

**OPTIMALISASI SISTEM KEAMANAN JARINGAN SSH DARI
SERANGAN BRUTE FORCE MENGGUNAKAN PORT
KNOCKING DAN PORT BLOCKING PADA ROUTER
MIKROTIK**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat
mencapai derajat Sarjana program studi Informatika



Disusun oleh

Lucky Anton Yudhistira

19.11.2609

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**OPTIMALISASI SISTEM KEAMANAN JARINGAN SSH DARI
SERANGAN BRUTE FORCE MENGGUNAKAN PORT
KNOCKING DAN PORT BLOCKING PADA ROUTER
MIKROTIK**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat
mencapai derajat Sarjana program studi Informatika



Disusun oleh

Lucky Anton Yudhistira

19.11.2609

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

i

HALAMAN PERSETUJUAN

**SKRIPSI
OPTIMALISASI SISTEM KEAMANAN JARINGAN SSH DARI
SERANGAN BRUTE FORCE MENGGUNAKAN PORT KNOCKING DAN
PORT BLOCKING PADA ROUTER MIKROTIK**

yang disusun dan diajukan oleh

**Lucky Anton yudhistira
19.11.2609**

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 21 Desember 2022

Dosen Pembimbing,

**Sudarmawan, S.T.,M.T
NIK. 190302035**

HALAMAN PENGESAHAN

SKRIPSI

**OPTIMALISASI SISTEM KEAMANAN JARINGAN SSH DARI
SERANGAN BRUTE FORCE MENGGUNAKAN PORT KNOCKING DAN
PORT BLOCKING PADA ROUTER MIKROTIK**

yang disusun dan diajukan oleh

Lucky Anton yudhistira
19.11.2609

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Desember 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Erni Seniwati, S.Kom, M.Cs
NIK. 190302231

Banu Santoso, S.T., M.Eng.
NIK. 190302327

Sudarmawan, S.T., M.T
NIK. 190302035

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Desember 2022

DEKAN FAKULTAS ILMU KOMPUTER



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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Lucky Anton Yudhistira
NIM : 19.11.2609

Menyatakan bahwa Skripsi dengan judul berikut:
**OPTIMALISASI SISTEM KEAMANAN JARINGAN SSH DARI
SERANGAN BRUTE FORCE MENGGUNAKAN PORT KNOCKING DAN
PORT BLOCKING PADA ROUTER MIKROTIK**

Dosen Pembimbing : Sudarmawan, S.T., M.T

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, 21 Desember 2022

Yang Menyatakan,


Lucky Anton Yudhistira

PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT, atuhan yang Maha Esa dan atas dukungan doa dari orang tua dan orang-orang tercinta, alhamdulillah skripsi ini dapat diselesaikan dengan baik dan tepat pada waktunya. Dengan rasa bahagia dan bangga saya ucapkan rasa syukur dan terimakasih kepada :

1. Allah SWT atas rahmat, anugrah, dan karunianya yang telah diberikan kepada kita semua, sehingga atas ijin Allah lah saya bisa seperti ini
2. Ibu dan Bapak serta keluarga besar saya yang tak henti-hentinya senantiasa memberi support dari materi sampai doa untuk kesuksesan saya, karena tiada doa mujarab selain doa orang tua kita sendiri, Terimakasih Ibu dan Bapak yang sudah banyak membiayai sampai lulus S1.
3. Dosen Pembimbing, penguji yang tulus dan ikhlas membimbing dan mengarahkan serta meluangkan waktunya agar saya menjadi lebih baik lagi.

Terimakasih yang sebesar-besarnya untuk kalian semua, akhir kata saya persembahkan skripsi ini untuk kalian semua dan semoga skripsi ini dapat memberikan manfaat yang banyak bagi semua pihak serta semua orang yang telah mensupport saya dalam menempuh skripsi ini, amin.

KATA PENGANTAR

Assalmu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur peneliti panjatkan kehadirat Allah SWT karena atas limpahan rahmat, hidayah serta inayah-Nya, peneliti masih diberikan kesempatan dan kemudahan untuk menyelesaikan skripsi ini.

Skripsi ini disusun dalam rangka memenuhi salah satu syarat kelulusan perguruan tinggi program studi Strata 1 Informatika di Universitas Amikom Yogyakarta dan meraih gelar Sarjana Komputer (S.Kom). Selain itu skripsi ini juga bertujuan untuk menambah pengetahuan tentang sistem keamanan Port SSH (*Secure Shell*) dengan menggunakan perangkat Mikrotik.

Pembuat skripsi ini tidak lepas dari berbagai pihak yang telah membantu baik dari segi materi dan spiritual. Penulis juga mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas Amikom Yogyakarta.
2. Bapak Sudarmawan S.T, M.T selaku dosen pembimbing yang telah meberikan masukan, saran, bantuan dan bimbingan dalam menyelesaikan naskah skripsi ini.
3. Hanif Al Fatta,S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Ibu Windah Mega Pradnya D,M.Kom selaku ketua Program Studi Informatika Universitas Amikom Yogyakarta.
5. Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu, dan pengalaman, termikasih semua jasa Bapak dan Ibu sekalian.
6. Orang tua yang tidak pernah lelah dalam memberikan dukungan restu dan do'anya.
7. Teman-teman dan sahabat yang telah memberikan semangat, motivasi dan bantuan dalam pengerjaan skripsi ini.

8. Seluruh staff karyawan Universitas Amikom Yogyakarta yang banyak membantu kelancaran segala aktivitas dan administrasi dalam penyusunan skripsi ini.
9. Semua pihak yang telah membantu sampai terselesaikannya penyusunan skripsi ini yang tentunya sangat berharga dan tidak bisa disebutkan satu persatu.

Peneliti menyadari sepenuhnya, bahwa skripsi ini masih jauh dari kesempurnaan, baik dalam hal penyajian skripsi maupun cara penyajian materi. Untuk itu dengan rendah hati peneliti memohon saran dan kritik yang membangun dari pembaca.

Semoga skripsi ini dapat bermanfaat bagi penulis pada khususnya dan bagi pembaca pada umumnya serta dapat digunakan sebagai referensi untuk penelitian yang lain.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Yogyakarta, 5 Januari 2023



Lucky Anton Yudhistira

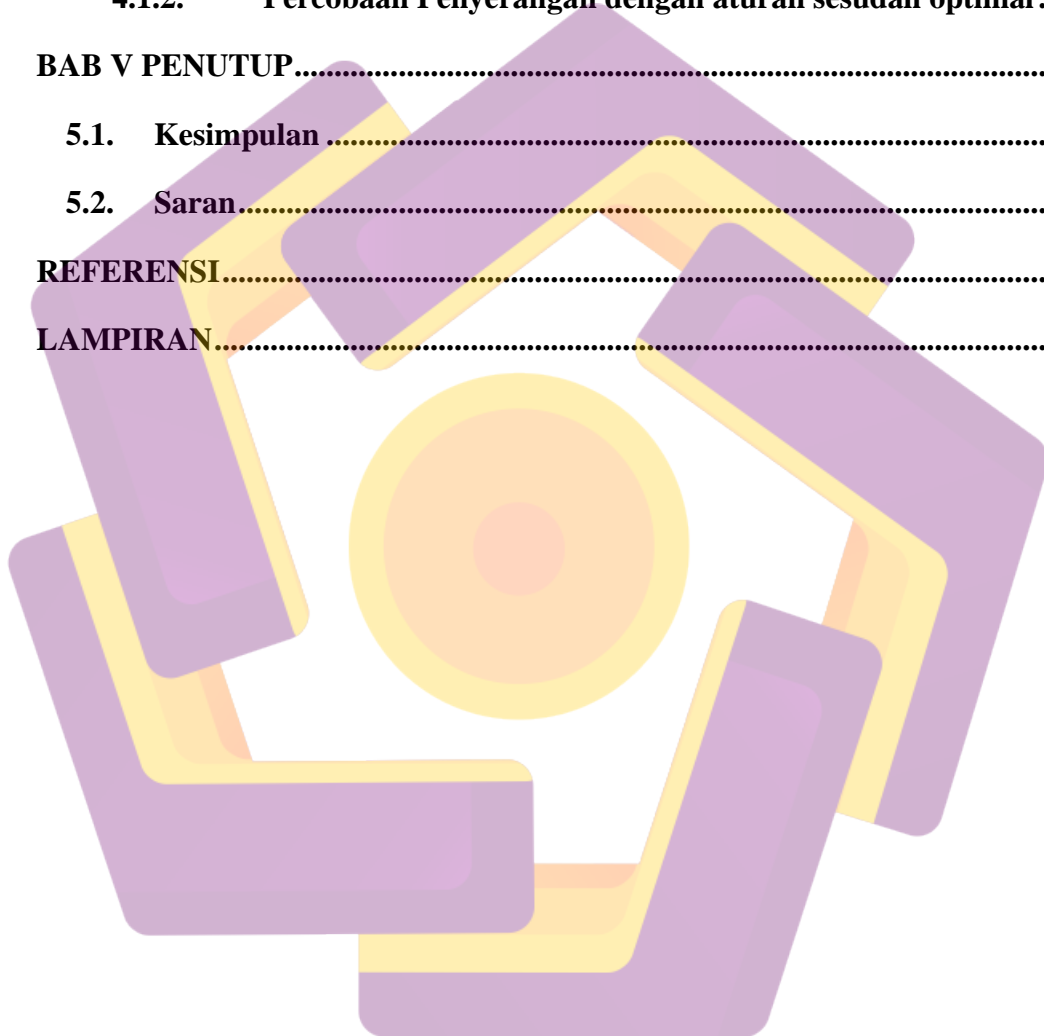
NIM. 19.11.2609

DAFTAR ISI

HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	iv
PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN	xiv
INTISARI	xv
ABSTRACT	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah.....	2
1.4. Tujuan Penelitian	2
1.5. Manfaat Penelitian	3
1.6. Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA.....	5
2.1. Studi Literatur	5
2.2. Dasar Teori	11
2.2.1. Keamanan Jaringan	11
2.2.2. SSH.....	11
2.2.3. Bruteforce	11

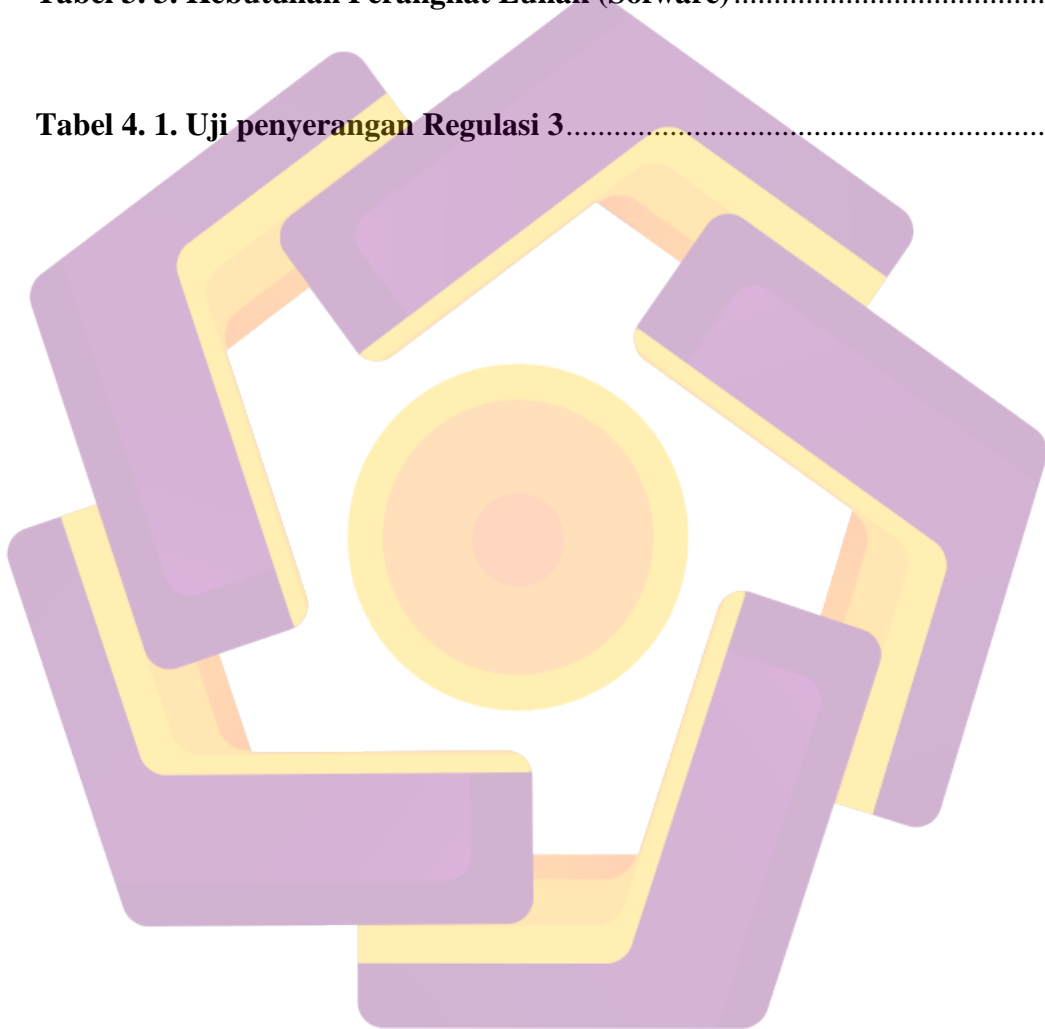
2.2.4.	Port Knocking	12
2.2.5.	Port Blocking.....	12
2.2.6.	Authentication.....	12
2.2.7.	Winbox.....	13
2.2.8.	Firewall	14
2.2.9.	Fitur Firewall Mikrotik.....	14
2.2.10.	Mikrotik.....	15
2.2.11.	Mikrotik Routerboard.....	15
2.2.12.	Kali Linux.....	16
2.2.13.	VMWare Workstation.....	16
2.2.14.	Ncrack	16
2.2.15.	NDLC	17
BAB III METODE PENELITIAN		18
3.1.	Objek Penelitian	18
3.1.1.	Gambaran umum serangan	19
3.1.2.	Gambaran penyerangan dengan Rules sebelum optimal ...	19
3.1.3.	Gambaran penyerangan dengan Rules sebelum optimal ...	20
3.2.	Alat dan Bahan	20
3.2.1.	Alat atau Instrumen	20
3.2.1.1.	Kebutuhan Perangkat Keras (Hardware).....	21
3.2.1.2.	Kebutuhan Perangkat Lunak (Software).....	23
3.3.	Alur Penelitian	24
3.3.1.	Alur Penelitian Skripsi	24
3.3.2.	Alur keamanan Autentikasi SSH	25
3.3.2.1.	Alur Kerja Keamanan SSH Sebelum Optimal	25

3.3.2.2. Alur Kerja Keamanan SSH Sesudah Optimal.....	29
BAB IV HASIL DAN PEMBAHASAN	36
4.1. Hasil Percobaan Penyerangan	36
4.1.1. Percobaan Penyerangan dengan aturan sebelum optimal..	36
4.1.2. Percobaan Penyerangan dengan aturan sesudah optimal ..	39
BAB V PENUTUP.....	41
5.1. Kesimpulan	41
5.2. Saran.....	41
REFERENSI.....	42
LAMPIRAN.....	46



DAFTAR TABEL

Tabel 2. 1. Keaslian Penelitian	7
Tabel 3. 1. Router Mikrotik RB951UI-2HND	21
Tabel 3. 2. Laptop Asus VivoBook A442U.....	22
Tabel 3. 3. Kebutuhan Perangkat Lunak (Software).....	23
Tabel 4. 1. Uji penyerangan Regulasi 3.....	37



DAFTAR GAMBAR

Gambar 2. 1. Winbox.....	13
Gambar 2. 2. Firewall	14
Gambar 2. 3. Logo Mikrotik	15
Gambar 2. 4. Mikrotik Routerboard	16
Gambar 3. 1. Gambaran Umum Serangan.....	19
Gambar 3. 2. skenario penyeerangan sebelum optimal	19
Gambar 3. 3 Skenario penyerangan sesudah optimal	20
Gambar 3. 4. RB951UI-2HND	21
Gambar 3. 5. Laptop Asus A442U	22
Gambar 3. 6. Alur kerja Penelitian	25
Gambar 3. 7. Alur Kerja Keamanan Login SSH ke-1	25
Gambar 3. 8. Aturan Sebelum Optimal Filter Rules Full Layar	27
Gambar 3. 9. Aturan Sebelum Optimal Filter Rules Fokus Aturan	27
Gambar 3. 10. Tampilan konfigurasi PuTTY sebelum optimal	28
Gambar 3. 11. Alur Kerja Keamanan Login SSH ke-2	29
Gambar 3. 12. Aturan Sesudah Optimal Filter Rules Full Layar	30
Gambar 3. 13. Aturan Sesudah Optimal Filter Rules Fokus Aturan	31
Gambar 3. 14. Tampilan konfigurasi PuTTY sesudah optimal	31
Gambar 3. 15. Service Router setelah di optimalkan	32
Gambar 3. 16. Rules Port Knocking	32
Gambar 3. 17. IP	33
Gambar 3. 18. Username dan password autentikasi mikrotik	33
Gambar 3. 19. Username untuk penelitian	34
Gambar 3. 20. Password untuk penelitian	34
Gambar 4. 1 Hasil Regulasi 1 login 1x	36
Gambar 4. 2 Hasil Regulasi 2 Login 2x.....	37
Gambar 4. 3. Grafik keberhasilan penyerangan dengan Regulasi 3	38

Gambar Lampiran. 1. General firewall before optimal	46
Gambar Lampiran. 2. Action percobaan 3x before optimal	47
Gambar Lampiran. 3. Advance firewall before optimal	48
Gambar Lampiran. 4. Rules pemblokiran firewall before optimal	49
Gambar Lampiran. 5. Action drop before optimal	50
Gambar Lampiran. 6. General firewall after optimal	51
Gambar Lampiran. 7. Action firewall percobaan 3x after optimal	52
Gambar Lampiran. 8. Advance firewall after optimal	53
Gambar Lampiran. 9. Action blocking firewall after optimal	54
Gambar Lampiran. 10. Action drop after optimal	54
Gambar Lampiran. 11. Tab general Port knocking aturan 1	55
Gambar Lampiran. 12. Tab action di aturan 1 Port knocking	55
Gambar Lampiran. 13. Tab general di aturan ke 2 Port Knocing	56
Gambar Lampiran. 14. Tab advance di aturan ke 1 Port Knocking	57
Gambar Lampiran. 15. Tab general di aturan drop Port Knocking	57
Gambar Lampiran. 16. Tab advance di aturan drop Port Knocking	58
Gambar Lampiran. 17. Action Drop di Port Knocking	58
Gambar Lampiran. 18. Hasil penyerangan sebelum optimal (Ncrack)	59
Gambar Lampiran. 19. Hasil Pemblokiran Ncrack	60

DAFTAR LAMPIRAN

Lampiran. 1. Detail Konfigurasi Pada Firewall.....	46
Lampiran. 2 Konfigurasi Port knocking.....	54
Lampiran. 3 Hasil uji coba penyerangan Ncrack	59



INTISARI

Keamanan jaringan menjadi salah satu hal terpenting dalam sebuah jaringan perusahaan ataupun instansi karena untuk melindungi data atau informasi dari serangan luar yang banyak mengancam jaringan perusahaan atau instansi. Jaringan internet juga digunakan dalam melakukan hal yang melanggar aturan, serta berbuat hal yang negatif seperti pengambilan data autentikasi perangkat jaringan dengan menggunakan serangan *brute force*, maka diperlukan keamanan yang cukup kuat untuk mengatasi serangan tersebut, seperti penggunaan *Port Knocking* dan *Port Blocking*.

Port Knocking dan *Port Blocking* sering digunakan untuk mengamankan perangkat router mikrotik pada port-port mikrotik seperti SSH, FTP *Port Knocking* digunakan untuk membuat kunci secara berurutan dan banyak kunci untuk membuka akses ke port mikrotik. Sedangkan *Port Blocking* digunakan untuk memblokir ip yang digunakan untuk mengakses jaringan router dengan menggunakan sistem login berulang, ketika *Port Knocking* berhasil di akses maka penyerang tidak akan bisa masuk untuk mengakses router tujuan penyerangan.

Tujuan dari penelitian ini adalah untuk membuat keamanan Autentikasi pada jaringan Port SSH (*Scure Shell*), dengan menerapkan metode *Port Knocking* dan login berulang agar membatasi yang mengakses router bukan dari pihak luar. Dan juga menerapkan *Port Blocking* dalam percobaan gagal beberapa kali. Sehingga router yang diserang menggunakan *brute force* tidak mengalami gangguan seperti perangkat kurang mengalami penurunan kinerja pada jaringan, dan setelah di optimalkan maka tingkat pencurian data 0 dari yang aturan sebelumnya belum di optimalkan di regulasi ke-3 dapat mencuri password dengan rata-rata waktu 27-48 detik dengan banyak password yang digunakan 30.

Kata Kunci : Mikrotik, SSH, Autentikasi, Port Knocking, Port Blocking, Ncrack, Kali Linux.

ABSTRACT

Network security is one of the most important things in a corporate or agency network because it protects data or information from outside attacks that threaten corporate or agency networks. The internet network is also used to do things that violate the rules, as well as to do negative things, such as retrieving network device authentication data using brute force attacks, so strong enough security is needed to overcome these attacks, such as the use of Port Knocking and Port Blocking.

Port Knocking and Port Blocking are often used to secure Mikrotik router devices on Mikrotik ports such as SSH, FTP Port Knocking is used to create keys sequentially and multiple keys to open access to Mikrotik ports. Meanwhile, Port Blocking is used to block IPs that are used to access the router network by using a repeated login system, when Port Knocking is successfully accessed, the attacker will not be able to enter the router to access the target of the attack.

The purpose of this research is to make Authentication security on SSH (Secure Shell) Port networks, by implementing the Port Knocking method and repeated logins so as to limit those who access the router not from outsiders. And also implement Port Blocking in failed attempts several times. So that routers that are attacked using brute force do not experience interference such as devices experiencing less performance on the network, and after being optimized, the data theft rate is 0 from the previous rules that have not been optimized in the 3rd regulation can steal passwords with an average time of 27- 48 seconds with multiple passwords used 30.

Keywords : Mikrotik, SSH, Authentication, Port Knocking, Port Blocking, Ncrack, Kali Linux.