

ABSTRAK

Dalam era digitalisasi yang semakin maju, keamanan jaringan menjadi komponen yang sangat krusial bagi berbagai organisasi maupun institusi pendidikan, termasuk SMK AL-AMIEN. Sebagai institusi pendidikan yang mengedepankan penerapan teknologi dalam proses pembelajaran SMK AL-AMIEN perlu memastikan bahwa jaringan yang digunakan oleh siswa, guru, dan staf administrasi terlindungi dengan baik. Identifikasi masalah yang terjadi pada jaringan SMK AL-AMIEN mencakup beberapa aspek utama, yaitu masalah bandwidth, penyusup, dan kurangnya monitoring jaringan. Permasalahan bandwidth sering terjadi akibat tingginya jumlah pengguna yang mengakses jaringan. Untuk mengantisipasi permasalahan tersebut, digunakan metode NDLC (*Network Development Life Cycle*) dengan penerapan teknik Port Knocking pada Mikrotik untuk membatasi akses hanya kepada pengguna yang sah. Hasil pengujian menunjukkan bahwa keamanan jaringan meningkat setelah implementasi Port Knocking. Berdasarkan pengukuran kualitas layanan (*Quality of Service*), diperoleh hasil throughput rata-rata sebesar 2673 kbps, delay rata-rata 3 ms, jitter 0 ms, dan packet loss sebesar 0,1%, yang masing-masing mendapatkan nilai indeks 4 dan

dikategorikan "Sangat Baik" berdasarkan standar TIPHON. Nilai indeks rata-rata sebelum dan sesudah implementasi tetap berada di angka 4, menandakan bahwa penerapan keamanan jaringan tidak menurunkan kualitas layanan. Dengan demikian, implementasi teknik Port Knocking pada Mikrotik terbukti berhasil meningkatkan keamanan jaringan tanpa mengorbankan performa jaringan di SMK AL-AMIEN.

Kata kunci: SMK AL-Amien, port knocking, keamanan jaringan

DAFTAR ISI

LEMBAR PENGESAHAN.....	ii
LEMBAR PERNYATAAN	iii
ABSTRAK.....	iv
KATA PENGANTAR	v
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah.....	6
1.4 Tujuan Penelitian.....	6
1.5 Manfaat Penelitian.....	7
BAB II TINJAUAN PUSTAKA.....	8
2.1 Studi Literatur	8
2.2 Landasan Teori	14
2.2.1 Keamanan Jaringan	14
2.2.2 Jaringan Komputer	15
2.2.3 Firewall.....	16
2.2.4 Mikrotik RouterBoard	18
2.2.5 Port Knocking.....	19
2.2.6 Winbox.....	21
2.2.7 Komponen Yang Di Uji.....	21
2.2.8 Parameter QOS.....	22
2.2.9 Diagram Alur Proses port knocking	28

BAB III METODOLOGI PENELITIAN.....	31
3.1 Metode Penelitian	31
3.2 Alur Penelitian	32
3.2.1 Analysis	32
3.2.2 Design.....	33
3.2.2.1 Analisis Perangkat Keras Untuk Membangun Sistem .	33
3.2.2.2 Analisis Perangkat Lunak Untuk Membangun Sistem	34
3.2.2.3 Desain Rancangan Keamanan Jaringan.....	34
3.2.2.4 Gambar Desain Rancangan Topologi.....	36
3.2.3 Simulation Prototyping	36
3.2.4 Implementation	37
3.2.5 Monitoring	37
3.2.6 Management	38
3.3 Pengumpulan Data	38
BAB IV HASIL DAN PEMBAHASAN.....	41
4.1 Implementasi Konfigurasi Port Knocking.....	41
4.2 Pengujian Sistem.....	59
4.2.1 Implementasi Port Knocking	59
4.2.2 Implementasi Tanpa Port Knocking	62
4.2.3 Implementasi Dengan Port Knocking	67
4.3 Profil Bandwidth Line Rate	72
4.4 Skenario Pengujian Kualitas Jaringan.....	73
4.5 Analisa Jaringan.....	73
4.5.1 Pengambilan Data Jaringan.....	74
4.5.2 Perhitungan Data.....	74
4.5.2.1 Perhitungan Data Sebelum implementasi keamanan jaringan.....	75

4.5.2.2 Perhitungan Data Sesudah implementasi keamanan jaringan.....	77
BAB V KESIMPULAN DAN SARAN	80
5.1 Kesimpulan	80
5.2 Saran	82
DAFTAR PUSTAKA	84
RIWAYAT HIDUP	89
LAMPIRAN	90

DAFTAR GAMBAR

Gambar 3. 1 NDLC	31
Gambar 3. 2. Firewall.....	34
Gambar 3. 3. Topologi Jaringan	36
Gambar 3. 4. Pengumpulan Data.....	40
Gambar 4. 1. Konfigurasi Port 2000	41
Gambar 4. 2. Konfigurasi Port 2000	42
Gambar 4. 3. Konfigurasi Port 2000	43
Gambar 4. 4. Konfigurasi Port 2005	44
Gambar 4. 5. Konfigurasi Port 2005	45
Gambar 4. 6. Konfigurasi Port 2005	46
Gambar 4. 7. Konfigurasi Port 2010	47
Gambar 4. 8. Konfigurasi Port 2010	48
Gambar 4. 9. Konfigurasi Port 2010	49
Gambar 4. 10. Konfigurasi Keamanan Save-ip.....	50
Gambar 4. 11. Konfigurasi Keamanan Save-ip.....	51
Gambar 4. 12. Konfigurasi Keamanan Save-ip.....	52
Gambar 4. 13. Konfigurasi Keamanan Penyusup	53
Gambar 4. 14. Konfigurasi Keamanan Penyusup	54
Gambar 4. 15. Konfigurasi Keamanan Penyusup	55
Gambar 4. 16. Konfigurasi Keamanan Drop-penyusup	56
Gambar 4. 17. Konfigurasi Keamanan Drop-penyusup	57
Gambar 4. 18. Konfigurasi Keamanan Drop-penyusup	58
Gambar 4. 19. Hasil Konfigurasi Filter Rules.....	59
Gambar 4. 20. Melakukan knocking port 2000.....	60
Gambar 4. 21. Melakukan knocking port 2005 dan 2010.....	61
Gambar 4. 22. Login ke Telnet (port 23)	61
Gambar 4. 23. Tampilan di address list.....	62
Gambar 4. 24. Tampilan Port 21(ftp) tanpa port knocking	63

Gambar 4. 25. Tampilan Port 22(ssh) tanpa port knocking 64

Gambar 4. 26. Tampilan Port 23(telnet) tanpa port knocking 65

Gambar 4. 27. Tampilan Port 8291(winbox) tanpa port knocking..... 66

Gambar 4. 28. Tampilan Port 80(www) tanpa port knocking 66

Gambar 4. 29. Gambar tampilan penyusup 67

Gambar 4. 30. Tampilan Port 21(ftp) setelah melakukan knocking..... 68

Gambar 4. 31. Tampilan Port 22(ssh) setelah melakukan knocking..... 69

Gambar 4. 32. Tampilan Port 23(telnet) setelah melakukan knocking..... 70

Gambar 4. 33. Tampilan Port 8291(winbox) setelah melakukan knocking..... 71

Gambar 4. 34. Tampilan Port 80(www) setelah melakukan knocking..... 71

Gambar 4. 35. Grafik penggunaan selama 2 minggu 72

Gambar 4. 36. Tampilan record wireshark..... 74

DAFTAR TABEL

Tabel 2. 1. Studi Literatur	13
Tabel 2. 2. Standart Nilai QOS.....	24
Tabel 2. 3. Standart Troughput.....	25
Tabel 2. 4. Standart Delay	26
Tabel 2. 5. Standart Jitter.....	27
Tabel 2. 6. Standart Packetloss.....	28
Tabel 4. 1. Hasil grafik.....	72
Tabel 4. 2. Skenario pengujian.....	73
Tabel 4. 3 Hasil Perhitungan Data Sebelum Implementasi Keamanan Jaringan	76
Tabel 4. 4. Hasil Perhitungan Data Sebelum Implementasi Keamanan Jaringan.....	78
Tabel 4. 5. Tabel Indek QoS Keseluruhan	79