

**ANALISIS KEAMANAN JARINGAN BERBASIS MIKROTIK
DENGAN METODE PORT KNOCKING DAN AUTO-
BLOCKING**

TUGAS AKHIR



**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

ANALISIS KEAMANAN JARINGAN BERBASIS MIKROTIK DENGAN METODE PORT KNOCKING DAN AUTO- BLOCKING

Tugas Akhir

Skema Skripsi

Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar

Sarjana Teknik pada Program Studi Teknik Informatika



Dave Travis

NIM. 2201020008

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

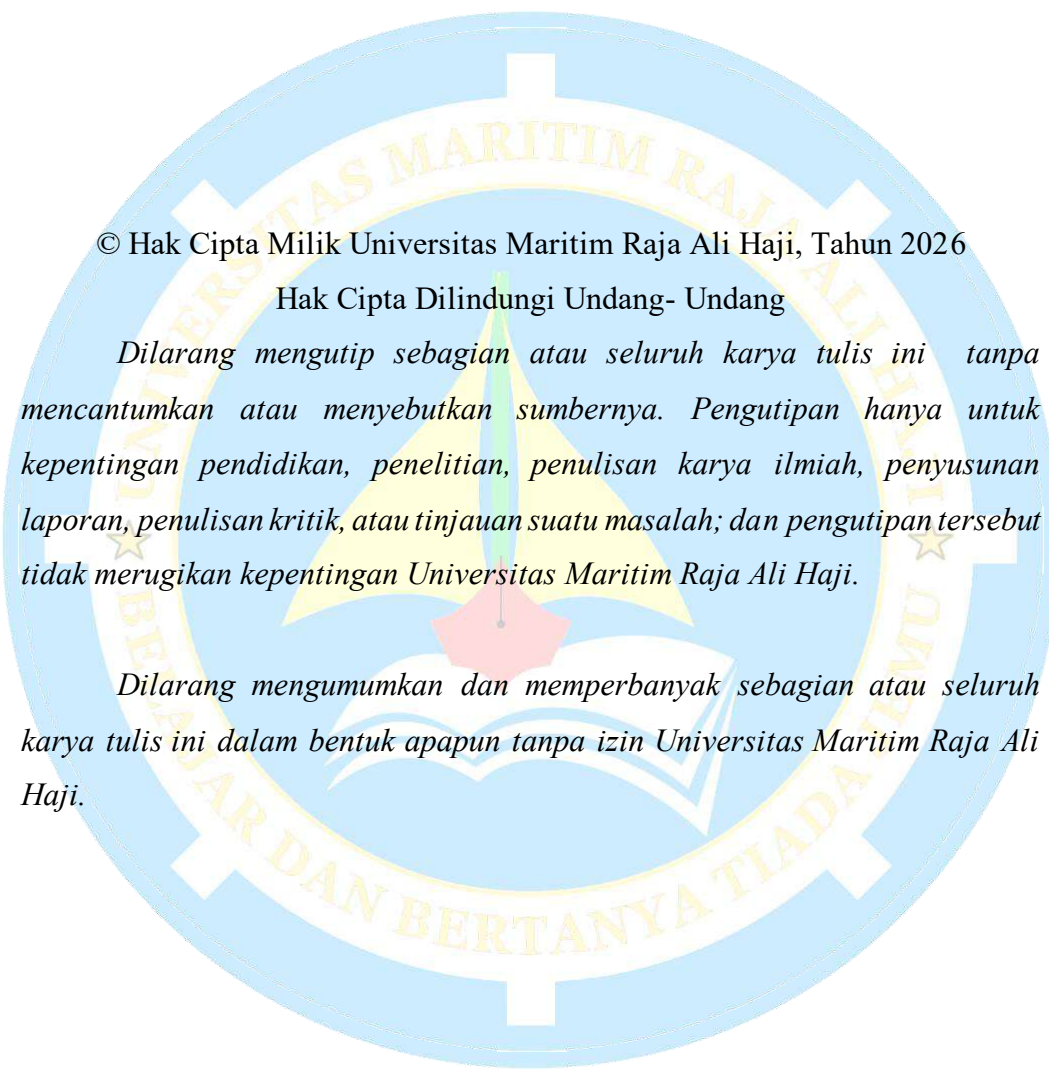
Dengan ini saya menyatakan bahwa tugas akhir berjudul “Analisis Keamanan Jaringan Berbasis MikroTik Dengan Metode *Port Knocking* dan *Auto-Blocking*” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, 23 Juli 2026



Dave Travis
NIM 2201020008



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2026

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.

HALAMAN PERSETUJUAN

Judul : Analisis Keamanan Jaringan Berbasis MikroTik
Dengan Metode *Port Knocking* dan *Auto-Blocking*
Nama : Dave Travis
NIM : 2201020008
Program Studi : Teknik Informatika
Tanggal Persetujuan : 30 Juni 2026

Disetujui oleh,
Komisi Pembimbing



Ferdi Chahyadi, S.Kom., M.Cs.
(Ketua)



Rifaldi Herikson, S.Kom., M.Kom.
(Anggota)

HALAMAN PENGESAHAN

Judul : Analisis Keamanan Jaringan Berbasis MikroTik
Dengan Metode *Port Knocking* dan *Auto-Blocking*
Nama : Dave Travis
NIM : 2201020008

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	(.....)
Anggota I	: Feri Irawan, S.Kom., M.Kom.	(.....)
Anggota II	: Berta Erwin SLAM, S.T., M.Kom.	(.....)
Anggota III	: Ferdi Chahyadi, S.Kom., M.Cs.	(.....)
Anggota IV	: Rifaldi Herikson, S.Kom., M.Kom.	(.....)

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika



Hollanda Arief Kusuma, S.IK., M.Si
NIP. 198904012019031016

Tanggal Ujian: 14 Juli 2026

Tanggal Lulus:

HALAMAN PERSEMBAHAN

Puji dan syukur penulis panjatkan ke hadirat Allah SWT. atas segala karunia dan anugerahnya yang telah dilimpahkan terhadap keseharian penulis sehingga masih sanggup melanjutkan hingga titik penulisan halaman ini, walaupun penulis telah berkali-kali memutuskan bahwa akhir dari proses yang ditempuh merupakan opsi yang terbaik saat menjalani kegiatan akademik ini pada suatu masa yang telah berlalu. Penulis juga sangat bersyukur atas kehadiran banyak orang yang senantiasa memberikan dukungan dan menemani setiap langkah perjalanan hidup penulis. Oleh karena itu, penulis mempersembahkan karya skripsi ini kepada:

1. Kedua orang tua tercinta, Alm. Pris Syafriadi dan Hartiyah. Terima kasih atas segala pengorbanan, doa, nasihat, cinta, serta kasih sayang yang telah diberikan kepada penulis selama ini. Terima kasih karena senantiasa memberikan kepercayaan, dukungan, dan semangat kepada penulis dalam setiap langkah dan keputusan yang diambil. Penulis merasa bersyukur dan bahagia karena dapat menepati salah satu janji terakhir kepada almarhum dengan menyelesaikan skripsi ini.
2. Bapak Ferdi Chahyadi, S.Kom., M.Cs. dan Bapak Rifaldi Herikson, S.Kom., M.Kom. selaku dosen pembimbing. Terima kasih atas waktu, bimbingan, arahan, serta masukan yang senantiasa diberikan dengan penuh kesabaran selama proses penyusunan skripsi ini, sehingga penulis dapat menyelesaikannya dengan baik.
3. Teman-teman penulis sejak masa mahasiswa baru, Anti Turu: Marcel Wangnandra, Grachiella Dian Malemukur, Aditya Firmansyah, M. Zaidan Nugroho, M. Noval, dan Faiz Arrafi. Terima kasih atas kebersamaan, dukungan, serta berbagai pengalaman yang telah dilalui bersama selama masa perkuliahan yang terasa begitu singkat.
4. Rekan daring penulis, Reytopia, Varian, dan Ciya. Terima kasih karena telah menemani keseharian penulis selama proses penyusunan skripsi ini, serta berbagi semangat dan kebersamaan melalui berbagai proyek animasi yang kami kerjakan bersama sebagai bagian dari hobi yang sama.
5. Partner kerja penulis, Clever Hooves, Obabscribbler, dan Nomad Flicker. Terima kasih atas kepercayaan yang telah diberikan kepada penulis untuk

memimpin berbagai proyek pribadi, serta atas karya-karya luar biasa yang menjadi sumber inspirasi dan memberikan pengalaman yang sangat berharga bagi penulis.

6. Kreator daring, SunnyNekoChan, Alumx, dan Aurelleah. Terima kasih atas karya yang telah menginspirasi penulis dan memberikan sudut pandang baru, sehingga penulis dapat lebih memahami dan mengenali jati diri selama menjalani berbagai proses dalam kehidupan.
7. Dana Terrace, kreator serial kartun The Owl House. Terima kasih atas karya yang telah memberikan inspirasi, semangat, serta menjadi salah satu sumber penguatan bagi penulis dalam menghadapi berbagai tantangan selama proses penyusunan skripsi ini.
8. Penulis karya fiksi, shortskirtandexplosion, Anzel, dan Crystal Wishes. Terima kasih atas karya-karya literatur yang telah memberikan inspirasi, motivasi, serta menjadi teman bagi penulis selama proses penyusunan skripsi, sehingga penulis dapat terus menjaga semangat untuk menyelesaikan penelitian ini.

Akhir kata, penulis menyadari bahwa skripsi ini tidak akan dapat terselesaikan tanpa doa, dukungan, kasih sayang, serta bantuan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah berkontribusi, baik secara langsung maupun tidak langsung, dalam proses penyusunan skripsi ini. Semoga segala kebaikan, perhatian, dan bantuan yang telah diberikan kepada penulis memperoleh balasan serta berkat yang melimpah dari Allah SWT. Penulis berharap semoga skripsi ini dapat memberikan manfaat, menambah wawasan, serta menjadi berkat bagi para pembaca dan semua pihak yang membutuhkannya.

PRAKATA

Puji syukur penulis panjatkan ke hadirat Allah *subhanahu wa ta'ala* atas segala karunia-Nya sehingga proposal tugas akhir ini berhasil diselesaikan. Topik yang dipilih dalam penelitian ini ialah keamanan jaringan, dengan rencana pelaksanaan pada bulan Maret 2026, berjudul **"Analisis Keamanan Jaringan Berbasis MikroTik Dengan Metode Port Knocking dan Auto-Blocking"**.

Penulis mengucapkan terima kasih kepada Bapak Ferdi Chahyadi, S.Kom., M.Cs. dan Bapak Rifaldi Herikson, S.Kom., M.Kom. yang telah banyak memberi saran dan bimbingan. Di samping itu, penghargaan penulis sampaikan kepada berbagai pihak yang telah membantu selama pembuatan proposal ini. Ungkapan terima kasih juga disampaikan kepada Alm. ayah, ibu, serta seluruh keluarga, atas segala doa dan kasih sayangnya.

Semoga proposal penelitian ini bermanfaat.

Tanjungpinang, 23 Juli 2026



Dave Travis

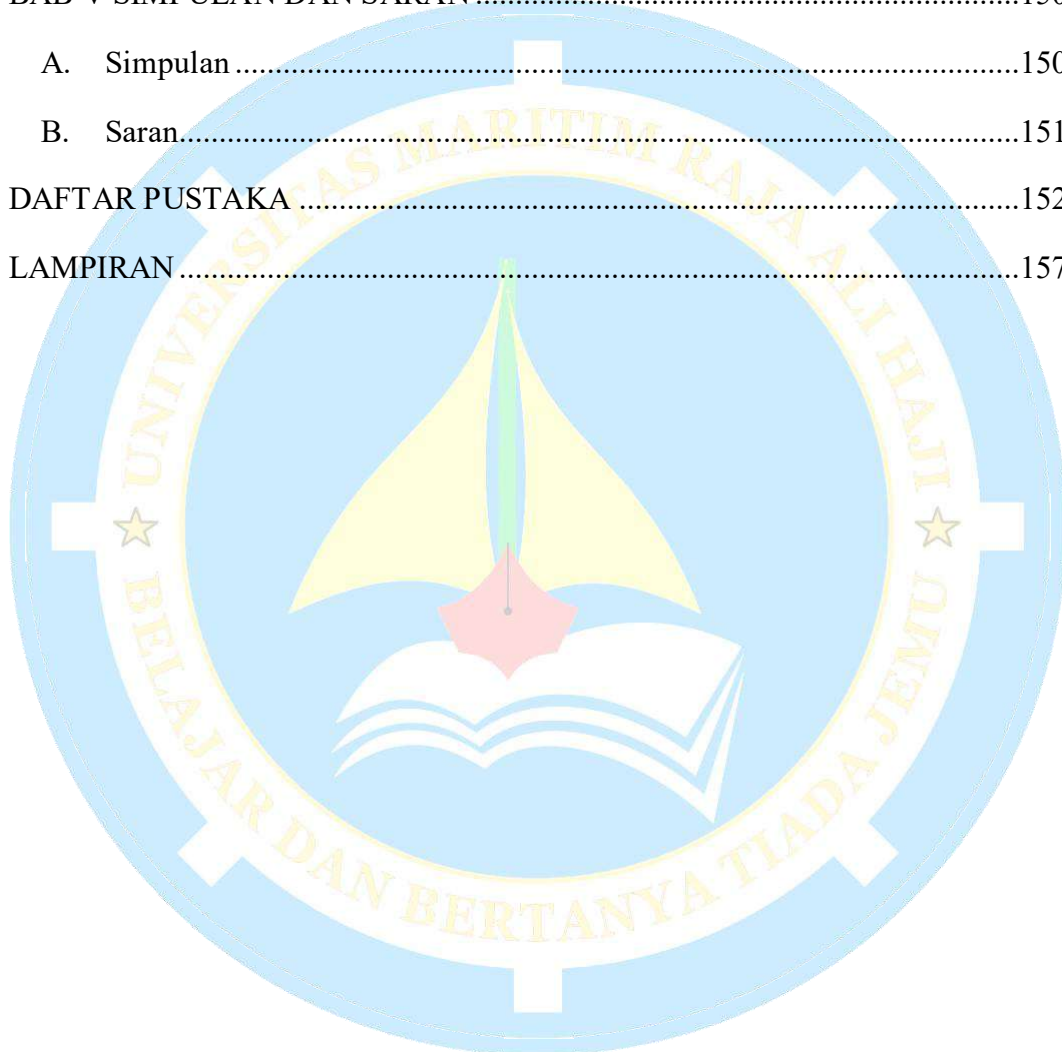
DAFTAR ISI

HALAMAN PERSETUJUAN	iv
HALAMAN PENGESAHAN	v
ABSTRAK	vi
ABSTRACT	vii
HALAMAN PERSEMBAHAN	viii
PRAKATA	x
DAFTAR ISI	xi
DAFTAR TABEL	xv
DAFTAR GAMBAR	xvii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Perumusan Masalah	6
C. Batasan Penelitian	6
D. Tujuan Penelitian	7
E. Manfaat Penelitian	7
BAB II KAJIAN LITERATUR	9
A. Tinjauan Pustaka	9
B. Landasan Teori	16
1. CIA Triad	16
2. Jaringan Komputer	17
3. Keamanan Jaringan	17
4. MikroTik	18
5. RouterOS	19
6. Port Knocking	20

7. Brute Force.....	21
8. Sniffing.....	23
9. Spoofing.....	23
10. WireGuard.....	24
11. L2TP/VPN.....	25
12. Bot Telegram.....	25
13. Design Science Research.....	27
14. NIST SP 800-115.....	29
15. Common Vulnerability Scoring System (CVSS).....	31
BAB III METODE PENELITIAN.....	33
A. Waktu dan Tempat Penelitian.....	33
B. Bahan dan Alat.....	34
C. Prosedur Pelaksanaan Penelitian.....	36
D. Perancangan Jaringan.....	51
1. Rancangan Jaringan LAN.....	51
2. Rancangan Jaringan WLAN.....	52
3. Rancangan Jaringan WAN.....	54
4. Rancangan Alur WireGuard.....	54
5. Rancangan RouterOS Script.....	56
E. Analisis Data.....	61
1. Kondisi Awal (Konfigurasi <i>Baseline</i>).....	62
2. Analisis Kondisi Kerentanan.....	63
3. Pasca Implementasi Model Keamanan.....	65
4. Parameter Evaluasi.....	68
BAB IV HASIL DAN PEMBAHASAN.....	72
A. Implementasi Rancangan Keamanan Jaringan.....	72

1. Konfigurasi Firewall	72
2. Konfigurasi Port Knocking dan Address-List.....	74
3. Konfigurasi VPS Transparent Relay	74
4. Konfigurasi WireGuard Tunnel	76
5. Konfigurasi RouterOS Scripts.....	79
B. Pengujian Tiap Kondisi.....	81
1. Pengujian Metode Auto-Blocking.....	81
2. Pengujian Metode Port Knocking	87
3. Pengujian Metode Gabungan (Hybrid)	92
C. Implementasi Antarmuka	102
D. Hasil Pengujian Skenario 1 (Auto-Blocking).....	103
1. Hasil Pengujian Reconnaissance & Sniffing.....	103
2. Hasil Pengujian Brute Force	105
3. Hasil Pengujian Knock Sequence & Knock Abuse	108
4. Hasil Pengujian IP Spoofing	111
E. Hasil Pengujian Skenario 2 (Port Knocking).....	114
1. Hasil Pengujian Reconnaissance & Sniffing.....	114
2. Hasil Pengujian Brute Force	117
3. Hasil Pengujian Knock Sequence & Knock Abuse	119
4. Hasil Pengujian IP Spoofing	122
F. Hasil Pengujian Skenario 3 (Hybrid: Port Knocking & Auto-Blocking).124	
1. Hasil Pengujian Reconnaissance & Sniffing.....	124
2. Hasil Pengujian Brute Force	131
3. Hasil Pengujian Knock Sequence & Knock Abuse	135
4. Hasil Pengujian IP Spoofing	139
G. Perbandingan Ketiga Skenario Pengujian.....	142

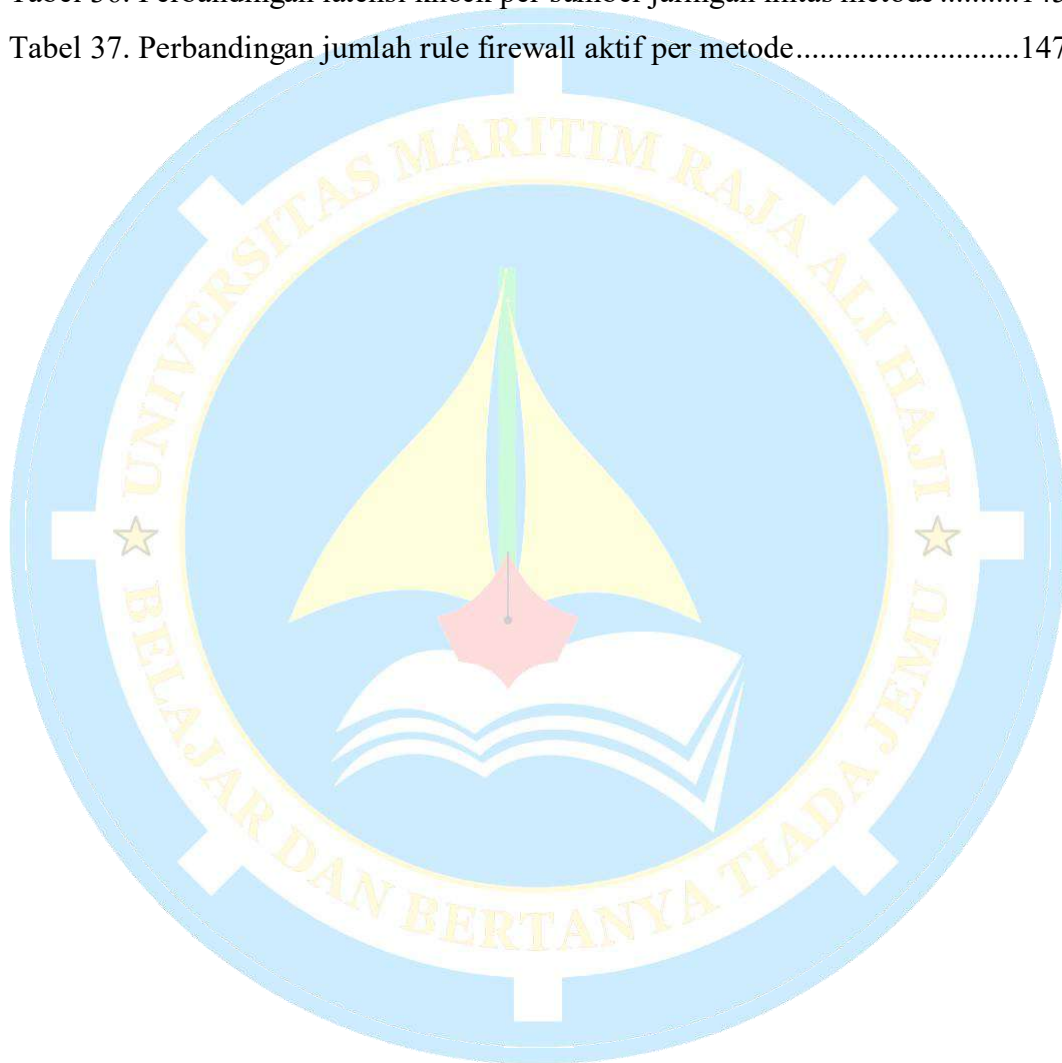
1. Perbandingan per Serangan.....	142
2. Perbandingan per Operasi Sistem	144
3. Perbandingan per Sumber Jaringan Serangan (LAN, WLAN, WAN)	145
4. Perbandingan Kompleksitas & Arsitektur Rule Firewall.....	146
5. Pembahasan.....	148
BAB V SIMPULAN DAN SARAN	150
A. Simpulan	150
B. Saran.....	151
DAFTAR PUSTAKA	152
LAMPIRAN	157



DAFTAR TABEL

Tabel 1. Tinjauan Pustaka.....	12
Tabel 2. Variabel pada tahapan <i>port knocking</i>	20
Tabel 3. Alat yang akan digunakan.....	34
Tabel 4. <i>Software</i> sebagai bahan yang akan digunakan.....	35
Tabel 5. Daftar rancangan skenario serangan	37
Tabel 6. Variabel Penelitian.....	39
Tabel 7. Daftar identifikasi konfigurasi awal.....	41
Tabel 8. Perangkat Uji Penelitian.....	42
Tabel 9. Rancangan Struktur Keamanan Jaringan	43
Tabel 10. Status verifikasi <i>pre-test</i>	45
Tabel 11. Matriks kondisi pengujian seluruh skenario	47
Tabel 12. Pemetaan tahapan, <i>script</i> , dan metrik pengujian per kondisi.....	48
Tabel 13. Perbandingan analisis data.....	50
Tabel 14. Tahapan <i>cascade</i> deteksi penyalahgunaan <i>knock sequence</i>	58
Tabel 15. Ilustrasi analisis temuan kerentanan pada kondisi <i>baseline</i>	64
Tabel 16. Parameter evaluasi data.....	68
Tabel 17. Perbandingan hasil pengujian antar sumber jaringan.....	69
Tabel 18. Hasil pengujian <i>port before-after</i> pada metode <i>auto-blocking</i>	104
Tabel 19. Hasil pengujian <i>reconnaissance & sniffing</i> metode <i>auto-blocking</i>	105
Tabel 20. Hasil pengujian <i>brute force</i> pada metode <i>auto-blocking</i>	108
Tabel 21. Hasil pengujian <i>knock sequence & knock abuse</i> metode <i>auto-blocking</i>	110
Tabel 22. Hasil pengujian IP <i>spoofing</i> pada metode <i>auto-blocking</i>	113
Tabel 23. Hasil pengujian <i>reconnaissance & sniffing</i> metode <i>port knocking</i>	117
Tabel 24. Hasil pengujian <i>brute force</i> pada metode <i>port knocking</i>	119
Tabel 25. Hasil pengujian <i>knock sequence & knock abuse</i> metode <i>port knocking</i>	121
Tabel 26. Hasil pengujian IP <i>spoofing</i> pada metode <i>port knocking</i>	124
Tabel 27. Rekap status <i>port</i> per kondisi pengujian.....	126
Tabel 28. Keterbacaan <i>knock sequence</i> per kondisi pengujian	130
Tabel 29. Rekap <i>Sfail</i> , <i>Tdetect</i> , dan R per kondisi pengujian	133

Tabel 30. Hasil pengujian <i>brute force</i> metode gabungan.....	135
Tabel 31. Rekap <i>Kabuse</i> dan <i>Tknock</i> per kondisi pengujian	137
Tabel 32. Hasil <i>knock sequence & knock abuse detection</i> metode gabungan.....	138
Tabel 33. Rekap <i>Sspoof</i> dan status akses pasca- <i>spoofing</i> per kondisi	141
Tabel 34. Perbandingan efektivitas ketiga metode per jenis serangan.....	142
Tabel 35. Perbandingan <i>Sfail</i> dan <i>Tdetect</i> lintas OS per metode	144
Tabel 36. Perbandingan latensi knock per sumber jaringan lintas metode	145
Tabel 37. Perbandingan jumlah rule firewall aktif per metode.....	147



DAFTAR GAMBAR

Gambar 1. CIA Triad	17
Gambar 2. Router MikroTik RB750r2 (hEX-Lite).....	18
Gambar 3. Alur kerja <i>brute force</i>	22
Gambar 4. Struktur diagram WireGuard.....	24
Gambar 5. Alur kerja Bot Telegram.....	26
Gambar 6. Alur tahapan metode DSR.....	27
Gambar 7. <i>Flowchart</i> alur DSR	28
Gambar 8. Alur tahapan metode <i>pentest</i> berdasarkan NIST SP 800-115	29
Gambar 9. Alur tahapan <i>pentest</i> NIST SP 800-115	30
Gambar 10. Alur kerja CVSS.....	31
Gambar 11. Peta lokasi penelitian.....	33
Gambar 12. Alur Prosedur Pelaksanaan Penelitian.....	36
Gambar 13. <i>Flowchart</i> pre-test tiap skenario.....	44
Gambar 14. Alur pelaksanaan pengujian seluruh skenario.....	46
Gambar 15. Rincian prosedur pengujian per kondisi.....	48
Gambar 16. Ilustrasi rancangan topologi jaringan LAN	51
Gambar 17. Ilustrasi rancangan topologi jaringan WLAN	52
Gambar 18. Ilustrasi rancangan topologi jaringan WAN.....	54
Gambar 19. Ilustrasi rancangan alur WireGuard	55
Gambar 20. Alur mekanisme <i>port knocking sequence</i>	56
Gambar 21. Alur deteksi penyalahgunaan <i>knock sequence</i>	57
Gambar 22. Alur Notifikasi Bot Telegram.....	59
Gambar 23. Alur rancangan <i>script</i> deteksi <i>brute force</i>	60
Gambar 24. Rumus logika evaluasi Pemblokiran IP.....	60
Gambar 25. URL untuk mengirimkan pesan ke bot Telegram	61
Gambar 26. Hasil <i>scanning</i> menggunakan Nmap kondisi awal.....	62
Gambar 27. Hasil <i>brute force</i> menggunakan Hydra kondisi awal.....	62
Gambar 28. Hasil log sistem dari MikroTik kondisi awal	63
Gambar 29. Rancangan Antarmuka Pengguna	64
Gambar 30. Hasil <i>scanning</i> menggunakan Nmap pasca implementasi	66
Gambar 31. Hasil <i>brute force</i> menggunakan Hydra pasca implementasi.....	66

Gambar 32. Hasil log sistem dari MikroTik pasca implementasi	67
Gambar 33. Hasil notifikasi bot Telegram pasca implementasi.....	67
Gambar 34. <i>Firewall</i> tabel RAW RouterOS	72
Gambar 35. Tabel <i>chain input firewall filter</i>	73
Gambar 36. Aturan <i>anti-spoofing</i> pada <i>chain input</i>	73
Gambar 37. Tampilan <i>address-list</i> status <i>timeout</i> penyerang.....	74
Gambar 38. Aturan <i>iptables rules</i> pada VPS	75
Gambar 39. Status <i>tunnel L2TP</i> pada VPS	76
Gambar 40. Konfigurasi <i>WireGuard interface</i> pada RouterOS.....	77
Gambar 41. Konfigurasi <i>WireGuard peer</i> pada RouterOS.....	77
Gambar 42. Konfigurasi <i>WireGuard client</i> pada Admin PC	78
Gambar 43. Status <i>tunnel WireGuard</i> aktif.....	79
Gambar 44. Daftar <i>scheduler</i> yang digunakan untuk pengujian.....	80
Gambar 45. Daftar <i>script</i> yang digunakan untuk pengujian	80
Gambar 46. Log terminal Nmap hasil <i>scanning</i> metode <i>auto-blocking</i>	81
Gambar 47. Log Wireshark menampilkan banner SSH pada sebuah paket.....	82
Gambar 48. Log terminal Hydra hasil <i>brute force</i> metode <i>auto-blocking</i>	83
Gambar 49. Log MikroTik pasca pemblokiran akses <i>user valid</i>	84
Gambar 50. Log Nmap pada port 7000 dan 8000.....	85
Gambar 51. Log MikroTik pasca <i>probing port</i> 7000 dan 8000.....	85
Gambar 52. Log <i>address-list</i> pada <i>list Blocked_IPs</i> pasca <i>spoofing IP</i>	86
Gambar 53. Log terminal Nmap pasca <i>scanning</i> metode <i>port knocking</i>	87
Gambar 54. Log Wireshark terhadap <i>knock sequence</i> tanpa WireGuard	88
Gambar 55. Log Wireshark terhadap <i>knock sequence</i> dengan WireGuard.....	89
Gambar 56. Log terminal Hydra yang gagal <i>connect</i> pada metode <i>port knocking</i>	89
Gambar 57. Log terminal hping3 terhadap <i>probing port</i> acak pada <i>port knocking</i>	90
Gambar 58. Log <i>address-list</i> yang kosong setelah <i>knock abuse</i> pada <i>port knocking</i>	91
Gambar 59. Log status filter MikroTik terhadap deteksi <i>knock abuse</i>	91
Gambar 60. Log terminal SSH yang berhasil spoofing IP	92
Gambar 61. Terminal Nmap saat dijalankan.....	93

Gambar 62. Wireshark aktif dari sisi penyerang.....	94
Gambar 63. Terminal Hydra saat dijalankan	95
Gambar 64. Log terminal Hydra tanpa dan setelahh knock valid metode hybrid..	96
Gambar 65. Log MikroTik dari sisi administrator selama Hydra dijalankan	97
Gambar 66. Log address-list knock_1 dan knock_2 <i>sequence valid</i>	98
Gambar 67. <i>Address-list</i> RouterOS selama <i>knock abuse</i> berlangsung.....	99
Gambar 68. Terminal hping3 saat persiapan IP <i>Spoofing</i>	101
Gambar 69. Tampilan <i>dashboard</i> analisis CVSS.....	102
Gambar 70. Tampilan <i>dashboard</i> visualisasi data via data csv	103
Gambar 71. Log terminal Nmap hasil <i>scanning</i> fase <i>After</i>	103
Gambar 72. Log terminal Hydra pasca <i>brute force</i> pada metode <i>auto-blocking</i> ..	106
Gambar 73. Data csv bagian metrik pengujian <i>brute force</i> fase <i>after auto-blocking</i>	106
Gambar 74. Log MikroTik pasca blokir IP pada <i>auto-blocking</i>	107
Gambar 75. Log MikroTik yang menunjukkan pemblokiran administrator.....	107
Gambar 76. Log terminal Nmap <i>port</i> 7000, 8000 pada metode <i>auto-blocking</i> ...	109
Gambar 77. Data csv metrik pengujian <i>knock abuse</i> fase <i>after auto-blocking</i>	109
Gambar 78. Log MikroTik kosong tanpa <i>probing</i> pada metode <i>auto-blocking</i> ...	110
Gambar 79. Log ARP table yang menampilkan MAC address penyerang.....	111
Gambar 80. Data csv metrik pengujian <i>anti-spoofing</i> fase <i>after auto-blocking</i> ..	112
Gambar 81. Log firewall bogon dari sisi WAN pada metode <i>auto-blocking</i>	112
Gambar 82. Log terminal Nmap pada metode <i>port knocking</i>	114
Gambar 83. Data csv bagian metrik <i>reconnaissance</i> fase <i>after port knocking</i>	115
Gambar 84. Log Wireshark <i>plaintext knock sequence</i> tanpa WireGuard.....	115
Gambar 85. Log Wireshark enkripsi WireGuard urutan <i>knock sequence</i>	116
Gambar 86. Log terminal Hydra gagal <i>connect</i> ke <i>port</i> 22 pada <i>port knocking</i> ..	117
Gambar 87. Data csv bagian metrik pengujian <i>brute force</i> fase <i>after port knocking</i>	118
Gambar 88. Log terminal hping3 <i>probing port</i> acak metode <i>port knocking</i>	120
Gambar 89. Data csv metrik pengujian <i>knock abuse</i> fase <i>after auto-blocking</i>	120
Gambar 90. Log address-list Knock_Fail tanpa pemblokiran pada <i>port knocking</i>	121

Gambar 91. Log terminal SSH berhasil pasca IP <i>Spoofing</i> pada <i>port knocking</i> ..	122
Gambar 92. Data csv metrik pengujian <i>anti-spoofing</i> fase <i>after port knocking</i> ..	123
Gambar 93. Log ARP table yang menampilkan MAC <i>address</i> penyerang	123
Gambar 94. Log terminal Nmap <i>scan result</i> pada fase <i>Before</i>	125
Gambar 95. <i>Screenshot</i> Wireshark <i>capture</i> pada fase <i>Before</i>	125
Gambar 96. <i>Screenshot</i> Nmap <i>scan result</i> pada fase <i>After</i>	126
Gambar 97. Data csv metrik pengujian <i>reconnaissance</i> pada metode hybrid	127
Gambar 98. <i>Screenshot Wireshark capture sniffing port sequence</i> fase <i>Before</i> ..	128
Gambar 99. <i>Screenshot Wireshark capture sniffing port sequence</i> fase <i>After</i>	129
Gambar 100. <i>Screenshot</i> Hydra <i>output</i> pada fase <i>Before</i>	131
Gambar 101. <i>Screenshot</i> log MikroTik pada fase <i>Before</i>	132
Gambar 102. <i>Screenshot</i> Hydra <i>output</i> pada fase <i>After</i>	132
Gambar 103. Tampilan log MikroTik pada fase <i>After</i>	133
Gambar 104. Tampilan notifikasi Bot Telegram	133
Gambar 105. Data csv metrik <i>brute force</i> metode gabungan.....	134
Gambar 106. Tampilan proses di mana <i>knock sequence</i> berhasil.....	136
Gambar 107. Tampilan log MikroTik kondisi <i>knock abuse Track A</i>	136
Gambar 108. Tampilan log MikroTik kondisi <i>knock abuse Track B</i>	136
Gambar 109. Data csv metrik pengujian <i>knock abuse</i> metode gabungan.....	137
Gambar 110. <i>Hit counter</i> aturan MAC <i>whitelist</i> pada RAW <i>table</i>	139
Gambar 111. Tampilan <i>hit counter</i> pada <i>interface</i> TRUE_WAN	140