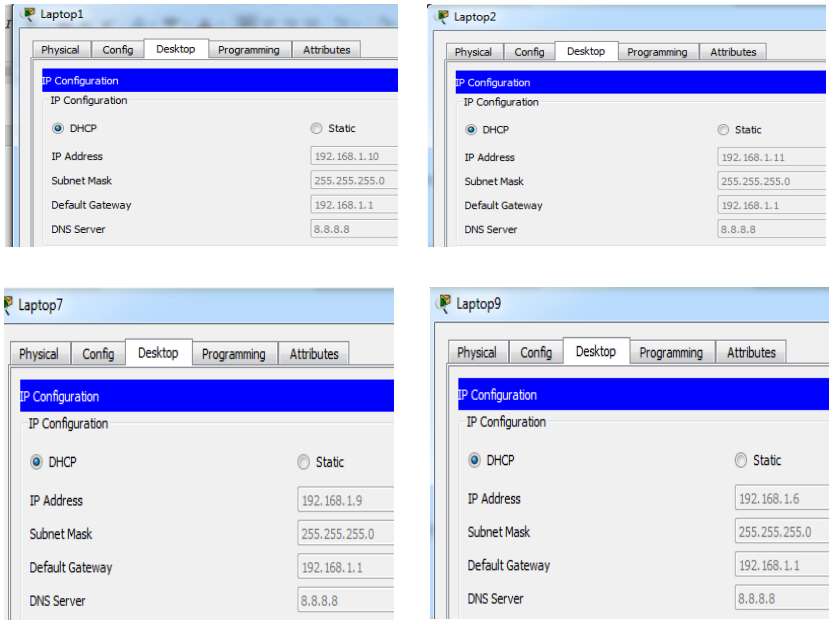
Membuat Vlan dengan id 10 dan nama *dhcp_snooping* pada *Switch*1:

Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name dhcp_snooping
Switch(config)#int range fa0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch>enable
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust

Perintah di atas membuat VLAN id 10 dengan nama *dhcp_snooping* sedangkan *interface FastEthernet*0/1-24 yaitu *port* yang tersedia pada *switch* mulai dari *port* 1 sampai dengan *port* 24 dirubah *mode acces* dari VLAN 1 dengan nama *default* menjadi VLAN 10 dengan nama *dhcp snooping.*

Perintah *IP dhcp snooping trust* pada *interface FastEthernet*0/1 adalah perintah untuk mengaktifkan *switch dhcp snooping* pada *port* atau *interface FastEthernet*0/1 menjadi *port* yang dipercaya sebagai *DHCP_SERVER*, sedangkan *port* selainnya tidak dapat digunakan untuk *Server DHCP*.

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456



Gambar 8. Pengujian PC dengan *DHCP Server Trusted*

Tabel 2. *IP Address* Menggunakan *DHCP Snooping*

Device	***Interface***	***IP address***	***Subnetmask***	***Gateway***	***Dns***
Server DHCP Trusted	Fa0/0 Fa0/1	192.168.1.1 8.8.8.1	255.255.255.0 255.255.255.0		8.8.8.8
Server DHCP Untrusted	Fa0/0 Fa0/1	100.10.10.1 10.10.10.1	255.255.255.0 255.255.255.0		1.1.1.1 1.1.1.1
PC1		192.168.1.2	255.255.255.0	192.168.1.1	8.8.8.8
PC2		192.168.1.5	255.255.255.0	192.168.1.1	8.8.8.8
PC3		192.168.1.3	255.255.255.0	192.168.1.1	8.8.8.8
PC4		192.168.1.4	255.255.255.0	192.168.1.1	8.8.8.8
Laptop1		192.168.1.10	255.255.255.0	192.168.1.1	8.8.8.8
Laptop2		192.168.1.11	255.255.255.0	192.168.1.1	8.8.8.8
Laptop3		192.168.1.7	255.255.255.0	192.168.1.1	8.8.8.8
Laptop4		192.168.1.14	255.255.255.0	192.168.1.1	8.8.8.8
Laptop5		192.168.1.12	255.255.255.0	192.168.1.1	8.8.8.8
Laptop6		192.168.1.15	255.255.255.0	192.168.1.1	8.8.8.8
Laptop7		192.168.1.9	255.255.255.0	192.168.1.1	8.8.8.8
Laptop8		192.168.1.8	255.255.255.0	192.168.1.1	8.8.8.8
Laptop9		192.168.1.6	255.255.255.0	192.168.1.1	8.8.8.8

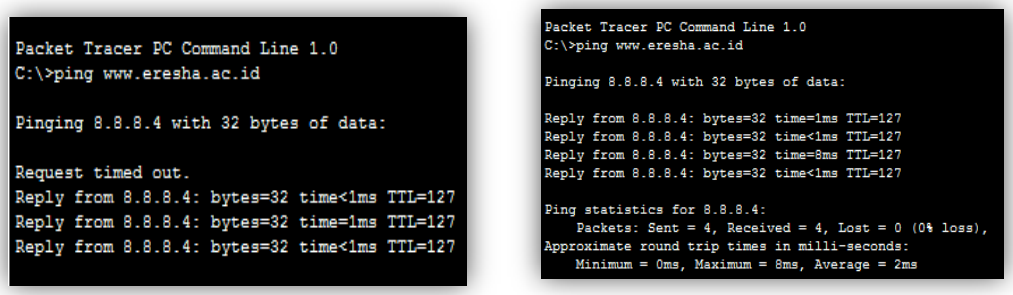
Pada tabel di atas tampak pada seluruh PC dan Laptop mendapatkan *IP Address*, *subnetmask* dan *gateway* dari sumber yang terpercaya sedangkan *Server DHCP Untrusted* tidak dapat memberikan *IP Address* dan *Gateway* pada komputer *client* yang terhubung pada jaringan.

Faktor Exacta *11 (2):* 167-178, 2018
p-ISSN: 1979-276X
e- ISSN: 2502-339X
DOI: 10.30998/faktorexacta.v11i2.2456

Tabel 3. Perbandingan *IP Address* Menggunakan *DHCP Snooping* dan Tanpa *DHCP Snooping*

Device	**Hasil *DHCP Snooping***			**Hasil Tanpa *DHCP Snooping***		
	IP address	***Gateway***	***DNS***	***IP address***	***Gateway***	***DNS***
PC1	192.168.1.2	192.168.1.1	8.8.8.8	192.168.1.110	192.168.1.1	8.8.8.8
PC2	192.168.1.5	192.168.1.1	8.8.8.8	100.10.10.67	100.10.10.1	1.1.1.1
PC3	192.168.1.3	192.168.1.1	8.8.8.8	100.10.10.54	100.10.10.1	1.1.1.1
PC4	192.168.1.4	192.168.1.1	8.8.8.8	100.10.10.52	100.10.10.1	1.1.1.1
Laptop1	192.168.1.10	192.168.1.1	8.8.8.8	100.10.10.61	100.10.10.1	1.1.1.1
Laptop2	192.168.1.11	192.168.1.1	8.8.8.8	192.168.1.129	192.168.1.1	8.8.8.8
Laptop3	192.168.1.7	192.168.1.1	8.8.8.8	192.168.1.116	192.168.1.1	8.8.8.8
Laptop4	192.168.1.14	192.168.1.1	8.8.8.8	100.10.10.70	100.10.10.1	1.1.1.1
Laptop5	192.168.1.12	192.168.1.1	8.8.8.8	100.10.10.63	100.10.10.1	1.1.1.1
Laptop6	192.168.1.15	192.168.1.1	8.8.8.8	100.10.10.71	192.168.1.1	8.8.8.8
Laptop7	192.168.1.9	192.168.1.1	8.8.8.8	100.10.10.66	192.168.1.1	8.8.8.8
Laptop8	192.168.1.8	192.168.1.1	8.8.8.8	100.10.10.72	100.10.10.1	1.1.1.1
Laptop9	192.168.1.6	192.168.1.1	8.8.8.8	100.10.10.77	192.168.1.1	8.8.8.8

Pengujian dilakukan dari PC1 dan PC2 menggunakan *DHCP Snooping* dengan hasil Sukses.



Gambar 9. Pengujian koneksi ke *server* dengan *DHCP Snooping*

PENUTUP

Simpulan

Berdasarkan uji coba implementasi secara simulasi dengan menggunakan *software cisco packet tracer* 7.1 maka dapat disimpulkan:

1. *DHCP Snooping* dapat memfilter dan memvalidasi terhadap *port* yang terpercaya dan yang tidak dipercaya.
2. Dengan menggunakan *DHCP Snooping* jaringan komputer akan lebih aman tidak terganggu dengan adanya *server* DHCP yang lain atau palsu.
3. VLAN dapat menghubungkan jaringan berdasarkan VLAN ID atau *Group* sehingga Komputer yang bukan *Group* tidak dapat terhubung dalam sebuah jaringan.

Saran

DHCP Snooping merupakan teknik dasar dalam keamanan pada jaringan komputer dan *internet*, untuk pengembangan lebih lanjut dapat di analisis tentang keamanan yang lebih besar

seperti kombinasi *DHCP Snooping*, VLAN, ACL dan *DHCP starvation* agar lebih memperkuat keamanan jaringan.

DAFTAR PUSTAKA

Ariyadi, T. (2017). Desain Keamanan DHCP Snooping untuk Mengurangi Serangan. *JUSIKOM, Vol 2, No. 1, Juni*, 28-36.

BPPT, C. . (2014). *Panduan Penanganan Insiden Keamanan Jaringan.* Indonesia: CSIRT - Badan Pengkajian dan Penerapan Teknologi.

Deriramdani. (2014, november 22). *http://blog.umy.ac.id*. Retrieved from http://blog.umy.ac.id.

Mufadhol. (2012). Simulasi Jaringan Komputer Menggunakan Cisco Packet Tracer. *JURNAL TRANSFORMATIKA, Volume, No. 2, Januari* , 64-71.

Prasetiono, S. J. (2010). Teknik Keamanan Access Point pada Jaringan Nirkabel . *Majalah Ilmiah IC Tech Vol 5 No 1Januari*, 17-22.

Sofana, I. (2009). *CISCO CCNA dan Jaringan Komputer*. Bandung: Informatika.

Sulaiman, O. K. (2016). Analisis Sistem Keamanan Jaringan dengan Menggunakan Switch Port Security. *CESS (Journal Of Computer Engineering, System And Science) Vol 1, No 1, Januari* , 9-14.

Tarkaa, N. S., Iannah, P. I., & Iber, I. T. (2017). Design and Simulation of Local Area Network Using Cisco Packet Tracer. *The International Journal of Engineering and Science (IJES) Volume 6 Issue 10* , 63- 77.