

**DETEKSI SERANGAN *DHCP STARVATION*
MENGUNAKAN DEEP PACKET INSPECTION
BERDASARKAN *DSCP* DAN *MAC ADDRESS* PADA
JARINGAN SMK VINAMA 2 KOTA BEKASI**

SKRIPSI

Oleh :
Abid Muchlisien
202010225123



**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2024**

LEMBAR PERSETUJUAN PEMBIMBING

LEMBAR PERSETUJUAN PEMBIMBING

Judul Tugas akhir : Deteksi Serangan *DHCP Starvation* Menggunakan Deep Packet Inspection Berdasarkan *DSCP* Dan *Mac Address* Pada Jaringan *SMK Vinama 2 Kota Bekasi*

Nama Mahasiswa : Abid Muchlisien

Nomor : 202010225123

Pokok Mahasiswa

Program Studi/Fakultas : Informatika / Ilmu Komputer

Tanggal Lulus Ujian Skripsi : Jakarta, 05 /Juli /2024

MENYETUJUI,

Pembimbing I

Pembimbing II

(Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.)

NIDN : 0322108201

(Siti Setiawati, S.Pd., M.Pd.)

NIDN : 0313107904

Ketua Program Studi

(Ahmad Fathurrozi, S.E., M.M.S.I.)

NIP : 2012786

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA

2024

i

LEMBAR PENGESAHAN

Judul Tugas akhir : DETEKSI SERANGAN DHCP STARVATION
MENGUNAKAN DEEP PACKET INSPECTION
BERDASARKAN DSCP DAN MAC ADDRESS PADA
JARINGAN SMK VINAMA 2 KOTA BEKASI

Nama Mahasiswa : ABID MUCHLISIEN

Nomor Pokok Mahasiswa : 202010225123

Program Studi/Fakultas : Informatika / Ilmu Komputer

Tanggal Lulus Ujian Tugas akhir : 26 Juni 2024

Jakarta, 05 / Juli / 2024

MENGESAHKAN,

Ketua Tim Penguji : Sugiyatno, S.Kom., M.Kom.

NIDN : 0313077206

Penguji I : Prio Kustanto, S.T., M.Kom.

NIDN : 0309047701

Penguji II : Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.

NIDN : 0322108201

MENGETAHUI,

Ketua

Dekan

Program Studi Informatika

Fakultas Ilmu Komputer

Ahmad Fathurrozi, S.E., M.M.S.I

NIP. 2012786

Dr. Dra. Tyastuti Sri Lestari, M.M

NIP. 1408206

LEMBAR PERNYATAAN BUKAN PLAGIASI

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini :

Nama : Abid Muchlisien
NPM : 202010225123
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Deteksi Serangan *DHCP Starvation* Menggunakan Deep Packet Inspection Berdasarkan *DSCP* Dan *Mac Address* Pada Jaringan SMK Vinama 2 Kota Bekasi

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Bekasi, 11 Juni 2024
Penulis



ABSTRAK

Abid Muchlisien. 202010225123. 2024. Deteksi Serangan *DHCP Starvation* Menggunakan Deep Packet Inspection Berdasarkan *DSCP* Dan *Mac Address* Pada Jaringan SMK Vinama 2 Kota Bekasi. Fakultas Ilmu Komputer. Universitas Bhayangkara Jakarta Raya Bekasi.

Pada zaman yang modern dan serba maju ini layanan internet sudah menjadi kebutuhan yang sangat penting terhadap kehidupan manusia. Layanan jaringan internet dapat bekerja berdasarkan infrastruktur jaringan komputer baik secara lokal ataupun global. Salah satu layanan penting didalam jaringan adalah *DHCP Server*. Jaringan yang diterapkan di SMK Vinama 2 Kota Bekasi tidak menerapkan firewall yang melindungi layanan *DHCP Server* sehingga pernah terjadinya salah satu serangan *DDoS* yaitu *DHCP Starvation* yang menyebabkan *CPU Load* pada router server menjadi full dan habisnya ketersediaan *IP Address* di *DHCP Server*, sehingga perlu diterapkannya model keamanan jaringan yang dapat melindungi layanan *DHCP Server*. Tujuan diterapkannya model keamanan jaringan tersebut yaitu konfigurasi Access Control List dan penerapan Deep Packet Inspection pada *firewall* sehingga dapat meningkatkan keamanan di layanan *DHCP Server*. Untuk menerapkan *firewall* tersebut peneliti menggunakan salah satu metodologi pengembangan jaringan yaitu *NDLC (Network Development Life Cycle)* yang terdiri dari tahapan – tahapan yaitu analisis, desain, simulasi, implementasi, monitoring dan manajemen. Hasil penerapan *firewall* dengan Deep Packet Inspection yaitu *firewall* yang telah diterapkan *DPI* mampu membuang packet data *DHCP Discover* yang berasal dari serangan *DHCP Starvation* serta menurunkan *Load CPU* dari 13% ke kondisi normal nya yaitu 2% dalam waktu 16 menit, paket data yang masuk saat serangan mampu diturunkan dari kondisi maksimum yaitu 14Mbps hingga ke kondisi normal yaitu 0,5Mbps dalam waktu 10 menit dan ketersediaan *IP Address* di *DHCP Server* tetap utuh dan tidak habis. Sehingga dari hasil penerapan model keamanan inspeksi data secara mendalam dan akses kontrol yang diterapkan pada *firewall* berhasil meningkatkan keamanan di layanan *DHCP Server*.

Kata Kunci : *NDLC, Firewall, Deep Packet Inspection, DHCP Starvation, DSCP*

ABSTRACT

Abid Muchlisien. 202010225123. 2024. *Detection of DHCP Starvation Attacks Using Deep Packet Inspection Based on DSCP and MAC Address on the Vinama 2 Vocational School Network. Faculty of Computer Science. Bhayangkara University Jakarta Raya.*

In this modern and advanced era, internet services have become a very important need for human life. Internet network services can work based on computer network infrastructure both locally and globally. One of the important services in the network is the DHCP Server. The network implemented at Vinama 2 Vocational School, Bekasi City, does not implement a firewall that protects the DHCP Server service, so one of the DDoS attacks, namely DHCP Starvation, occurred which caused the CPU load on the router server to become full and the availability of IP addresses on the DHCP Server ran out, so it is necessary to implement a security model network that can protect the DHCP Server service. The aim of implementing this network security model is configuring the Access Control List and implementing Deep Packet Inspection on the firewall so that it can improve security in the DHCP Server service. To implement the firewall, researchers used a network development methodology, namely NDLC (Network Development Life Cycle) which consists of stages, namely analysis, design, simulation, implementation, monitoring and management. The result of implementing a firewall with Deep Packet Inspection is that the firewall that has been implemented by DPI is able to remove DHCP Discover data packets originating from DHCP Starvation attacks and reduce CPU Load from 13% to its normal condition of 2% within 16 minutes, data packets that came in during the attack able to be reduced from maximum conditions, namely 14Mbps, to normal conditions, namely 0.5Mbps, within 10 minutes and the availability of IP addresses on the DHCP Server remains intact and does not run out. So the results of implementing the security model of in-depth data inspection and access control applied to the firewall have succeeded in increasing security in the DHCP Server service.

Keywords: NDLC, Firewall, Deep Packet Inspection, DHCP Starvation, DSCP

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini :

Nama : Abid Muchlisien
NPM : 202010225123
Program Studi : Informatika
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul :

Deteksi Serangan *DHCP Starvation* Menggunakan Deep Packet Inspection Berdasarkan *DSCP* Dan *Mac Address* Pada Jaringan SMK Vinama 2 Kota Bekasi

berserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 11 Juni 2024
Yang Menyatakan



KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadiran Allah SWT yang telah memberikan rahmat dan petunjuk serta memberikan kemudahan, sehingga penulis dapat menyelesaikan skripsi yang berjudul “Deteksi Serangan *DHCP Starvation* Menggunakan Deep Packet Inspection Berdasarkan *DSCP* Dan *Mac Address* Pada Jaringan SMK Vinama 2 Kota Bekasi”. Tidak lupa juga penulis mengucapkan terimakasih sebesar-besarnya kepada semua pihak yang secara langsung maupun tidak langsung terlibat dalam penulisan skripsi ini. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada :

1. Bapak Irjen Pol.(purn) Prof. Dr. Drs. H. Bambang Karsono, S.H., M.M. Ph.D., D.Crim (HC) selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Ibu Dr. Dra. Tyastuti Sri Lestari, M.M. selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. selaku ketua Program studi Informatika Universitas Bhayangkara Jakarta Raya.
4. Bapak Rakhmat Purnomo, S.Pd., S.Kom., M.Kom. selaku Dosen Pembimbing I yang telah membimbing penulis dalam penyusunan skripsi
5. Ibu Siti Setiawati, S.Pd., M.Pd. selaku Dosen Pembimbing akademik sekaligus pembimbing II yang telah membimbing penulis dalam penyusunan skripsi ini.
6. Bapak dan Ibu Dosen Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya yang selama ini memberikan ilmu pengetahuan.
7. Staf Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya atas bantuan dalam urusan administrasi

8. Bapak Akmal Fauzan, S.Kom. yang telah mengizinkan serta memberikan waktu dan tempat serta bantuan dalam melaksanakan penelitian di SMK Vinama 2 Kota Bekasi.
 9. Teristimewa kepada orang tua, terutama Bapak dan Ibu yang selalu sabar dan memberikan dukungan apapun dengan penuh kasih sayang dan doa yang terus mengiringi langkah penulis sehingga dapat menyelesaikan skripsi ini.
 10. Rekan-rekan seperjuangan mahasiswa angkatan 2020 dari Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya atas dukungan dan kerjasamanya dalam penyelesaian skripsi ini
- Penulis menyadari bahwa masih banyak kekurangan dari skripsi ini, baik dari materi maupun teknik penyajiannya, mengingat kurangnya pengetahuan dan pengalaman menulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun.

Jakarta, 11 Juni 2024


Abid Muchlisien

202010225123

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	i
LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iii
ABSTRAK	iv
ABSTRACT	v
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL.....	xvii
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah	5
1.3 Batasan Masalah.....	5
1.4 Rumusan Masalah	5
1.5 Tujuan dan Manfaat Penelitian.....	5
1.5.1 Tujuan Penelitian	5
1.5.2 Manfaat Penelitian	6
1.6 Sistematika Penulisan.....	6

BAB II LANDASAN TEORI	8
2.1 Hasil Penelitian terdahulu yang relevan	8
2.2 Sistem	11
2.3 Sistem Keamanan Jaringan.....	11
2.3.1 Deteksi.....	12
2.3.2 Serangan.....	12
2.3.3 <i>DHCP Starvation</i>	12
2.4 <i>Deep Packet Inspection</i>	13
2.5 <i>Differentiated Services Code Point</i>	16
2.6 <i>Mac Address</i>	17
2.7 Jaringan Komputer	17
2.7.1 <i>IP Address</i>	18
2.7.2 <i>Network Development Life Cycle</i>	23
2.8 <i>Flowchart</i>	23
2.9 <i>Packet Tracer</i>	25
2.9.1 Kelebihan dan Kekurangan <i>Packet Tracer</i>	26
2.9.2 System Requirement <i>Packet Tracer</i>	26
BAB III METODOLOGI PENELITIAN	28
3.1 Gambaran Umum Tempat Penelitian	28
3.2 Kerangka Penelitian.....	28

3.3	Metode Pengumpulan Data	31
3.3.1	Data Primer & Data Sekunder.....	32
3.4	<i>Network Development Life Cycle</i>	34
3.4.1	<i>Analysis</i>	34
3.4.2	<i>Design</i>	34
3.4.3	<i>Simulation Prototyping</i>	34
3.4.4	<i>Implementation</i>	35
3.4.5	<i>Monitoring</i>	35
3.4.6	<i>Management</i>	35
3.5	Metode Analisis.....	35
3.5.1	Analisis sistem berjalan.....	35
3.5.2	Analisis sistem usulan.....	37
3.5.3	Analisis Permasalahan	39
3.6	Alat & Software Pendukung.....	40
3.6.1	Alat Pendukung Penelitian:.....	40
3.6.2	Software Pendukung Penelitian	40
BAB IV HASIL DAN PEMBAHASAN.....		41
4.1	Analisis.....	41
4.1.1	Kelebihan & Kekurangan Sistem Berjalan	41
4.1.2	Kelebihan & Kekurangan Sistem Usulan	42

4.1.3	Kebutuhan Sistem	42
4.2	Design Topologi	43
4.2.1	Perancangan Topologi Sebelumnya.....	43
4.2.2	Hasil Perancangan Topologi Jaringan.....	44
4.3	Simulasi Protoyping	45
4.3.1	Tahap 1 Persiapan	45
4.3.2	Tahap 2 Simulasi Topologi <i>Packet Tracer</i>	46
4.3.3	Tahap 3 Menjalankan Simulasi Protoyping Pada <i>Packet Tracer</i>	50
4.3.4	Hasil Simulasi Protoyping Pada <i>Packet Tracer</i>	50
4.4	Implementasi Mikrotik	53
4.4.1	Konfigurasi Mikrotik	53
4.4.2	<i>Interfaces</i>	56
4.4.3	<i>IP Address</i>	58
4.4.4	<i>DHCP Client</i>	59
4.4.5	<i>DNS Server</i>	60
4.4.6	<i>Firewall NAT (Network Address Translation)</i>	62
4.4.7	<i>DHCP Server</i>	63
4.4.8	<i>Bridge Interfaces</i>	64
4.4.9	<i>Port Bridge</i>	65
4.4.10	<i>Bridge Filtering</i>	66

4.4.11	<i>Firewall Filter Rules</i>	68
4.4.12	<i>Firewall Mangle</i>	69
4.4.13	<i>Logging Mikrotik</i>	70
4.5	Monitoring.....	72
4.5.1	Monitoring <i>CPU Load</i> Mikrotik.....	72
4.5.2	Monitoring Paket Data Mikrotik.....	73
4.6	Manajemen	74
4.7	Hasil Penelitian.....	75
4.7.1	Sebelum Penerapan Sistem Keamanan <i>Deep Packet Inspection</i>	75
4.7.2	Sesudah Penerapan Sistem Keamanan <i>Deep Packet Inspection</i>	77
4.8	Pembahasan Penelitian	79
BAB V PENUTUP	82
5.1	Kesimpulan	82
5.2	Saran.....	83
DAFTAR PUSTAKA	84
LAMPIRAN	89

DAFTAR GAMBAR

Gambar 2.1 Pola Serangan <i>DHCP Starvation</i>	13
Gambar 2.2 Perbedaan DPI dengan analisis paket data biasa	15
Gambar 2.3 Alur kerja <i>Deep Packet Inspection</i>	15
Gambar 2.4 Topologi <i>Bus</i>	20
Gambar 2.5 Topologi <i>Ring</i>	21
Gambar 2.6 Topologi <i>Star</i>	22
Gambar 2.7 Topologi <i>Mesh</i>	22
Gambar 2.8 Alur tahapan <i>NDLC</i>	23
Gambar 3.1 Lokasi SMK Vinama 2 Kota Bekasi	28
Gambar 3.2 Kerangka Penelitian.....	29
Gambar 3.3 Alur Kerja <i>Firewall</i> dan <i>DPI</i>	30
Gambar 3.4 Hirarki Pengumpulan Data	32
Gambar 3.5 Topologi yang sedang berjalan.....	36
Gambar 3.6 Topologi jaringan usulan	38
Gambar 4.1 Perancangan Topologi Sebelumnya	43
Gambar 4.2 Hasil Perancangan Topologi Jaringan	44
Gambar 4.3 Topologi Usulan di Packet Tracer	46
Gambar 4.4 <i>Mac Filtering Wireless</i>	50
Gambar 4.5 Hasil Simulasi Prototyping <i>Wireline</i>	51
Gambar 4.6 Hasil Simulasi Prototyping Pengguna	51
Gambar 4.7 Hasil Simulasi Prototyping <i>Wireless</i>	52
Gambar 4.8 <i>Interfaces</i> Mikrotik Sebelumnya	57

Gambar 4.9 Hasil Konfigurasi <i>Interfaces</i> Mikrotik.....	57
Gambar 4.10 <i>IP Address</i> Mikrotik Sebelumnya.....	58
Gambar 4.11 Hasil Konfigurasi <i>IP Address</i> Mikrotik.....	59
Gambar 4.12 <i>DHCP Client</i> Mikrotik Sebelumnya.....	59
Gambar 4.13 Hasil Konfigurasi <i>DHCP Client</i>	60
Gambar 4.14 <i>DNS Server</i> Mikrotik Sebelumnya	61
Gambar 4.15 Hasil Konfigurasi <i>DNS Server</i> Mikrotik.....	61
Gambar 4.16 <i>NAT Masquerade</i> Mikrotik Sebelumnya.....	62
Gambar 4.17 Hasil Konfigurasi <i>NAT Masquerade</i> Mikrotik.....	62
Gambar 4.18 <i>DHCP Server</i> Mikrotik Sebelumnya.....	63
Gambar 4.19 Hasil Konfigurasi <i>DHCP Server</i> Mikrotik	64
Gambar 4.20 <i>Bridge Interfaces</i> Sebelumnya.....	64
Gambar 4.21 Hasil Konfigurasi <i>Bridge Interfaces</i>	65
Gambar 4.22 <i>Port Bridge</i> Sebelumnya.....	66
Gambar 4.23 Hasil Konfigurasi <i>Port Bridge</i>	66
Gambar 4.24 <i>Bridge Filtering</i> Sebelumnya	67
Gambar 4.25 Hasil Konfigurasi <i>Bridge Filtering</i>	67
Gambar 4.26 <i>Firewall Filter Rules</i> Sebelumnya.....	68
Gambar 4.27 Hasil Konfigurasi <i>Firewall Filter Rules</i>	69
Gambar 4.28 <i>Firewall Mangle</i> Sebelumnya	69
Gambar 4.29 Hasil Konfigurasi <i>Firewall Mangle</i>	70
Gambar 4.30 <i>Logging</i> Topologi Sebelumnya	71
Gambar 4.31 Hasil konfigurasi fitur <i>logging</i>	71

Gambar 4.32 Hasil Monitoring <i>CPU Load</i> Mikrotik	72
Gambar 4.33 Monitoring <i>CPU Load</i> Saat Serangan	73
Gambar 4.34 Monitoring Paket Data Mikrotik	73
Gambar 4.35 Monitoring Paket Data Saat Serangan	74
Gambar 4.36 <i>Load CPU</i> Sebelum Penerapan	75
Gambar 4.37 Pengujian Paket Data Sebelum Penerapan	76
Gambar 4.38 Pengujian <i>DHCP Lease</i> Sebelum Penerapan	77
Gambar 4.39 Pengujian <i>CPU Load</i> Sesudah Penerapan	77
Gambar 4.40 Kondisi Paket Data Sesudah Penerapan	78
Gambar 4.41 Kondisi <i>DHCP Lease</i> Sesudah Penerapan	79
Gambar 4.42 Hasil ekstraksi paket data DPI dan perbandingan dengan algoritma lain yang sejenis	80



DAFTAR TABEL

Tabel 2.1 Hasil Penelitian terdahulu yang relevan.....	8
Tabel 2.2 Kode <i>Differentiated Services Code Point</i>	16
Tabel 2.3 Simbol <i>Flowchart</i>	24
Tabel 2.4 Minimum Spesifikasi <i>Packet Tracer</i>	26
Tabel 2.5 Recommended Spesifikasi <i>Packet Tracer</i>	27
Tabel 3. 1 Daftar Pengguna Jaringan	37
Tabel 3. 2 Daftar Pengguna Jaringan Usulan	39
Tabel 3. 3 Alat Pendukung Penelitian	40
Tabel 3. 4 Software Pendukung Penelitian.....	40
Tabel 4. 1 Kebutuhan Sistem.....	42
Tabel 4. 2 Hasil Simulasi Protoyping <i>Wireline</i>	51
Tabel 4. 3 Hasil Simulasi Protoyping <i>Wireless</i>	52

DAFTAR LAMPIRAN

Lampiran 1. Foto Penelitian	90
Lampiran 2. Denah Lt 1	91
Lampiran 3. Denah Server Lab Lt 2.....	92
Lampiran 4. Denah Lt 3	93
Lampiran 5. Surat Pernyataan Wawancara	94
Lampiran 6. Hasil Wawancara.....	95
Lampiran 7. Surat Izin Penelitian.....	96
Lampiran 8. Surat Balasan Penelitian.....	97
Lampiran 9. Hasil Cek Turnitin.....	98
Lampiran 10. Kartu Bimbingan Dosbing 1.....	99
Lampiran 11. Kartu Bimbingan Dosbing 2.....	100
Lampiran 12. Biodata Mahasiswa.....	101

