KEAMANAN JARINGAN SISTEM PENCEGAHAN SERANGAN DHCP *ROGUE* DENGAN DHCP *SNOOPING*

PROJEK

Sebagai salah satu syarat untuk menyelesaikan studi di
Program Studi Teknik Komputer DIII

Oleh

ALFINA WIJAYANTI
NIM 09040581822013

PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
JULI 2021

HALAMAN PENGESAHAN

KEAMANAN JARINGAN SISTEM PENCEGAHAN SERANGAN DHCP *ROGUE* DENGAN DHCP *SNOOPING*

PROJEK
Sebagai salah satu syarat untuk menyelesaikan studi di
Program Studi Teknik Komputer DIII

Oleh

ALFINA WIJAYANTI
NIM 09040581822013

Palembang, 26 Juli 2021

Pembimbing I,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Tri Wanda Septian, M.Sc.**
NIP 198701222015041002	**NIK 1901062809890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari **: Kamis**

Tanggal **: 01 Juli 2021**

Tim Penguji :

1. Ketua : Huda Ubaya, M.T. _____
2. Pembimbing I : Ahmad Heryanto, M.T. _____
3. Pembimbing II : Tri Wanda Septian, M.Sc. _____
4. Penguji : Adi Hermansyah, M.T. _____

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	:	Alfina Wijayanti
NIM	:	09040581822013
Program Studi	:	Teknik Komputer
Jenjang	:	DIII
Judul Projek	:	Keamanan Jaringan Sistem Pencegahan Serangan DHCP *Rogue* dengan DHCP *Snooping*
Hasil Pengecekan Software *iThenticate/Turnitin*	:	13 %

Menyatakan bahwa Laporan Projek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan projek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 26 Juli 2021

Alfina Wijayanti
NIM 09040581822013

HALAMAN PERSEMBAHAN

"Pejuang Tugas Akhir"

Malam hening sepi senyap mengulas memori

Lembut gemulai jemari merangkai kata

Sayup redup mata yang hendak tertutup

Menemui pekat malam makin terbelalak

Secangkir kopi pendamping rasa

Dinginnya malam membawa kedamaian

Pikirku hanya pada tinta hitam di layar itu

Buatku semakin dalam memasukinya

Secercah goresan kata yang berbaris indah

Di ukir pada penghujung malam hingga fajar

Pesona malam selalu menjadi teman ramah

Semilir angin malam bawa ke alam memori

Tak begitu mudah untuk ku gapai

Begitu banyak jalan yang terjal kuhadapi

Jatuh lalu bangkit kembali itu hal yang sudah biasa

Ya, begitulah…

Sebuah perjuangan pasti dilalui proses yang mahal

Juli 2021

KATA PENGANTAR

Segala puji dan syukur atas kehadiran Allah SWT, karena berkat rahmat dan karunia-Nyalah penulis dapat menyelesaikan penulisan projek aknir ini dengan judul "Keamanan Jaringan Sistem Pencegahan Serangan DHCP *Rogue* dengan DHCP *Snooping*".

Pada kesempatan ini, penulis mengucapkan terima kasih kepada semua pihak yang telah membantu, membimbing, dan terus mendukung penulis dalam menyelesaikan projek akhir ini di antaranya:

1. Allah SWT yang telah memberikan hamba kesehatan, kemudahan, dan kelancaran sehingga hamba dapat menyelesaikan laporan projek akhir sebagai seorang mahasiswa.
2. Kedua orang tua serta keluarga yang telah memberikan dukungan dan do'a untuk kelancaran penyelesaian laporan projek akhir ini.
3. Bapak Huda Ubaya, M.T. selaku Koordinator Program Studi Teknik Komputer Universitas Sriwijaya.
4. Bapak Ahmad Heryanto, M.T. dan Bapak Tri Wanda Septian, M.Sc. selaku Dosen Pembimbing I dan II projek akhir, yang telah memberikan bimbingan, arahan dan semangat kepada penulis dalam menyelesaikan projek akhir.
5. Bapak Kemahyanto Exaudi, S.Kom., M.T. selaku Dosen Pembimbing Akademik, yang telah membimbing penulis dari semester tiga hingga terselesaikannya projek akhir ini dengan baik.
6. Bapak Adi Hermansyah, M.T. selaku Dosen Penguji sidang projek akhir yang telah memberikan kritik dan saran serta ilmu yang sangat bermanfaat sehingga

tulisan ini menjadi lebih baik.

7. Seluruh Dosen Program Studi Teknik Komputer, Fakultas Ilmu Komputer serta Universitas Sriwijaya.
8. Staff di Program Studi Teknik Komputer, khususnya Mba Faula yang telah membantu penyelesaian proses administrasi.
9. Teruntuk teman-teman satu angkatan, khususnya Teknik Komputer Jaringan 2018. Semoga sukses dan sehat untuk kita semua.
10. Amalia Cahya Fitri dan Nur Vita Syakbaini Putri selaku sahabat yang selalu bersama penulis dalam menyemangati dan mendukung penulis.
11. Dwi Okta Sulistiani selaku teman seperjuangan dari semester 1 hingga semester 6 selalu bersama melewati suka maupun duka dan selalu menyemangati satu sama lain.
12. Serta Organisasi di Fakultas Ilmu Komputer Universitas Sriwijaya, DPM KM dan LDF WIFI. Terima kasih atas kesempatannya sehingga menjadi bagian keluarga besar serta ilmu yang telah diberikan semoga bermanfaat sampai kapanpun.

Akhir kata penulis berharap semoga laporan projek akhir ini dapat bermanfaat bagi pembaca khususnya Mahasiswa Program Studi Teknik Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Semoga laporan projek akhir ini menjadi lebih baik di masa mendatang. Terima Kasih.

Palembang, 26 Juli 2021

Penulis

KEAMANAN JARINGAN SISTEM PENCEGAHAN SERANGAN DHCP *ROGUE* DENGAN DHCP *SNOOPING*

Oleh

ALFINA WIJAYANTI
NIM 09040581822013

Abstrak

Fokus penelitian ini adalah melindungi jaringan dari DHCP *Rogue* (*server* DHCP palsu), dengan implementasi DHCP *Snooping* dan VLAN pada salah satu perangkat jaringan yaitu *switch*. Jaringan yang dibangun pada penelitian ini memiliki dua *router* di mana *router* sah yang memberikan alamat IP yang benar ke *client* dan *router hacker* yang memberikan alamat IP yang salah ke *client*, dan *client* akan tertipu. Dan satu laptop sebagai *client* yang menerima alamat IP dengan menggunakan kabel UTP + kabel USB *to serial*. Pada penelitian ini dilakukan dua skenario pengecekan: (1) pengecekan pertama pada alamat IP sebelum implementasi DHCP *Snooping* dan VLAN, dan (2) pengecekan kedua pada alamat IP setelah DHCP *Rogue* aktif. Hasil yang diperoleh dari penelitian : *client* mendapatkan alamat IP dari *server* DHCP yang sah, setelah melakukan implementasi DHCP *Snooping* dan VLAN *port* jauh lebih aman.
Kata Kunci: Keamanan jaringan, DHCP *Snooping*, *Virtual Local Area Network* (VLAN)

Palembang, 26 Juli 2021

Pembimbing I,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Tri Wanda Septian, M.Sc.**
NIP 198701222015041002	**NIK 1901062809890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

NETWORK SAFETY DHCP ROGUE ATTACK PREVENTION SYSTEM WITH DHCP SNOOPING

By

ALFINA WIJAYANTI
NIM 09040581822013

Abstract

The focus of this research is to protect the network from DHCP Rogue (fake DHCP server), by implementing DHCP Snooping and VLAN on one of the network devices, namely a switch. The network built in this study has two routers where a legitimate router that gives the correct IP address to the client and a hacker router that gives the wrong IP address to the client, and the client will be tricked. And a laptop as a client that receives an IP address using a UTP cable, a USB to serial cable. In this study, two checking scenarios were carried out: (1) checking the first IP address before implementing DHCP Snooping and VLAN, and (2) checking the second on the IP address after DHCP Rogue is active. The results obtained from the research: the client gets an IP address from a valid DHCP server, after implementing DHCP Snooping and the VLAN port is much safer.
Keyword: Network security, DHCP Snooping, Virtual Local Area Network (VLAN)

Palembang, 26 Juli 2021

Pembimbing I,	**Pembimbing II,**
Ahmad Heryanto, M.T.	**Tri Wanda Septian, M.Sc.**
NIP 198701222015041002	**NIK 1901062809890001**

Mengetahui

Koordinator Program Studi Teknik Komputer,

Huda Ubaya, M.T.
NIP 198106162012121003

DAFTAR ISI

Halaman

DAFTAR SIMBOL

DOS	=	*Denial of Servicce*
TCP	=	*Transmission Control Protocol*
WEB	=	*Website*
IDS	=	*Intruder Detection System*
IDCERT	=	*Indonesia Computer Emergency Response Team*
DHCP	=	*Dynamic Host Configuration Protocol*
IP Address	=	*Internet Protocol Address*
ACK	=	*Acknowledgement*
LOG	=	*Logging*
LPR	=	*Line Printer Requester*
MTU	=	*Maximum Transmission Unit*
ARP	=	*Address Resolution Protocol*
TTL	=	*Time to Live*
NETBIOS	=	*Network Basic Input/Output System*
SMTP	=	*Simple Mail Transfer Protocol*
POP3	=	*Post Office Protocol 3*
NNTP	=	*Network News Transport Protocol*
WWW	=	*World Wide Web*
IRC	=	*Internet Relay Chat*
STDA	=	*Streettalk Directory Assistance*
TFTP	=	*Trivial File Transfer Protocol*

VLAN	=	*Virtual Local Area Network*
MAC	=	*Macintosh Operating System*
VMPS	=	*Vlan Management Policy Server*
NIC	=	*Network Interface Card*
ISDN	=	*Integrated Services Digital Network*
PPP	=	*Point to Point Protocol*
RAM	=	*Random Access Memory*
ROM	=	*Read Only Memory*
CPU	=	*Central Processing Unit*
NVRAM	=	*Non-Volatile Random Access Memory*
IOS	=	*Iphone Operating System*
UTP	=	*Unshielded Twisted Pair*
USB	=	*Universial Serial Bus*
PLC	=	*Programmable Logic Controllers*

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

Halaman

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan komputer adalah teknik deteksi dan pencegahan terhadap aktivitas yang mengganggu sistem komputer (Gollmann, Dieter, 1999). Banyak upaya yang dilakukan untuk memberikan proteksi terhadap serangan pengguna komputer salah satunya menggunakan DHCP *Snooping* yang merupakan fitur keamanan pada *layer* 2.

Saat membangun sistem jaringan berbasis *internet*, masalah keamanan sangat penting [1]. Keamanan jaringan komputer mencakup banyak aspek, mulai dari melindungi perangkat fisik (seperti perangkat keras), mengakses sumber daya jaringan, melindungi data dan informasi di jaringan, hingga mencegah pencurian data [2].

Studi kasus pencurian/penipuan untuk bank Indonesia dan Malaysia. Sebagian besar kasus yang dilaporkan ke ID-CERT terkait pencurian/penipuan adalah situs *web* perbankan palsu di Indonesia yang dibuat menyerupai situs aslinya. Biasanya situs palsu menggunakan nama *domain* yang sama (.com dan .net). Untuk bank dengan nama *domain* .co.id, laporan jarang diterima. Hal yang sama juga terjadi pada situs-situs perbankan di Malaysia dan Eropa. Situs-situs ini dipalsukan dan diposting di situs *web* Indonesia dan alamat IP organisasi [3].

Penelitian yang berjudul Simulasi Keamanan Jaringan dengan Metode DHCP *Snooping* dan VLAN (Miftah, Zaeni, 2018). Penelitian ini menjelaskan tentang keamanan jaringan komputer di lingkungan STMIK Eresha yang masih memiliki kekurangan karena memberikan akses jaringan hanya melalui DHCP *server*. Hal

ini dapat menyebabkan serangan dalam bentuk DHCP *Rogue* di mana *server* DHCP palsu memberikan alamat *gateway* yang salah ke komputer klien, mencegah komputer terhubung ke jaringan dan *internet*.

Berdasarkan uraian latar belakang tersebut maka penulis bermaksud untuk melakukan penelitian dengan mengajukan kasus di atas sebagai judul pada tugas akhir dengan judul "**Keamanan Jaringan Sistem Pencegahan Serangan DHCP *Rogue* dengan DHCP *Snooping***".

1.2 Tujuan

Adapun tujuan yang ingin dicapai dari penelitian projek akhir ini, di antaranya sebagai berikut:

1. Melindungi dan membatasi lalu lintas jaringan DHCP dari DHCP *Rogue* atau DHCP *server* palsu terhadap sumber yang terpercaya dan yang tidak terpercaya.
2. Menghubungkan jaringan berdasarkan kelompok atau grup dalam satu *network*.

1.3 Manfaat

Berikut manfaat yang diharapkan penulis dalam penelitian projek akhir ini adalah sebagai berikut:

1. Jaringan komputer akan lebih aman terhindar dari DHCP *server* palsu.
2. Mengurangi kemungkinan terjadinya penyalahgunaan hak akses suatu data.

1.4 Batasan Masalah

Batasan masalah dalam tugas akhir ini adalah sebagai berikut:

1. Proses konfigurasi DHCP *Snooping* dan VLAN.
2. Perangkat keras dan perangkat lunak yang akan digunakan yaitu *router cisco*, *switch cisco*, kabel UTP jenis *straight*, *console*, kabel USB *to Serial*, laptop/komputer, *putty*, *wireshark* serta *wifi*.
3. Mengimplementasikan DHCP *Server* pada *router cisco* dan mengimplementasikan DHCP *Snooping* dan VLAN pada *switch cisco*.
4. Pengujian sistem keamanan dilakukan secara *real time*.
5. Hasil yang diinginkan penulis adalah *client* mendapatkan alamat IP dari DHCP *server* yang asli.

1.5 Metode Penelitian

Agar penelitian ini tercapai tujuannya, metode yang digunakan penulis terdapat beberapa tahapan metode, di antaranya adalah sebagai berikut:

1. Waktu dan Tempat Penelitian

Proses penelitian dilakukan di Laboratorium Jaringan Komputer Fakultas Ilmu Komputer Palembang Universitas Sriwijaya. Ini akan berlangsung sekitar 4 (empat) bulan mulai dari Maret 2021 s.d. Juni 2021.

2. Alat dan Bahan

Alat dan bahan yang akan digunakan penulis dalam pembuatan sistem pencegahan DHCP *Rogue* ini adalah *router cisco*, *switch cisco*, kabel UTP jenis *straight*, *console*, kabel USB *to Serial*, laptop/komputer, *putty*, *wireshark* serta *wifi*.

3. Teknik Pengumpulan Data

Studi Pustaka, metode ini dilakukan dengan cara meninjau dan meneliti literatur dan bahan referensi berupa jurnal, *paper* dan naskah ilmiah lainnya, serta *browsing internet* untuk mencari artikel yang berhubungan langsung dengan judul tugas akhir ini. Observasi Metode ini mengamati pengujian sistem secara *real time*, sehingga diperoleh data hasil pengujian yang memenuhi batas masalah yang telah ditetapkan untuk memperoleh hasil yang terbaik.

4. Metodologi Pengembangan Sistem

Membahas skenario-skenario apa yang akan dilakukan seperti menentukan topologi apa yang akan sesuai, menentukan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang diperlukan untuk mendukung sistem keamanan, serta metode keamanan jaringan yang digunakan untuk diimplementasikan.

DAFTAR PUSTAKA

[1] Hasibuan, Muhammad Siddik, "Keylogger pada Aspek Keamanan Komputer," *Teknovasi*, vol. 3, no. 1, pp. 8–15, 2016.

[2] Miftah, Zaeni, "Simulasi Keamanan Jaringan Dengan Metode Dhcp Snooping Dan Vlan," *Fakt. Exacta*, vol. 11, no. 2, pp. 167–178, 2018, doi: 10.30998/faktorexacta.v11i2.2456.

[3] Rachman, Derry Alif, M. Decky N dan Galih Kazaruni, "Keamanan Sistem Informasi (Studi: Spoofing)," 2014.

[4] Erlando, Rinto, Diana dan Maria Ulfa, "Penerapan Sistem Keamanan Firewall Pada Router Cisco 1841 Dan Monowall Pada Sistem Operasi Bsd (Berkeley Software Distribution)," pp. 236–243, 2020.

[5] Sohibi, Ahmad, "Analisa Jaringan Komputer Local Area Network pada Kantor Indonesia untuk Kemanusiaan Jakarta," vol. 1–78, 2017.

[6] Hidayatullah, dkk, "Bab II Landasan Teori," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 7–24, 2018.

[7] B. CSIRT, "Panduan Penanganan Insiden Keamanan Jaringan," pp. 1–49, 2014.

[8] Manginsela, Antonius P.G, "Ancaman & Insiden Keamanan Jaringan Komputer Topik Bahasan," *Tek. Elektro*, no. 2, 2015.

[9] Simanjuntak, Nurcahaya, "Analisa dan Perancangan Keamanan Jaringan Wireless dari Serangan Man In The Middle Attack Menggunakan Mikrotik Wireless," pp. 8–34, 2019.

[10] Tahir, Heri dan Riskawati, "Penanganan Kasus Cyber Crime Di Kota

Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar),” *J. Pemikiran, Penelit. Hukum, Pendidik. Pancasila dan Kewarganegaraan*, vol. 3, no. 2, pp. 93–103, 2016.

[11] Antoni, “Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online,” *Nurani J. Kaji. Syari’ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018, doi: 10.19109/nurani.v17i2.1192.

[12] Enggarani, Nuria Siswi, “Penanggulangan kejahatan internet di indonesia,” vol. 15, no. 2, pp. 149–168, 2012.

[13] Arifah, Dista Amalia, “Kasus Cybercrime Di Indonesia,” *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.

[14] Setia, Muji, “Pengertian DHCP Server,” pp. 1–6, 2019.

[15] Muttaqin, Zakaria, “Pengembangan Modul Gns3 Sebagai Media Pembelajaran Untuk Meningkatkan Kemampuan Siswa Dalam Konfigurasi Dhcp Server Pada Mata Pelajaran Administrasi Sistem Jaringan,” *It-Edu*, vol. 3, no. 01, pp. 159–165, 2018.

[16] Syarifudin, Akhmad, “Konfigurasi DHCP Server,” *Fak. Komput.*, pp. 1–22, 2020.

[17] Chandra, Iwan, “Media Iklan Berbasus WEB Lokal Dengan Pemanfaatan Segmentasi Jaringan Pada Local Area Nework,” *IDeaTech*, no. Jaringan, pp. 1–8, 2015.

[18] S. Alexander and R. Droms, “DHCP Options and BOOTP Vendor Extensions,” *Req. Comments*, pp. 1–34, 1997.

[19] Younes, Osama S., “A Secure DHCP Protocol to Mitigate LAN Attacks,” *J. Comput. Commun.*, vol. 04, no. 01, pp. 39–50, 2016, doi:

10.4236/jcc.2016.41005.

[20] Bayu, Teguh Indra dan Nurhanif, "Model Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue," *Indones. J. Comput. Model.*, vol. 1, no. 2, pp. 55–60, 2018, doi: 10.24246/j.icm.2018.v1.i2.p55-60.

[21] Adenam, Muhammad Idham Hilman bin, "DHCP Snooping," [Online]. Available:https://docplayer.info/50235478-Dhcp-snooping-penulis-muhammad-idham-hilman-bin-adenam-jawatan-penolong-pegawai-teknologi-maklumat-bahagian-unit-rangkaian-telekomunikasi.html.

[22] Putra, Aldea Alfian Pertama, "Analisa Vlan (Virtual Local Area Network) Pada Head Office Pt. Pandu Siwi Sentosa Jakarta," *AMIK BSI Jakarta*, 2017.

[23] Micro, Andi, "Dasar-Dasar Jaringan Komputer," pp. 1–207, 2012.

[24] Nugroho, Kukuh, "Analisis Penggunaan Tipe Pengkabelan Crossover Pada Gigabit-Ethernet," *Semin. Nas. Inov. dan Tren*, pp. 38–42, 2015.

[25] Syafriadi, M, "Rancang Bangun Alat Pendeteksi Warna Menggunakan Kamera Dan Output Suara Berbasis Komputer," *Politek. NEGERI Sriwij.*, pp. 3–20, Nov. 2017.

[26] Putri, Desinta Ningrum Belsa, "Membangun Jaringan Klien Server File Dan Direktori Sharing Menggunakan Samba." 2010.

[27] Cisco, "Connecting a Terminal to the Console Port on Catalyst Switches," *Cisco*, pp. 1–19, 2005.

[28] Razaque, Abdul dan Khaled Elleithy, "Controlling Attacks of Rogue Dynamic Host Configuration Protocol (DHCP) to Improve Pedagogical Activities in Mobile Collaborative Learning (MCL) Environment," *J.*

Commun. Comput. Eng., vol. 3, no. 1, p. 15, 2012, doi: 10.20454/jcce.2013.426.

[29] Kadafi, Muamar dan Khusnawi, "Analisis Rogue DHCP Packets Menggunakan Wireshark Network Protocol Analyzer," *Creat. Inf. Technol. J.*, vol. 2, no. 2, p. 165, 2015, doi: 10.24076/citec.2015v2i2.46.