

**IMPLEMENTASI METODE PORT KNOCKING SEBAGAI
PENCEGAHAN SERANGAN SNIFFING DAN BRUTEFORCE
PADA AKSES LOGIN ROUTER MIKROTIK**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

HERDAN ADIYOCE ATMAJA

19.11.2628

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**IMPLEMENTASI METODE PORT KNOCKING SEBAGAI
PENCEGAHAN SERANGAN SNIFFING DAN BRUTEFORCE
PADA AKSES LOGIN ROUTER MIKROTIK**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

**HERDAN ADIYOCE ATMAJA
19.11.2628**

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023**

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI METODE PORT KNOCKING SEBAGAI PENCEGAHAN
SERANGAN SNIFFING DAN BRUTEFORCE PADA AKSES LOGIN ROUTER
MIKROTIK**

yang disusun dan diajukan oleh

Herdan Adiyoce Atmaja

19.11.2628

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Mei 2023

Dosen Pembimbing,



Majid Rahardi, S.Kom., M.Eng

NIK. 19030xxxx

HALAMAN PENGESAHAN
SKRIPSI
IMPLEMENTASI METODE PORT KNOCKING SEBAGAI PENCEGAHAN
SERANGAN SNIFFING DAN BRUTEFORCE PADA AKSES LOGIN ROUTER
MIKROTIK

yang disusun dan diajukan oleh

Herdan Adiyoce Atmaja

19.11.2628

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Mei 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ainul Yaqin, M.Kom
NIK. 190302255

Uyock Anggoro Saputro, M.Kom
NIK. 190302419

Majid Rahardi, S.Kom., M.Eng
NIK. 190302393



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Mei 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Herdan Adiyoce Atmaja
NIM : 19.11.2628

Menyatakan bahwa Skripsi dengan judul berikut:

Implementasi Metode Port Knocking sebagai Pencegahan Serangan Sniffing dan Bruteforce pada Akses Login Router Mikrotik

Dosen Pembimbing : Majid Rahardi, S.Kom., M.Eng

1. Karya tulis ini adalah benar-benar **ASLI** dan **BELUM PERNAH** diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian **SAYA** sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab **SAYA**, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini **SAYA** buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka **SAYA** bersedia menerima **SANKSI AKADEMIK** dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 29 Mei 2023

Yang Menyatakan,



Herdan Adiyoce Atmaja

HALAMAN PERSEMBAHAN

Skripsi ini saya persembahkan untuk Ayah dan Ibu, terima kasih atas doa, semangat, motivasi, pengorbanan, nasihat serta kasih sayang yang tidak pernah henti sampai saat ini.

Skripsi ini juga saya persembahkan untuk Bapak dan Ibu Dosen Program Studi Informatika yang selalu memberikan yang terbaik bagi mahasiswanya, terutama Bapak Majid Rahardi, S.Kom., M.Eng selaku pembimbing saya. Terima kasih karena telah memberikan bantuan, semangat, dan doa sehingga skripsi ini dapat diselesaikan.



KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah SWT Sang Maha Segalanya, atas seluruh curahan rahmat dan hidayat Nya sehingga penulis mampu menyelesaikan skripsi yang berjudul “IMPLEMENTASI METODE PORT KNOCKING SEBAGAI PENCEGAHAN SERANGAN SNIFFING DAN BRUTEFORCE PADA AKSES LOGIN ROUTER MIKROTIK” ini tepat pada waktunya. Skripsi ini ditulis dalam rangka memenuhi syarat untuk mencapai gelar Sarjana Komputer pada Program Studi Informatika Universitas Amikom Yogyakarta.

Dalam penyelesaian studi dan penulisan skripsi ini, penulis banyak memperoleh bantuan baik pengajaran, bimbingan dan arahan dari berbagai pihak baik secara langsung maupun tidak langsung. Untuk itu penulis menyampaikan penghargaan dan terima kasih yang tak terhingga kepada:

1. Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al-Fatta, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Majid Rahardi, S.Kom., M.Eng., selaku Dosen Pembimbing yang telah meluangkan waktu ditengah kesibukan beliau, memberikan kritik, saran dan pengarahan kepada Penulis dalam proses penulisan skripsi ini.
4. Segenap Dosen Prodi Informatika yang telah mendidik dan memberikan ilmu selama kuliah dan seluruh staf yang selalu sabar melayani segala administrasi selama proses penelitian ini.
5. Semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Yogyakarta, 29 Mei 2023

Penulis



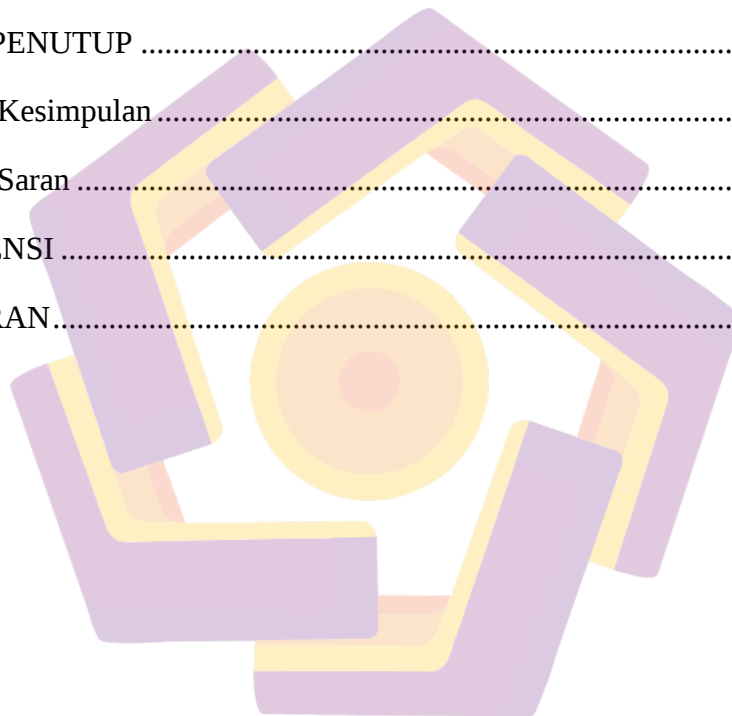
DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN.....	xiii
INTISARI	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA.....	5
2.1 Studi Literatur	5
2.2 Dasar Teori	12
2.2.1 Router.....	12

2.2.2	Mikrotik	12
2.2.3	Putty	12
2.2.4	Wireshark	12
2.2.5	Nmap	13
2.2.6	Sniffing	13
2.2.7	Port	13
2.2.8	Port Scanning	14
2.2.9	Port Knocking	14
2.2.10	Brute Force	15
2.2.11	Firewall	15
2.2.12	TCP/IP	15
2.2.13	FTP	16
2.2.14	SSH	16
2.2.15	Telnet	16
2.2.16	WebFig	17
2.2.17	Winbox	17
BAB III METODE PENELITIAN		18
3.1	Objek Penelitian	18
3.2	Alur Penelitian	18
3.2.1	Tahap Analysis	19
3.2.1.1	Analisa Kebutuhan	19
3.2.1.2	Analisa Permasalahan	19
3.2.1.3	Analisa Keinginan Pengguna	20
3.2.1.4	Analisa Topologi Jaringan	20
3.2.2	Tahap <i>Design</i>	20

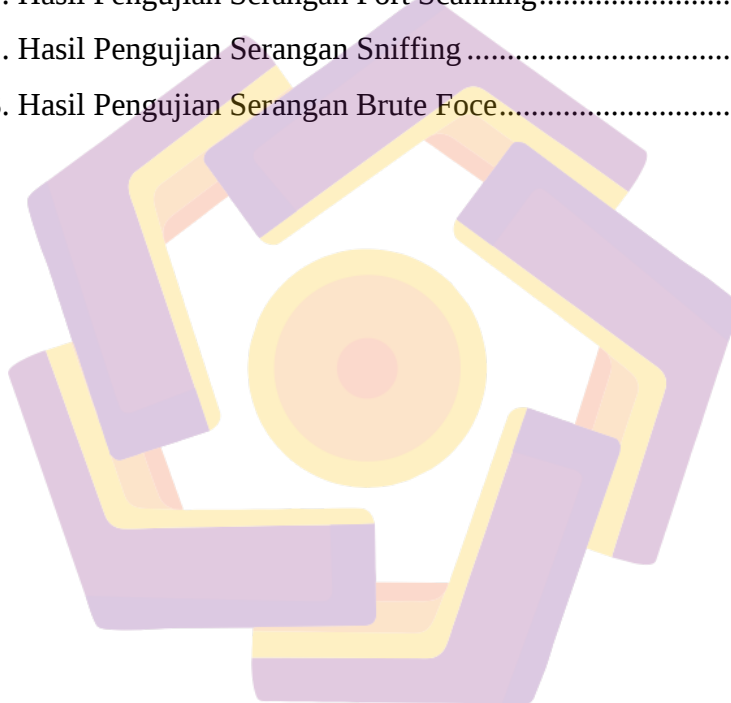
3.2.3	Tahap Simulation Prototyping	21
3.2.4	Tahap Implementation	21
3.2.4.1	Konfigurasi IP Address	22
3.2.4.2	Konfigurasi Port Knocking	22
3.2.4.3	Use Case System	22
3.2.4.4	Alur Autentikasi Port Knocking.....	23
3.2.6	Tahap Management.....	24
3.3	Analisa Kebutuhan Sistem.....	24
3.3.1	Kebutuhan Perangkat Keras.....	24
3.3.2	Kebutuhan Perangkat Lunak.....	26
BAB IV HASIL DAN PEMBAHASAN		27
4.1	Rule Konfigurasi.....	27
4.1.1	Knock Port	28
4.1.2	Safe IP	29
4.1.3	Penyusup	30
4.1.4	Drop	32
4.2	Pengujian Serangan.....	34
4.2.1	Port Scanning	34
4.2.2	Sniffing	36
4.2.2.1	FTP (21)	36
4.2.2.2	SSH (22).....	38
4.2.2.3	Telnet (23)	39
4.2.2.4	WebFig (80)	41
4.2.2.5	Winbox (8291)	42
4.2.3	Brute Force.....	43

4.2.3.1	FTP.....	44
4.2.3.2	SSH.....	45
4.2.3.3	Telnet.....	46
4.3	Hasil Pengujian.....	47
4.3.1	Hasil Pengujian Port Scanning.....	48
4.3.2	Hasil Pengujian Sniffing.....	50
4.3.3	Hasil Pengujian Brute Force.....	53
BAB V PENUTUP		56
5.1	Kesimpulan.....	56
5.2	Saran	57
REFERENSI		58
LAMPIRAN.....		61



DAFTAR TABEL

Tabel 2.1. Keaslian Penelitian.....	7
Tabel 3.1. Konfigurasi IP Address.....	22
Tabel 3.2. Konfigurasi Port Knocking	22
Tabel 3.3. Spesifikasi Laptop User 1	24
Tabel 3.4. Spesifikasi Laptop User 2	24
Tabel 3.5. Spesifikasi Router	25
Tabel 4.1. Hasil Pengujian Serangan Port Scanning.....	48
Tabel 4.2. Hasil Pengujian Serangan Sniffing	51
Tabel 4.3. Hasil Pengujian Serangan Brute Force.....	54

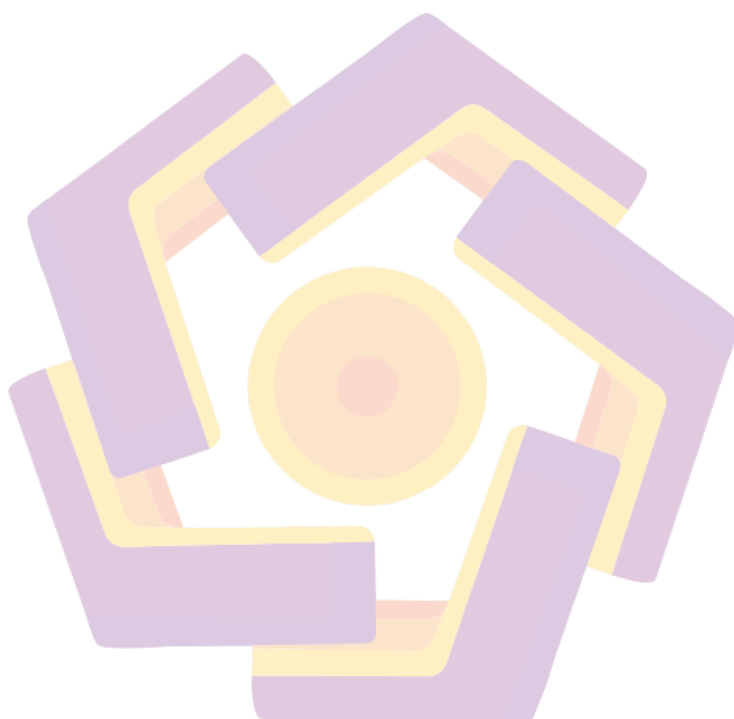


DAFTAR GAMBAR

Gambar 3.1. Alur Penelitian	19
Gambar 3.2. Topologi Jaringan.....	20
Gambar 3.3. Simulation Prototyping	21
Gambar 3.4. Use Case System	22
Gambar 3.5. Alur Autentikasi	23
Gambar 4.1. Rule Konfigurasi Firewall.....	27
Gambar 4.2. Rule Knock Port Tab General	28
Gambar 4.3. Rule Knock Port Tab Action.....	28
Gambar 4.4. Rule Safe IP Tab General.....	29
Gambar 4.5. Rule Safe IP Tab Advanced	30
Gambar 4.6. Rule Safe IP Tab Action	30
Gambar 4.7. Rule Penyusup Tab General.....	31
Gambar 4.8. Rule Penyusup Tab Advanced	31
Gambar 4.9. Rule Penyusup Tab Action.....	32
Gambar 4.10. Rule Drop Tab General	32
Gambar 4.11. Rule Drop Tab Advanced.....	33
Gambar 4.12. Rule Drop Tab Action.....	33
Gambar 4.13. Dalam Mode Normal tanpa Port Knocking.....	34
Gambar 4.14. Dalam Mode Port Knocking Aktif	35
Gambar 4.15. FTP Sebelum Port Knocking di Aktifkan	36
Gambar 4.16. FTP Setelah Port Knocking di Aktifkan	37
Gambar 4.17. Gagal Login WinSCP.....	37
Gambar 4.18. SSH Sebelum Port Knocking di Aktifkan.....	38
Gambar 4.19. SSH Setelah Port Knocking di Aktifkan	39
Gambar 4.20. Telnet Sebelum Port Knocking di Aktifkan.....	39
Gambar 4.21. Telnet Setelah Port Knocking di Aktifkan	40
Gambar 4.22. WebFig Sebelum Port Knocking di Aktifkan	41
Gambar 4.23. WebFig Setelah Port Knocking di Aktifkan	41
Gambar 4.24. Tidak dapat Mengakses Menu Login	42
Gambar 4.25. Winbox Sebelum Port Knocking di Aktifkan	42
Gambar 4.26. Winbox Setelah Port Knocking di Aktifkan	43
Gambar 4.27. Brute Force FTP Sebelum Port Knocking di Aktifkan	44
Gambar 4.28. Brute Force FTP Setelah Port Knocking di Aktifkan	44
Gambar 4.29. Brute Force SSH Sebelum Port Knocking di Aktifkan.....	45
Gambar 4.30. Brute Force SSH Setelah Port Knocking di Aktifkan	45
Gambar 4.31. Brute Force Telnet Sebelum Port Knocking di Aktifkan	46
Gambar 4.32. Brute Force Telnet Setelah Port Knocking di Aktifkan	47

DAFTAR LAMPIRAN

Lampiran 1. Dokumentasi Penelitian.....	61
---	----



INTISARI

Router merupakan suatu perangkat yang berperan penting dalam proses menghubungkan jaringan internet terutama untuk mengatur keluar dan masuknya data pada suatu jaringan. Banyak yang menjadikan router sebagai target serangan oleh orang-orang tidak bertanggung jawab, karena perangkat router ini secara langsung berada pada lapisan terluar yang terhubung ke jaringan publik. Dengan begitu banyak serangan, salah satu contoh serangan yang paling umum adalah dengan menggunakan packet sniffing atau bahasa umumnya adalah penyadapan, hal ini terjadi karena komunikasi yang bersifat terbuka dan sudah banyak yang menjadi korban dari serangan ini. Serangan tersebut terjadi pada port-port yang terbuka, sehingga akan dengan mudah orang-orang yang tidak mempunyai hak akses pada perangkat maupun yang tidak berkepentingan untuk dapat masuk ke dalamnya. Untuk mengantisipasi hal tersebut, maka dalam penelitian ini penulis akan menggunakan metode Port Knocking. Dimana fungsi dari metode Port Knocking ini adalah untuk menjaga hak akses perangkat Router dari pengguna yang tidak bertanggung jawab untuk mengaksesnya. Dengan metode Port Knocking penulis melakukan uji coba terhadap keamanan dari sebuah port yang menggunakan Port Knocking pada router, hal tersebut dilakukan untuk mengetahui seberapa aman metode Port Knocking dalam melindungi suatu port. Dalam penelitian ini penulis menggunakan sebuah perangkat Router Mikrotik RB941 lalu dengan menggunakan software winbox untuk memantau dan melakukan konfigurasi, dan juga dengan memakai layanan web pada webfig winbox yang sudah ada pada router mikrotik itu sendiri.

Kata Kunci : Keamanan Jaringan, Port Knocking, Packet Sniffing, Router, Mikrotik

ABSTRACT

Router is a device that plays an important role in the process of connecting the internet network, especially to regulate the entry and exit of data on a network. Many make routers the target of attacks by irresponsible people, because these router devices are directly on the outermost layer connected to the public network. With so many attacks, one of the most common examples of attacks is to use packet sniffing or the common language is wiretapping, this happens because of open communication and many have become victims of this attack. These attacks occur on open ports, so it will be easy for people who do not have access rights to the device or who are not interested in getting into it. To anticipate this, in this study the author will use the Port Knocking method. Where the function of the Port Knocking method is to maintain the access rights of the Router device from users who are not responsible for accessing it. With the Port Knocking method, the author tests the security of a port that uses Port Knocking on the router, this is done to find out how safe the Port Knocking method is in protecting a port. In this study the author uses a Mikrotik RB941 Router device and then uses Winbox software to monitor and configure, and also by using web services on the Winbox WebFig that already exists on the Mikrotik router itself.

Keyword : Network Security, Port Knocking, Packet Sniffing, Router, Mikrotik