

**ANALISIS SERANGAN *MAN IN THE MIDDLE* SEBAGAI *ROGUE*  
DHCP SERVER MENGGUNAKAN WIRESHARK**

**SKRIPSI**



disusun oleh

**Ariyo Pratomo**

**14.11.7684**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**ANALISIS SERANGAN *MAN IN THE MIDDLE* SEBAGAI *ROGUE*  
DHCP *SERVER* MENGGUNAKAN WIRESHARK**

**SKRIPSI**

untuk memenuhi sebagian persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Ariyo Pratomo**

**14.11.7684**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA  
2018**

**PERSETUJUAN**

**SKRIPSI**

**ANALISIS SERANGAN *MAN IN THE MIDDLE* SEBAGAI *ROGUE*  
DHCP *SERVER* MENGGUNAKAN WIRESHARK**

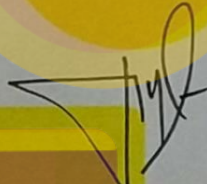
yang dipersiapkan dan disusun oleh

**Ariyo Pratomo**

**14.11.7684**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 27 Maret 2017

**Dosen Pembimbing**



**Joko Dwi Santoso, M.Kom**

**NIK. 190302181**

# PENGESAHAN

## SKRIPSI

### ANALISIS SERANGAN *MAN IN THE MIDDLE* SEBAGAI *ROGUE* DHCP SERVER MENGGUNAKAN WIRESHARK

yang dipersiapkan dan disusun oleh

**Ariyo Pratomo**  
14.11.7684

telah dipertahankan di depan Dewan Penguji  
pada tanggal 23 Agustus 2018

#### Susunan Dewan Penguji

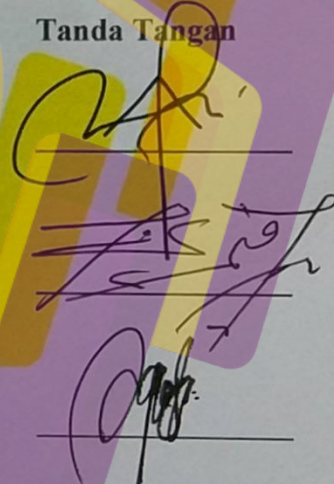
**Nama Penguji**

**Tanda Tangan**

Andi Sunyoto, M.Kom  
NIK. 190302052

Ferry Wahyu Wibowo, S.Si., M.Cs  
NIK. 190302235

Agus Fatkhurohman, M.Kom  
NIK. 190302249



Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
30 Agustus 2018

**DEKAN FAKULTAS ILMU KOMPUTER**



Krisnawati, S.Si, M.T.  
NIK. 190302038

## PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 30 Agustus 2018

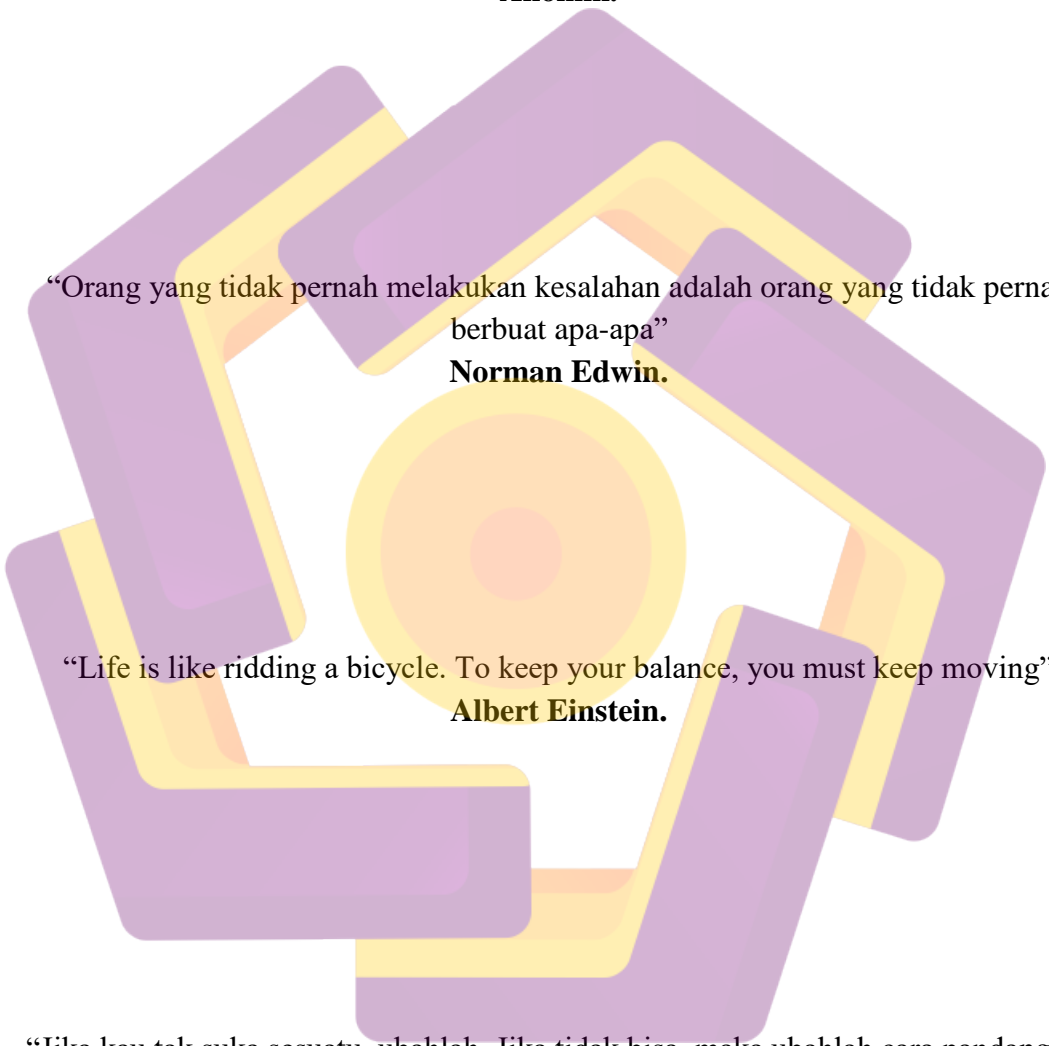


Ariyo Pratomo  
NIM. 14.11.7684

## MOTTO

“Pandanglah segala sesuatu dari kaca mata orang lain. Apabila hal itu menyakitkan hatimu, sangat mungkin hal itupun menyakitkan hatinya”

**Anonim.**



“Orang yang tidak pernah melakukan kesalahan adalah orang yang tidak pernah berbuat apa-apa”

**Norman Edwin.**

“Life is like ridding a bicycle. To keep your balance, you must keep moving”

**Albert Einstein.**

“Jika kau tak suka sesuatu, ubahlah. Jika tidak bisa, maka ubahlah cara pandangmu tentangnya”

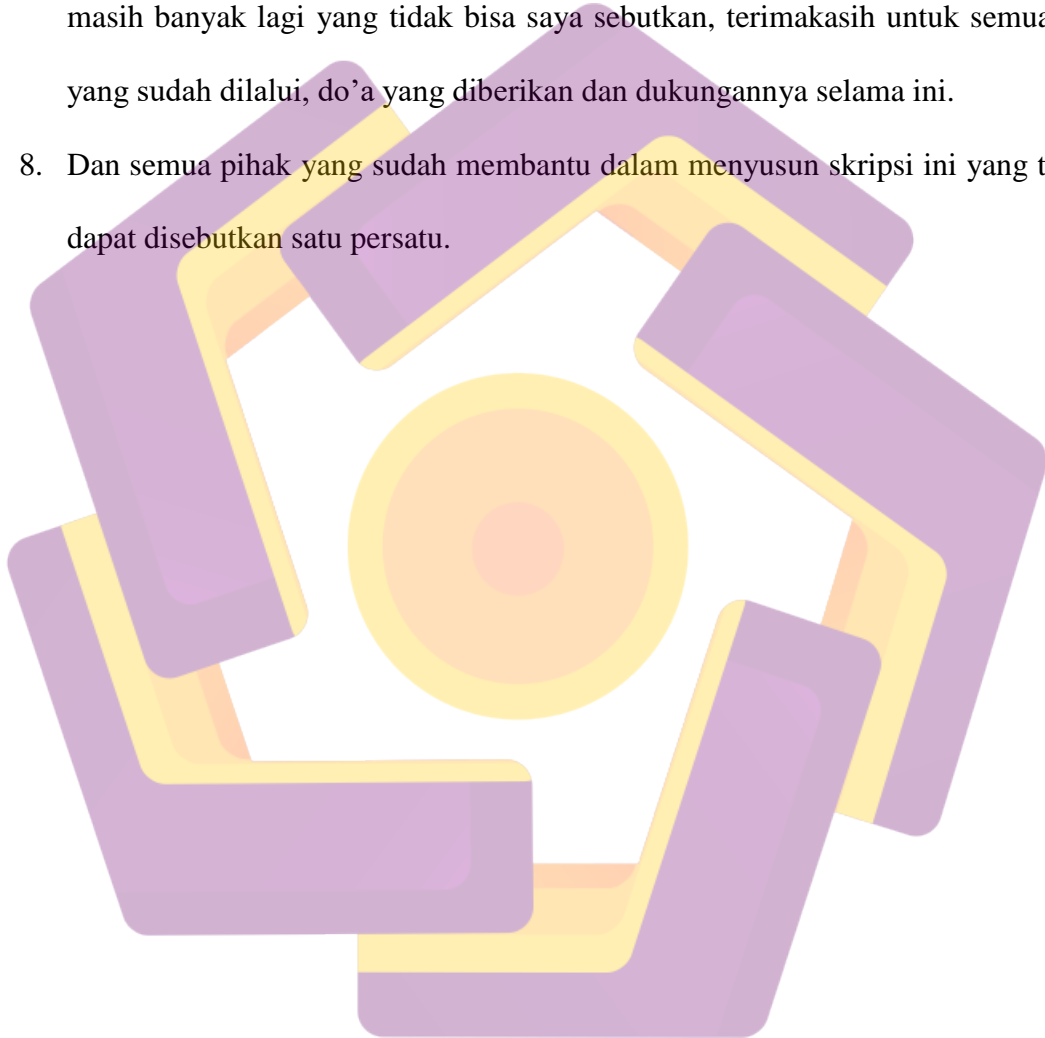
**Maya Angelou.**

## PERSEMBAHAN

Dengan mengucapkan puji dan syukur kehadirat Allah SWT, yang telah melimpahkan rahmat serta karunia-Nya sehingga skripsi ini dapat terselesaikan dengan lancar, baik dan kedepannya dapat bermanfaat. Skripsi ini penulis persembahkan untuk:

1. Kedua orang tua yang sangat saya sangat amat cintai, Bapak Tumaryo dan Ibu Tutik Rahayu atas limpahan do'a yang tiada hentinya, kasih sayang sepanjang masanya dan pengorbanan yang sampai tak terhingga jumlahnya.
2. Simbah saya yaitu Simbah Tukirah yang sangat saya cintai, terimakasih atas kesabarannya mengurus saya selama berada di Yogyakarta dan memberikan banyak nasihat-nasihat yang sangat berguna untuk kehidupan saya dimasa mendatang.
3. Bapak Joko Dwi Santoso selaku dosen pembimbing, terimakasih atas bimbingannya sehingga saya dapat menyelesaikan skripsi ini dengan baik dan lancar.
4. Bapak Andi Sunyoto, Bapak Ferry Wahyu Wibowo dan Bapak Agus Fatkhurohman selaku dosen penguji, terimakasih atas saran untuk pengembangan skripsi ini.
5. Bapak dan Ibu Dosen Universitas AMIKOM Yogyakarta yang telah memberi banyak sekali ilmu yang sangat bermanfaat pada waktu perkuliahan.

6. Teman-teman 14-S1TI-02, terimakasih untuk waktu yang sangat menyenangkan dan mengesankan baik didalam kelas maupun diluar kelas. Semoga kita semua dimudahkan dan dilancarkan untuk kedepannya.
7. Untuk Riansyah, Yuda, Rico, Arief, Samuel, Erwin, Joko, Imam dan Azhar serta masih banyak lagi yang tidak bisa saya sebutkan, terimakasih untuk semua hal yang sudah dilalui, do'a yang diberikan dan dukungannya selama ini.
8. Dan semua pihak yang sudah membantu dalam menyusun skripsi ini yang tidak dapat disebutkan satu persatu.





## KATA PENGANTAR

Assalamu alaikum wr.wb

Alhamdulillah, puji dan syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi yang berjudul “Analisis Serangan *Man In the Middle* Sebagai *Rogue DHCP Server* Menggunakan Wireshark” dengan lancar dan baik. Tak lupa sholawat serta salam kepada junjungan Nabi besar Muhammad SAW yang telah mengajarkan ilmu-ilmu Agama Islam sehingga dapat menjadi bekal dalam menjalani kehidupan sekarang dan pada akhirat.

Pada kesempatan ini penulis berterimakasih atas bimbingan, dukungan, bantuan, serta do'a kepada semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini, khususnya kepada:

1. Allah SWT atas limpahan rahmat, hidayah dan nikmat dalam kehidupan.
2. Nabi Muhammad SAW sebagai suri tauladan bagi umat-Nya.
3. Bapak Tumaryo dan Ibu Tutik Rahayu yang tercinta atas segala dukungan, do'a, dan nasihat sehingga penulis dapat menyelesaikan skripsi ini.
4. Simbah Tukirah yang tercinta atas segala kesabaran, nasihat dan dukungannya.
5. Bapak Prof. Dr. M. Suyanto M.M, selaku Ketua Universitas AMIKOM Yogyakarta.
6. Bapak Akhmad Dahlan, M.Kom selaku Dosen Wali penulis.
7. Ibu Krisnawati, S.Si, M.T. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

8. Bapak Sudarmawan, M.T selaku Ketua Program Studi S1 Informatika Universitas AMIKOM Yogyakarta.
9. Bapak Joko Dwi Santoso, M.Kom selaku Dosen Pembimbing Skripsi yang telah memberikan bimbingan dan dukungan dalam penyusunan Skripsi ini.
10. Bapak Andi Sunyoto, M.Kom, Bapak Ferry Wahyu Wibowo, S.Si, M.Cs dan Bapak Agus Fatkhurohman, M.Kom selaku Dosen Penguji yang telah memberikan koreksi dan masukan terhadap Skripsi ini.
11. Dan kepada semua pihak yang telah membantu dan memberi motivasi sehingga penulis dapat menyelesaikan Skripsi ini.

Penulis menyadari dalam penyusunan Skripsi ini masih jauh dari kata sempurna. Penulis mengharapkan kritik dan saran yang membangun dari para pembaca demi perbaikan penulis dimasa yang akan datang.

Wassallamu alaikum wr.wb

Yogyakarta, 30 Agustus 2018

Penulis

Ariyo Pratomo  
NIM. 14.11.7684

## DAFTAR ISI

<b>SAMPUL DEPAN</b> .....	<b>i</b>
<b>JUDUL</b> .....	<b>ii</b>
<b>PERSETUJUAN</b> .....	<b>iii</b>
<b>PENGESAHAN</b> .....	<b>iv</b>
<b>PERNYATAAN</b> .....	<b>v</b>
<b>MOTTO</b> .....	<b>vi</b>
<b>PERSEMBAHAN</b> .....	<b>vii</b>
<b>KATA PENGANTAR</b> .....	<b>ix</b>
<b>DAFTAR ISI</b> .....	<b>xi</b>
<b>DAFTAR TABEL</b> .....	<b>xv</b>
<b>DAFTAR GAMBAR</b> .....	<b>xvi</b>
<b>INTISARI</b> .....	<b>xviii</b>
<b>ABSTRACT</b> .....	<b>xix</b>
<b>BAB I</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah .....	2
1.4 Maksud dan Tujuan Penelitian.....	3
1.4.1 Maksud Penelitian.....	3
1.4.2 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
1.6 Metodologi Penelitian .....	4
1.7 Sistematika Penulisan .....	4
<b>BAB II</b> .....	<b>6</b>
2.1 Kajian Pustaka .....	6
2.2 DHCP.....	7
2.3 DHCP <i>Packets</i> .....	7
2.3.1 DHCPDISCOVER.....	7
2.3.2 DHCPOFFER .....	7

2.3.3	DHCPREQUEST .....	7
2.3.4	DHCPACK.....	8
2.3.5	DHCPNAK.....	8
2.3.6	DHCPDECLINE.....	8
2.3.7	DHCPINFORM .....	8
2.3.8	DHCPRELEASE .....	8
2.4	DHCP Server .....	9
2.5	DHCP Client .....	9
2.6	BOOTP Relay Agent .....	9
2.7	Man In The Middle.....	9
2.8	Jenis-jenis Serangan yang dapat terjadi .....	9
2.8.1	DHCP Starvation .....	10
2.8.2	Rogue DHCP Server .....	10
2.8.3	Sniffing The Network Trafic.....	10
2.8.4	Denial of Service Attack ( DoS ).....	10
2.9	Model Jaringan.....	11
2.9.1	Peer to Peer.....	11
2.9.2	Client - Server .....	11
2.10	Topologi Jaringan .....	12
2.10.1	Topologi Bus .....	12
2.10.2	Topologi Ring .....	12
2.10.3	Topologi Tree .....	13
2.10.4	Topologi Star .....	14
2.10.5	Topologi Mesh .....	14
2.11	Routerboard MikroTik .....	15
2.12	Software Pendukung Penelitian .....	15
2.12.1	Mikrotik RouterOS .....	15
2.12.2	Wireshark Network Protocol Analyzer .....	15
2.12.3	Winbox.....	16
2.12.4	VMWare.....	16
2.12.5	Kali Linux.....	16

<b>BAB III.....</b>	<b>17</b>
3.1 Tinjauan Umum .....	17
3.2 Alur Penelitian .....	17
3.3 Rancangan Topologi Jaringan.....	18
3.4 Analisis Kebutuhan Perangkat Keras.....	20
3.5 Analisis Kebutuhan Perangkat Lunak.....	21
3.6 Rancangan Konfigurasi Mikrotik pada Router Bridge .....	21
3.6.1 Konfigurasi <i>Interface</i> .....	21
3.6.2 Konfigurasi <i>Bridge</i> .....	22
3.6.3 Konfigurasi Alamat IP .....	22
3.6.4 Konfigurasi Firewall NAT.....	23
3.6.5 Konfigurasi DHCP <i>server</i> .....	23
3.7 Rancangan Penggunaan Wireshark Pada Jaringan .....	23
3.7.1 Teknik <i>Tapping</i> .....	24
3.7.2 <i>Packet Sniffer</i> .....	24
3.8 Analisis DHCP <i>Packets</i> Sebelum Adanya <i>Rogue DHCP Server</i> .....	25
3.9 Analisis DHCP <i>Packets</i> Setelah Adanya <i>Rogue DHCP Server</i> .....	26
3.10 Dampak Yang Terjadi akibat Adanya <i>Rogue DHCP Server</i> .....	28
3.11 Analisis <i>Monitoring</i> dan Pencegahan <i>Rogue DHCP Server</i> .....	28
3.12 Rancangan <i>Monitoring</i> dan Pencegahan <i>Rogue DHCP Server</i> .....	30
3.13 Analisis DHCP <i>Packets</i> Setelah Adanya Pencegahan <i>Rogue DHCP</i> .....	31
<b>BAB IV.....</b>	<b>33</b>
4.1 Konfigurasi Alamat IP Host WMware WMnet 1 pada Laptop .....	33
4.2 Konfigurasi Alamat IP <i>Host</i> WMware VMnet8 pada Laptop Asli.....	34
4.3 Konfigurasi Alamat IP <i>Host</i> Laptop Asli Untuk Koneksi Internet.....	34
4.4 Konfigurasi Mikrotik pada Router Bridge.....	35
4.4.1 Konfigurasi <i>Interface</i> .....	36
4.4.2 Konfigurasi <i>Bridge</i> .....	36
4.4.3 Konfigurasi Alamat IP .....	37
4.4.4 Konfigurasi DNS .....	37
4.4.5 Konfigurasi <i>Firewall</i> NAT .....	38

4.4.6	Konfigurasi <i>DHCP Server</i> .....	38
4.4.7	Konfigurasi <i>Packet Sniffer</i> .....	40
4.5	Konfigurasi <i>Client 2</i> .....	42
4.6	Pengujian <i>DHCP Packets</i> sebelum adanya <i>Rogue DHCP Server</i> .....	43
4.6.1	Pertukaran <i>DHCP Packets</i> antara <i>DHCP Server</i> dengan <i>Client 1</i> .....	43
4.6.1.1	<i>DHCPDISCOVER</i> .....	44
4.6.1.2	<i>DHCPOFFER</i> .....	45
4.6.1.3	<i>DHCPREQUEST</i> .....	46
4.6.1.4	<i>DHCPACK</i> .....	47
4.6.2	Parameter <i>DHCP Packets</i> antara <i>DHCP Server</i> dengan <i>Client 1</i> .....	48
4.6.3	Hasil konfigurasi yang diamati pada <i>DHCP Server</i> dan <i>Client 1</i> .....	50
4.6.3.1	Dari sisi <i>DHCP Server</i> .....	50
4.6.3.2	Dari sisi <i>Client 1</i> .....	51
4.7	Konfigurasi <i>Rogue DHCP Server</i> pada Kali Linux .....	53
4.7.1	Konfigurasi alamat IP .....	53
4.7.2	Konfigurasi <i>IP Forwarding</i> , <i>Default Gateway</i> dan <i>IP Tables</i> .....	54
4.7.3	Konfigurasi <i>Rogue DHCP server</i> dengan Metasploit .....	55
4.8	Pengujian <i>DHCP Packets</i> setelah adanya <i>Rogue DHCP Server</i> .....	57
4.8.1	<i>DHCP Packets</i> pada saat pengujian .....	58
4.9	Dampak yang timbul akibat adanya <i>Rogue DHCP Server</i> .....	62
4.10	Implementasi <i>Monitoring</i> dan Pencegahan <i>Rogue DHCP Server</i> .....	63
4.10.1	<i>Monitoring</i> dengan fitur <i>Alert</i> pada <i>DHCP Server</i> asli di Mikrotik .....	64
4.10.2	Pencegahan menggunakan <i>Firewall Filter</i> pada Mikrotik .....	67
4.11	Pengujian <i>DHCP Packets</i> setelah adanya pencegahan .....	68
<b>BAB V</b>	.....	<b>74</b>
5.1	Kesimpulan .....	74
5.2	Saran .....	75
<b>DAFTAR PUSTAKA</b>	.....	<b>77</b>

## DAFTAR TABEL

Tabel 3. 1 Tabel Pengalamatan IP .....	20
Tabel 3. 2 Kebutuhan perangkat keras .....	20
Tabel 3. 3 Kebutuhan perangkat lunak .....	21
Tabel 3. 4 Konfigurasi Interface .....	22
Tabel 3. 5 Konfigurasi Alamat IP .....	22
Tabel 3. 6 Firewall NAT .....	23
Tabel 3. 7 Konfigurasi DHCP <i>Server</i> .....	23
Tabel 3. 8 Parameter pada DHCP Packets .....	27
Tabel 3. 9 Konfigurasi fitur <i>Alert</i> .....	30
Tabel 3. 10 Konfigurasi <i>Firewall filter rules</i> .....	31
Tabel 4. 1 Parameter DHCPDISCOVER pada <i>client 1</i> .....	49
Tabel 4. 2 Parameter DHCPOFFER pada <i>client 1</i> .....	49
Tabel 4. 3 Parameter DHCPREQUEST pada <i>client 1</i> .....	50
Tabel 4. 4 Parameter DHCPACK pada <i>client 1</i> .....	50
Tabel 4. 5 Data perolehan konfigurasi alamat IP pada <i>Client 1</i> .....	60
Tabel 4. 6 Perolehan DHCPACK pada <i>Client 1</i> .....	61
Tabel 4. 7 Perolehan konfigurasi alamat IP pada <i>Client 1</i> setelah pencegahan.....	70
Tabel 4. 8 Parameter DHCPOFFER pada <i>Client 1</i> setelah pencegahan .....	71
Tabel 4. 9 Parameter DHCPACK pada <i>Client 1</i> setelah pencegahan .....	71
Tabel 4. 10 Data perolehan alamat IP pada <i>Client 1</i> setelah pencegahan.....	72
Tabel 4. 11 Perbandingan perolehan alamat IP pada <i>Client 1</i> .....	73

## DAFTAR GAMBAR

Gambar 2. 1 Topologi <i>Bus</i> .....	12
Gambar 2. 2 Topologi <i>Ring</i> .....	13
Gambar 2. 3 Topologi <i>Tree</i> .....	13
Gambar 2. 4 Topologi <i>Star</i> .....	14
Gambar 2. 5 Topologi <i>Mest</i> .....	15
Gambar 3. 1 Alur Diagram Penelitian .....	18
Gambar 3. 2 Topologi Penelitian .....	19
Gambar 3. 3 Proses analisis pada wireshark .....	24
Gambar 3. 4 Alur DHCP <i>Packets</i> sebelum adanya <i>Rogue DHCP Server</i> .....	25
Gambar 3. 5 Alur DHCP <i>Packets</i> setelah adanya <i>Rogue DHCP Server</i> .....	26
Gambar 3. 6 Alur DHCP <i>Packets</i> setelah adanya pencegahan <i>Rogue DHCP</i> .....	32
Gambar 4. 1 Kondigurasi Alamat IP <i>Host</i> Wmware Wmnet 1 pada Laptop .....	33
Gambar 4. 2 Konfigurasi alamat IP <i>Host</i> VMware VMnet8 pada laptop asli .....	34
Gambar 4. 3 Konfigurasi Alamat IP <i>Host</i> Laptop Asli Untuk Koneksi Internet ...	35
Gambar 4. 4 Konfigurasi <i>Interface</i> pada Mikrotik .....	36
Gambar 4. 5 Konfigurasi <i>Bridge</i> pada Mikrotik .....	36
Gambar 4. 6 Konfigurasi Alamat IP .....	37
Gambar 4. 7 Konfigurasi DNS .....	38
Gambar 4. 8 Konfigurasi <i>Firewall NAT</i> .....	38
Gambar 4. 9 Konfigurasi <i>DHCP Server</i> .....	39
Gambar 4. 10 Konfigurasi <i>DHCP Server</i> pada Tab <i>Network</i> .....	39
Gambar 4. 11 Konfigurasi IP Pool pada Mikrotik .....	39
Gambar 4. 12 Konfigurasi <i>Packet Sniffer</i> .....	40
Gambar 4. 13 Konfigurasi <i>Packet Sniffer</i> pada Tab <i>Streaming</i> .....	41
Gambar 4. 14 Konfigurasi <i>Packet Sniffer</i> pada Tab <i>Filter</i> .....	41
Gambar 4. 15 Cara menggunakan <i>Wireshark</i> untuk pemantauan.....	42
Gambar 4. 16 Tampilan ketika melakukan pemantauan.....	42
Gambar 4. 17 Kondisi awal paket DHCPDISCOVER pada <i>Client 1</i> .....	44



Gambar 4. 18 Kondisi awal paket DHCP OFFER pada <i>Client 1</i> .....	45
Gambar 4. 19 Kondisi awal paket DHCP REQUEST pada <i>Client 1</i> .....	46
Gambar 4. 20 Kondisi awal paket DHCP ACK pada <i>Client 1</i> .....	47
Gambar 4. 21 <i>Flow Graph</i> DHCP Packets pada <i>Client 1</i> sebelum adanya <i>Rogue DHCP Server</i> .....	48
Gambar 4. 22 Hasil konfigurasi DHCP kondisi awal pada <i>Server</i> .....	51
Gambar 4. 23 Hasil konfigurasi DHCP kondisi awal pada <i>Client 1</i> .....	51
Gambar 4. 24 <i>Client 1</i> melakukan Ping ke Google pada kondisi awal.....	52
Gambar 4. 25 <i>Client 1</i> melakukan <i>Tracert</i> ke Google pada kondisi awal .....	52
Gambar 4. 26 Konfigurasi alamat IP pada <i>Client 3</i> .....	53
Gambar 4. 27 Hasil konfigurasi alamat IP di <i>Client 3</i> .....	54
Gambar 4. 28 Konfigurasi IP <i>Forwarding</i> , <i>Default Gateway</i> dan <i>IP Tables</i> .....	55
Gambar 4. 29 Hasil konfigurasi <i>Routing Table</i> .....	55
Gambar 4. 30 Tampilan awal Metasploit.....	56
Gambar 4. 31 Konfigurasi <i>Rogue DHCP Server</i> pada <i>Client 3</i> .....	56
Gambar 4. 32 Tampilan pada saat menjalankan <i>Rogue DHCP Server</i> .....	57
Gambar 4. 33 Pertukaran DHCP Packets setelah adanya <i>Rogue DHCP Server</i> ....	58
Gambar 4. 34 <i>Flow Graph</i> DHCP Packets setelah adanya <i>Rogue DHCP Server</i> .59	
Gambar 4. 35 Grafik perolehan DHCP ACK <i>Client 1</i> .....	61
Gambar 4. 36 Konfigurasi alamat IP <i>Client 1</i> dari <i>Rogue DHCP Server</i> .....	62
Gambar 4. 37 <i>Client 1</i> melakukan <i>Tracert</i> ke Google .....	63
Gambar 4. 38 Konfigurasi fitur <i>Alert</i> pada DHCP Server asli di Mikrotik .....	64
Gambar 4. 39 Pertukaran DHCP Packets pada fitur <i>Alert</i> .....	65
Gambar 4. 40 Notifikasi pada DHCP Alert hasil <i>Monitoring</i> .....	66
Gambar 4. 41 Notifikasi pada Log hasil <i>Monitoring</i> .....	66
Gambar 4. 42 Konfigurasi koneksi <i>Bridge</i> dengan <i>Firewall Filter</i> .....	67
Gambar 4. 43 Konfigurasi <i>Firewall Filter</i> pada <i>Filter Rules</i> .....	67
Gambar 4. 44 Notifikasi pada Log setelah <i>Monitoring</i> dan pencegahan .....	68
Gambar 4. 45 <i>Flow Graph</i> DHCP Packets setelah pencegahan .....	69
Gambar 4. 46 Grafik perolehan DHCP ACK <i>Client 1</i> setelah pencegahan.....	70

## INTISARI

*Dynamic Host Configuration Protocol* (DHCP) adalah *protocol* internet yang bertugas memberikan informasi TCP atau IP secara otomatis kepada komputer dan perangkat jaringan lain yang menggunakan *protocol* TCP atau IP. DHCP telah menjadi layanan kritis pada banyak lembaga atau perusahaan, namun keamanan *server* ini masih sangat sering dilewatkan dalam pengaman keamanan jaringan.

Jika tidak terdapat pemrosesan otentikasi selama pertukaran pesan DHCP antara *client* dan *server*, maka *server* tidak mengetahui apakah *client* yang meminta *address* merupakan *client* yang sah di dalam jaringan, dan *client* juga tidak mengetahui apakah *server* DHCP yang memberikan *address* adalah *server* yang sah. Kemungkinan hadirnya *client* dan *server* yang nakal pada jaringan dapat menyebabkan berbagai jenis masalah. Sebagai contohnya adalah serangan *Man in the Middle* yaitu *client* yang berperan sebagai *Rogue DHCP server* atau DHCP *server* palsu yang bertujuan untuk menyediakan informasi palsu, membaca *traffic* pengguna lain dan bahkan melakukan serangan *Denial of Service* (DoS).

Dengan adanya permasalahan ini penelitian dilakukan untuk mengetahui bagaimana proses terjadinya serangan terhadap DHCP *server*, sebelum adanya *Rogue DHCP server*, setelah adanya *Rogue DHCP server*, dan setelah adanya pencegahan terhadap *Rogue DHCP server* di dalam jaringan DHCP berbasis IPv4, sehingga keamanan dari sebuah jaringan dapat ditingkatkan untuk mencegah terjadinya serangan terhadap DHCP *server*.

**Kata Kunci** : DHCP, *Rogue DHCP*, serangan *Man in the Middle*, *Client Server*

## **ABSTRACT**

*Dynamic Host Configuration Protocol (DHCP) is an internet protocol that is responsible for automatically providing TCP or IP information to computers and other network devices that use TCP or IP protocols. DHCP has become a critical service for many institutions or companies, but server security is still very often missed in network security safeguards.*

*If there is no authentication processing during the exchange of DHCP messages between the client and server, the server does not know whether the client requesting the address is a legitimate client on the network, and the client also does not know whether the DHCP server that provides the address is the legitimate server. The possibility of the presence of Rogue clients and servers on the network can cause various types of problems. An example is the attack of Man in the Middle, a client that acts as a Rogue DHCP server or a fake DHCP server that aims to provide false information, read other users' traffic and even perform Denial of Service (DoS) attacks.*

*With this problem, the research was conducted to determine how the attack occurred on the DHCP server, prior to the Rogue DHCP server, after the Rogue DHCP server, and after the Rogue DHCP server was prevented from being based on IPv4 DHCP networks, the security of a network could be increased to prevent attacks on the DHCP server.*

**Keywords:** *DHCP, Rogue DHCP, Man in the Middle attack, Client Server*