

**TUGAS AKHIR**

**OPTIMALISASI KEAMANAN JARINGAN DENGAN METODE  
VULNERABILITY ASSESSMENT DAN HARDENING PADA  
INFRASTRUKTUR JARINGAN KOMPUTER PT XYZ**

**Diajukan guna melengkapi sebagian syarat dalam mencapai gelar**

**Sarjana Strata Satu (S1)**



**UNIVERSITAS  
MERCU BUANA**  
**Disusun Oleh :**

**NAMA : MOHAMAD SOFYAN KUSUMAH PUTRA**  
**NIM : 41410110018**  
**Program Studi : Teknik Elektro**

**PROGRAM STUDI TEKNIK ELEKTRO**

**FAKULTAS TEKNIK**

**UNIVERSITAS MERCU BUANA**

**JAKARTA**

**2017**

## LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Mohamad Sofyan Kusumah Putra  
NIM : 41410110018  
Fakultas : Teknik  
Program Studi : Teknik Elektro  
Judul Tugas Akhir : Optimalisasi Keamanan Jaringan Dengan Metode Vulnerability Assesment dan Hardening Pada Infrastruktur Jaringan Komputer PT XYZ

Dengan ini menyatakan bahwa hasil penulisan Tugas Akhir yang saya buat ini merupakan hasil karya sendiri dan benar keasliannya. Apabila ternyata dikemudian hari penulisan Tugas Akhir ini merupakan hasil plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggung jawabkan sekaligus bersedia menerima sanksi berdasarkan aturan tata tertib di Universitas Mercu Buana.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Penulis,



[ Mohamad Sofyan Kusumah Putra ]

**LEMBAR PENGESAHAN**

**OPTIMALISASI KEAMANAN JARINGAN DENGAN METODE  
VULNERABILITY ASSESSMENT DAN HARDENING PADA  
INFRASTRUKTUR JARINGAN KOMPUTER PT XYZ**

Disusun Oleh :

Nama : Mohamad Sofyan Kusumah Putra

NIM : 41410110018

Jurusan : Teknik Elektro

Pembimbing Tugas Akhir

UNIVERSITAS  
MERCU BUANA

[ Fadli Sirait, S.Si., M.T. ]

Mengetahui,

Koordinator Tugas Akhir / Ketua Program Studi



[ Dr. Setyo Budiyanto, S.T., M.T. ]

## KATA PENGANTAR

Dengan mengucapkan rasa syukur kehadirat Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penelitian dan penulisan Tugas Akhir dengan judul: **“OPTIMALISASI KEAMANAN JARINGAN DENGAN METODE VULNERABILITY ASSESSMENT DAN HARDENING PADA INFRASTRUKTUR JARINGAN KOMPUTER PT XYZ”** dapat diselesaikan dengan baik.

Dalam proses kegiatan ini, dari awal hingga terbentuknya tulisan dalam laporan ini banyak pihak yang telah membantu dan berpartisipasi memberikan bantuan dan kontribusi kepada penulis dalam penyusunan laporan ini. Untuk itu, penulis mengucapkan terima kasih kepada :

1. Allah SWT,
2. Kedua Orang Tua
3. Istriku Intan Prajawati S. beserta keluarga tercinta,
4. Bapak Dr. Setyo Budiyanto, S.T., M.T. selaku Ketua Program Studi Teknik Elektro,
5. Bapak Fadli Sirait, S.Si., MT. selaku Koordinator Tugas Akhir,
6. Bapak Fadli Sirait, S.Si., MT. selaku Pembimbing Akademis,
7. Bapak Hadrijanto selaku pembimbing di PT Systel Indonesia,
8. Rekan-rekan engineer PT Systel Indonesia dan Pusdatin Kementerian Kesehatan RI,
9. Rekan-rekan elektro angkatan 17 Universitas Mercu Buana,
10. Semua pihak yang telah membantu dalam penyelesaian laporan ini.

Semoga penelitian dan penulisan Tugas Akhir ini dapat bermanfaat baik untuk pribadi penulis, Dosen pembimbing, serta rekan rekan Mahasiswa Universitas Mercu Buana, dan masyarakat umum.

Jakarta, Juli 2017

Penulis

Mohamad Sofyan Kusumah Putra



## DAFTAR ISI

Halaman Judul	
Halaman Pengesahan .....	ii
Halaman Pengesahan .....	iii
Abstrak .....	iv
Kata Pengantar .....	v
Daftar Isi.....	vii
Daftar Gambar.....	x
Daftar Tabel .....	xi
Daftar Grafik.....	xii
BAB I. PENDAHULUAN	
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penelitian.....	4
1.5 Batasan Masalah.....	5
1.5 Metodologi Penelitian.....	5
1.6 Sistematika Penulisan.....	7
BAB II. LANDASAN TEORI	
2.1 Konsep Jaringan Komputer.....	8
2.1.1 Model Referensi OSI.....	13
2.1.2 TCP/IP.....	15

2.2 Perkembangan Teknologi Internet.....	16
2.3 Konsep Keamanan Jaringan.....	18
2.3.1 Resiko ( <i>Risk</i> ).....	19
2.3.2 Ancaman ( <i>Threat</i> ).....	19
2.3.3 Kelemahan ( <i>Awareness</i> ).....	20
2.3.4 Policy Keamanan Jaringan ( <i>Security Policy</i> ).....	20
2.4 Topologi dan Perangkat Keamanan Jaringan.....	21
2.4.1 Firewall.....	22
2.4.2 Router.....	23
2.4.3 Switch.....	23
2.5 Insiden Keamanan Jaringan.....	24
2.6 Vulnerability Assessment.....	30
2.6.1 Vulnerability Scanner.....	32
2.6.2 Tenable Nessus.....	33

### BAB III. METODE PENELITIAN DAN SIMULASI

3.1 Tahapan-Tahapan Penelitian.....	37
3.2 Desain Perancangan Implementasi.....	40
3.3 Kebutuhan Pendukung Implementasi.....	41
3.4 Konfigurasi Jaringan.....	45
3.4.1 Konfigurasi Perangkat Jaringan.....	47
3.4.2 Konfigurasi Nessus.....	50

3.5 Vulnerability Assessment dan Remediation.....	52
3.6 Hardening.....	53
3.6.1 Jenis-Jenis Hardening.....	54

#### BAB IV. PENGUJIAN DAN ANALISA

4.1 Umum.....	56
4.2 Pengujian Vulnerability Assessment Tahap I.....	56
4.2.1 Pengujian Core-WAN.....	58
4.2.2 Pengujian Dist-Switch.....	60
4.2.3 Pengujian Web-Server.....	61
4.2.4 Pengujian PC-Client.....	63
4.3 Vulnerability Assessment Report (Pra Optimalisasi).....	65
4.4 Hardening.....	66
4.4.1 Hardening Core-WAN-L3.....	66
4.4.2 Hardening Dist-Switch.....	67
4.4.3 Hardening Server/Web-Server.....	68
4.4.4 Hardening Workstation.....	70
4.4.5 Hardening Desain Topologi Jaringan.....	72
4.5 Pengujian Vulnerability Assessment Tahap II.....	73
4.5.1 Pengujian Firewall-WAN.....	74
4.5.2 Pengujian Core-Switch.....	75
4.5.3 Pengujian Dist-Switch.....	76
4.5.4 Pengujian Server/Web-Server.....	77



4.6 Vulnerability Assessment Report (Pasca Optimalisasi).....	78
4.7 Analisis Data.....	79
BAB V. PENUTUP	
5.1 Kesimpulan.....	85
5.2 Saran.....	88
Daftar Pustaka .....	89
Lampiran	



## DAFTAR GAMBAR

Gambar 2.1 Sistem Komunikasi .....	8
Gambar 2.2 Internetworking .....	9
Gambar 2.3 Desain Topologi Bus .....	9
Gambar 2.4 Desain Topologi Star .....	10
Gambar 2.5 Desain Topologi Tree .....	11
Gambar 2.6 Desain Topologi Ring .....	11
Gambar 2.7 Desain Topologi Mesh .....	12
Gambar 2.8 Desain Topologi Extended Star.....	13
Gambar 2.9 OSI Layer .....	14
Gambar 2.10 Lapisan Atas (Upper Layer).....	14
Gambar 2.11 Lapisan Bawah (Lower Layer).....	15
Gambar 2.12 TCP/IP Layer dan Protokol.....	15
Gambar 2.13 Peta Teknologi Network Security .....	21
Gambar 2.14 Penempatan Firewall dan Fungsi DMZ .....	22
Gambar 2.15 Ancaman Tindakan Kejahatan di Dunia Maya .....	25
Gambar 2.16 Session Hijacking.....	26
Gambar 2.17 Packet Sniffer .....	27
Gambar 2.18 Denial of Service (DoS).....	28
Gambar 2.19 Man-in-the-Middle.....	29
Gambar 2.20 Fase Vulnerability Assessment .....	30
Gambar 2.21 Nessus's Vulnerability Scanner .....	33
Gambar 3.1 Diagram Alir Implementasi.....	37
Gambar 3.2 Desain Topologi Jaringan sebelum dioptimalisasi.....	40
Gambar 3.3 Desain Topologi Jaringan setelah dioptimalisasi.....	41
Gambar 3.4 Perancangan Implementasi Jaringan tanpa firewall.....	43
Gambar 3.5 Perancangan Implementasi Jaringan menggunakan firewall .....	44
Gambar 3.6 Status interfaces Switch L3 (CORE-WAN-E22).....	47
Gambar 3.7 Konfigurasi interface Switch L3 (CORE-WAN-E22).....	47
Gambar 3.8 Status IP Gateway tiap vlan di CORE-WAN-E22.....	48

Gambar 3.9 Status routingan yang aktif di CORE-WAN-E22 .....	48
Gambar 3.10 Status interfaces Firewall (Depkes-DC-J23).....	49
Gambar 3.11 Status routingan yang aktif di Firewall (Depkes-DC-J23).....	49
Gambar 3.12 Aplikasi Nessus Scanner .....	50
Gambar 3.13 Plugin Template Basic Network Scan.....	51
Gambar 3.14 Konfigurasi host yang akan di scan.....	51
Gambar 3.15 Daftar host target yang akan di scan .....	52
Gambar 4.1 Pengujian Desain Jaringan Tahap I.....	57
Gambar 4.2 Hasil Scanning menggunakan Nessus dari Tenable.....	58
Gambar 4.3 Hasil Vulnerability Scanning CORE-WAN-L3.....	58
Gambar 4.4 Detail Vulnerability Assessment CORE-WAN-L3 .....	59
Gambar 4.5 Hasil Vulnerability Scanning Dist-Switch .....	60
Gambar 4.6 Detail Vulnerability Assessment Dist-Switch.....	61
Gambar 4.7 Hasil Vulnerability Scanning Web-Server.....	61
Gambar 4.8 Detail Vulnerability Assessment Web-Server.....	62
Gambar 4.9 Hasil Vulnerability Scanning PC-Client .....	63
Gambar 4.10 Detail Vulnerability Assessment PC-Client.....	64
Gambar 4.11 Desain Jaringan menggunakan Firewall dan Zona DMZ.....	72
Gambar 4.12 Hasil Scanning Nessus dari Tenable (Pasca Optimalisasi).....	73
Gambar 4.13 Hasil Vulnerability Scanning Firewall-WAN.....	74
Gambar 4.14 Hasil Vulnerability Scanning Core-Switch.....	75
Gambar 4.15 Hasil Vulnerability Scanning Dist-Switch .....	76
Gambar 4.16 Hasil Vulnerability Scanning Web-Server.....	77
Gambar 4.17 Arsitektur Desain Keamanan Jaringan.....	79
Gambar 4.18 Desain Jaringan menggunakan Firewall dan Zona DMZ.....	80

## DAFTAR TABEL

Tabel 2.2 Estimasi Profil Pengguna Internet di Lima Benua Tahun 2008.....	17
Tabel 2.2 Datasheet Tenable Nessus Scanner.....	35
Tabel 3.3 Detail Mekanisme Tahapan Penelitian .....	38
Tabel 3.2 Desain Konfigurasi Alamat IP sebelum dioptimalisasi .....	45
Tabel 3.3 Desain Konfigurasi Alamat IP sesudah dioptimalisasi .....	46
Tabel 4.1 Perangkat yang diuji tahap 1.....	57
Tabel 4.2 Tingkat Resiko Vulnerabilities CORE-WAN-L3 .....	59
Tabel 4.3 Tingkat Resiko Vulnerabilities Dist-Switch.....	60
Tabel 4.4 Tingkat Resiko Vulnerabilities Web-Server.....	62
Tabel 4.5 Tingkat Resiko Vulnerabilities PC-Client .....	63
Tabel 4.6 Summary Report Vulnerability Assessment Pra Optimization .....	65
Tabel 4.7 Tingkat Resiko Vulnerabilities Firewall-WAN.....	74
Tabel 4.8 Tingkat Resiko Vulnerabilities Core-Switch.....	75
Tabel 4.9 Tingkat Resiko Vulnerabilities Dist-Switch .....	76
Tabel 4.10 Tingkat Resiko Vulnerabilities Web-Server.....	77
Tabel 4.11 Summary Report Vulnerability Assessment Pasca Optimization..	78

## DAFTAR GRAFIK

Grafik 4.4 Grafik Vulnerabilities (Pra Optimalisasi).....	81
Grafik 4.2 Grafik Vulnerabilities (Pasca Optimalisasi).....	84
Grafik 5.1 Grafik Perbandingan Pengujian Tahap 1 dan Tahap 2.....	87

