

SKRIPSI

**ANALISIS PENGGUNAAN *PORT KNOCKING* PADA
KEAMANAN JARINGAN MIKROTIK**

***ANALYSIS OF UTILIZATION OF PORT KNOCKING IN
MIKROTIK NETWORK SECURITY***



Disusun oleh:

WIEDYASTOMO TAUFIQ

19101027

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

**ANALISIS PENGGUNAAN *PORT KNOCKING* PADA
KEAMANAN JARINGAN MIKROTIK**

***ANALYSIS OF UTILIZATION OF PORT KNOCKING IN
MIKROTIK NETWORK SECURITY***

**Skripsi ini digunakan sebagai salah satu syarat untuk
memperoleh Gelar Sarjana Teknik (S.T.)
di Institut Teknologi Telkom Purwokerto
2023**

Disusun oleh:

WIEDYASTOMO TAUFIQ

19101027

DOSEN PEMBIMBING

Eka Wahyudi, S.T., M.Eng.

Eko Fajar Cahyadi, S.T., M.T., Ph.D.

**PROGRAM STUDI S1 TEKNIK TELEKOMUNIKASI
FAKULTAS TEKNIK TELEKOMUNIKASI DAN ELEKTRO
INSTITUT TEKNOLOGI TELKOM PURWOKERTO**

2023

HALAMAN PENGESAHAN
ANALISIS PENGGUNAAN *PORT KNOCKING* PADA
KEAMANAN JARINGAN MIKROTIK

ANALYSIS OF UTILIZATION OF PORT KNOCKING IN
MIKROTIK NETWORK SECURITY

Disusun oleh

WIEDYASTOMO TAUFIQ

19101027

Telah dipertanggungjawabkan di hadapan Tim Penguji pada tanggal 7 Agustus
2023

Susunan Tim Penguji

Pembimbing Utama : Eka Wahyudi, S.T., M.Eng.

NIDN. 0617117601

Pembimbing Pendamping : Eko Fajar Cahyadi, S.T., M.T., Ph.D.

NIDN. 0616098703

Penguji 1 : Jafaruddin Gusti Amri Ginting, S.T., M.T.

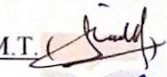
NIDN. 0620108901

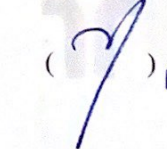
Penguji 2 : Fauza Khair, S.T., M.Eng.

NIDN. 0622039001

 21/8

 18/8/23

 18/08/23

 18/08/23

Mengetahui,

Ketua Program Studi S1 Teknik Telekomunikasi
Institut Teknologi Telkom Purwokerto


Prasetyo Yulianto, S.T., M.T.

NIDN. 0620079201

HALAMAN PERNYATAAN ORISINALITAS

Dengan ini saya, **WIEDYASTOMO TAUFIQ**, menyatakan bahwa skripsi dengan judul “**ANALISIS PENGGUNAAN *PORT KNOCKING* PADA KEAMANAN JARINGAN MIKROTIK**” adalah benar-benar karya saya sendiri. Saya tidak melakukan penjiplakan kecuali melalui pengutipan sesuai dengan etika keilmuan yang berlaku. Saya bersedia menanggung risiko ataupun sanksi yang dijatuhkan kepada saya apabila ditemukan pelanggaran terhadap etika keilmuan dalam skripsi saya ini.

Purwokerto, 3 Agustus 2023

Yang menyatakan,



(Wiedyastomo Taufiq)

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan kasih dan sayang-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “**Analisis Penggunaan *Port Knocking* pada Keamanan Jaringan Mikrotik**”.

Maksud dari penyusunan skripsi ini adalah untuk memenuhi salah satu syarat dalam menempuh ujian sarjana Teknik Telekomunikasi pada Fakultas Teknik Telekomunikasi dan Elektro Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, banyak pihak yang sangat membantu penulis dalam berbagai hal. Oleh karena itu, penulis sampaikan rasa terima kasih yang sedalam-dalamnya kepada:

1. Kedua orang tua yang selalu mendoakan serta mendukung saya untuk menyelesaikan skripsi ini.
2. Ibu Tenia Wahyuningrum, S.Kom., M.T., selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Ibu Dr. Anggun Fitriani Isnawati, M.Eng., selaku Dekan Fakultas Teknik Telekomunikasi dan Elektro.
4. Bapak Prasetyo Yuliantoro, S.T., M.T., selaku Ketua Program Studi S1 Teknik Telekomunikasi
5. Bapak Eka Wahyudi, S.T., M.Eng., selaku Dosen Pembimbing I
6. Bapak Eko Fajar Cahyadi, S.T., M.T., Ph.D., selaku Dosen Pembimbing II
7. Semua pihak yang tidak dapat disebutkan satu persatu.

Akhir kata penulis ucapkan terima kasih, dan diharapkan agar laporan yang disusun oleh penulis dapat berguna dan bermanfaat serta mampu memperluas serta menambah pengetahuan bagi semua pihak.

Purwokerto, 3 Agustus 2023

(Wiedyastomo Taufiq)

ABSTRAK

Seiring dengan perkembangan teknologi, sistem keamanan jaringan juga harus selalu ditingkatkan, banyaknya serangan dari pihak tak bertanggung jawab yang dapat dengan mudah mengakses dan mengendalikan *port-port* yang belum diamankan. Maka untuk mengatasi serangan tersebut, digunakanlah metode *port knocking*. Metode *port knocking* akan membuka dan menutup akses *block* ke *port* tertentu dengan memasukan *rule* yang sudah dibuat pada fitur *firewall*. Parameter uji pada penelitian ini akan diterapkan pada *service port* 8291, 80 dan 23, dan dalam menganalisis hasil tersebut menggunakan parameter QoS pada saat kondisi normal, *port knocking off* dan *port knocking on*. Nilai *throughput* terbesar pada saat kondisi normal didapatkan nilai 2647 Kbps, untuk kondisi *port knocking off* nilai *throughput* terbesar nilai 1189 Kbps, dan untuk kondisi *port knocking on* nilai *throughput* terbesar didapatkan nilai 2043 Kbps. Untuk pengujian nilai *packet loss* didapatkan nilai sebesar 0% pada kondisi normal sementara pada kondisi *port knocking (off)* mempunyai nilai *packet loss* sebesar 0,3 %, dan untuk kondisi *port knocking on* diperoleh hasil *packet loss* 0,1%. Hasil pengukuran *delay* diketahui bahwa nilai *delay* pada kondisi normal terkecil didapatkan nilai 1,043 ms, untuk kondisi *port knocking off* pengukuran *delay* terkecil sebesar 5,023 ms dan kondisi *port knocking on* pengukuran *delay* terkecil sebesar 3,974 ms. Hasil pengukuran *jitter* diketahui bahwa nilai *jitter* pada kondisi normal terkecil didapatkan nilai 1,04 ms, untuk kondisi *port knocking off* pengukuran *jitter* terkecil sebesar 5,02 ms dan kondisi *port knocking on* pengukuran *jitter* terkecil sebesar 3,97 ms. Dari hasil pengujian *port knocking* didapatkan bahwa *user* tidak dapat mengakses *port* 8291, 80, dan 23 jika sudah terpasang *port knocking*, *user* harus membuka kunci terlebih dahulu jika ingin mengakses *port* tersebut. Kunci tersebut hanya dapat terbuka jika *user* melakukan *knock 5555*. Dan dari pengujian *port scanning*, didapatkan bahwa *service port* yang telah terpasang *port knocking* sudah dalam keadaan tertutup. Dan hasil QoS dengan metode *port knocking* bisa dikategorikan efisien, karena bisa memberikan gambaran dalam upaya perbaikan dan mengatasi *traffic* yang terjadi disebabkan oleh *attacker*.

Kata Kunci: Keamanan Jaringan, *Port Knocking*, *Port Scanning*

ABSTRACT

Along with technological developments, network security systems must also always be improved, there are many attacks from irresponsible parties who can easily access and control unsecured ports. So to overcome this attack, the port knocking method is used. The port knocking method will open and close block access to certain ports by entering the rules that have been made in the firewall feature. The test parameters in this study will be applied to service ports 8291, 80 and 23, and in analyzing these results using QoS parameters during normal conditions, port knocking off and port knocking on. The highest throughput value during normal conditions is 2647 Kbps, for port knocking off conditions the highest throughput value is 1189 Kbps, and for port knocking on conditions the highest throughput value is 2043 Kbps. To test the packet loss value, a value of 0% is obtained in normal conditions while in port knocking (off) conditions it has a packet loss value of 0.3%, and for port knocking on conditions, a packet loss result of 0.1% is obtained. The results of the delay measurement show that the delay value in the smallest normal condition is 1,043 ms, for the port knocking off condition the smallest delay measurement is 5,023 ms and the port knocking on condition the smallest delay measurement is 3,974 ms. From the results of jitter measurements, it is known that the jitter value in the smallest normal condition is 1,04 ms, for the port knocking off condition the smallest jitter measurement is 5,02 ms and the port knocking on condition the smallest jitter measurement is 3,97 ms. From the results of the port knocking test, it was found that the user cannot access ports 8291, 80, and 23 if port knocking has been installed, the user must unlock it first if he wants to access the port. The lock can only be opened if the user knocks 5555. And from the port scanning test, it is found that the service port that has port knocking installed is already closed. And the results of QoS with the port knocking method can be categorized as efficient, because it can provide an overview of efforts to repair and overcome traffic caused by attackers.

Keyword: Network Security, Port Knocking, Port Scanning

DAFTAR ISI

| | |
|---|------|
| HALAMAN PENGESAHAN | iii |
| HALAMAN PERNYATAAN ORISINALITAS | iv |
| PRAKATA..... | v |
| ABSTRAK..... | vi |
| <i>ABSTRACT</i> | vi |
| DAFTAR ISI..... | viii |
| DAFTAR TABEL..... | x |
| DAFTAR GAMBAR..... | xi |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Tujuan | 2 |
| 1.5 Manfaat | 3 |
| 1.6 Sistematika Penulisan | 3 |
| BAB II DASAR TEORI | 4 |
| 2.1 KAJIAN PUSTAKA..... | 4 |
| 2.2 DASAR TEORI | 5 |
| 2.2.1 Jaringan Komputer..... | 5 |
| 2.2.2 <i>IP Address</i> | 16 |
| 2.2.3 Sistem Keamanan Jaringan..... | 17 |
| 2.2.4 <i>Port Knocking</i> | 22 |
| 2.2.5 <i>Firewall</i> | 25 |
| 2.2.6 <i>Port Scanning</i> | 25 |
| 2.2.7 Mikrotik RouterOS | 25 |
| 2.2.8 <i>Quality of Service (QoS)</i> | 27 |
| BAB III METODOLOGI PENELITIAN | 30 |
| 3.1 PERANGKAT YANG DIGUNAKAN | 30 |
| 3.1.1 Perangkat Keras (<i>Hardware</i>) | 30 |
| 3.1.2 Perangkat Lunak (<i>Software</i>) | 31 |
| 3.2 ALUR PENGUJIAN..... | 32 |

| | | |
|-----------------------------------|---|----|
| 3.3 | TOPOLOGI JARINGAN..... | 34 |
| 3.4 | PENERAPAN <i>PORT KNOCKING</i> | 39 |
| BAB IV HASIL DAN PEMBAHASAN | | 44 |
| 4.1 | Pengujian <i>Quality of Service (QoS)</i> | 44 |
| 4.2 | Pengujian <i>Port Knocking</i> | 52 |
| 4.3 | Pengujian <i>Port Scanning</i> | 53 |
| BAB V PENUTUP | | 54 |
| 5.1 | KESIMPULAN..... | 54 |
| 5.2 | SARAN | 55 |
| DAFTAR PUSTAKA | | 56 |
| LAMPIRAN..... | | 59 |

DAFTAR TABEL

| | | |
|-----------|---|----|
| Tabel 2.1 | Perbedaan IPv4 dengan IPv6..... | 17 |
| Tabel 2.2 | Performasi Jaringan Berdasarkan <i>Throughput</i> | 27 |
| Tabel 2.3 | Performasi Jaringan Berdasarkan <i>Delay</i> | 28 |
| Tabel 2.4 | Performasi Jaringan Berdasarkan <i>Packet Loss</i> | 28 |
| Tabel 2.5 | Performasi Jaringan Berdasarkan <i>Jitter</i> | 29 |
| Tabel 3.1 | Spesifikasi Perangkat Keras Laptop..... | 30 |
| Tabel 3.2 | Spesifikasi Perangkat Keras Laptop untuk serangan DoS | 30 |
| Tabel 3.3 | Spesifikasi Perangkat Keras Mikrotik <i>Router Board RB941-2nD (hAP-Lite)</i> | 31 |
| Tabel 4.1 | Hasil Pengukuran <i>Throughput</i> | 44 |
| Tabel 4.2 | Hasil Pengukuran <i>Packet Loss</i> | 46 |
| Tabel 4.3 | Hasil Pengukuran <i>Delay</i> | 48 |
| Tabel 4.4 | Hasil Pengukuran <i>Jitter</i> | 50 |
| Tabel 4.5 | Hasil Data <i>Port Knocking</i> Pertama | 52 |
| Tabel 4.6 | Hasil Data <i>Port Knocking</i> Kedua | 52 |
| Tabel 4.7 | Pengujian <i>Port Scanning</i> Sebelum Instalasi <i>Port Knocking</i> | 53 |
| Tabel 4.8 | Pengujian <i>Port Scanning</i> Setelah Instalasi <i>Port Knocking</i> | 53 |

DAFTAR GAMBAR

| | | |
|-------------|---|----|
| Gambar 2.1 | <i>Personal Area Network (PAN)</i> | 7 |
| Gambar 2.2 | <i>Local Area Network (LAN)</i> | 7 |
| Gambar 2.3 | <i>Metropolitan Area Network (MAN)</i> | 8 |
| Gambar 2.4 | <i>Wide Area Network (WAN)</i> | 9 |
| Gambar 2.5 | <i>Client-Server</i> | 10 |
| Gambar 2.6 | <i>Peer-to-Peer</i> | 11 |
| Gambar 2.7 | Topologi <i>Bus</i> | 12 |
| Gambar 2.8 | Topologi <i>Star</i> | 13 |
| Gambar 2.9 | Topologi <i>Ring</i> | 14 |
| Gambar 2.10 | Topologi <i>Mesh</i> | 15 |
| Gambar 2.11 | Topologi <i>Tree</i> | 16 |
| Gambar 2.12 | Inisial <i>Request</i> | 23 |
| Gambar 2.13 | <i>Server</i> mengirimkan urutan <i>port</i> | 24 |
| Gambar 2.14 | <i>Client</i> melakukan komunikasi terhadap urutan <i>port</i> yang ditentukan | 24 |
| Gambar 2.15 | <i>Client</i> terautentikasi dan dapat mengakses layanan <i>server</i> | 24 |
| Gambar 2.16 | Router OS Mikrotik..... | 27 |
| Gambar 3.1 | <i>Flowchart</i> Pengujian | 33 |
| Gambar 3.2 | Topologi Jaringan..... | 34 |
| Gambar 3.3 | Mengaktifkan <i>Wireless</i> | 35 |
| Gambar 3.4 | <i>Security Profile</i> | 35 |
| Gambar 3.6 | Konfigurasi <i>Wireless</i> | 36 |
| Gambar 3.7 | <i>Scan WiFi</i> | 36 |
| Gambar 3.8 | Konfigurasi IP – DHCP <i>Client</i> (1) | 37 |
| Gambar 3.9 | Konfigurasi IP – DHCP <i>Client</i> (2) | 38 |
| Gambar 3.10 | Konfigurasi IP – DHCP <i>Client</i> (3) | 38 |
| Gambar 3.11 | <i>Test PING</i> | 38 |
| Gambar 3.12 | <i>Rules</i> Penelitian | 39 |
| Gambar 3.13 | <i>Rules</i> Identifikasi Alamat IP (1)..... | 39 |
| Gambar 3.14 | <i>Rules</i> Identifikasi Alamat IP (2)..... | 40 |
| Gambar 3.15 | <i>Rules Port Knocking 5555</i> (1)..... | 40 |

| | | |
|-------------|---|----|
| Gambar 3.16 | <i>Rules Port Knocking 5555 (2)</i> | 41 |
| Gambar 3.17 | <i>Rules Port Knocking 5555 (3)</i> | 41 |
| Gambar 3.18 | <i>Rules Drop (1)</i> | 42 |
| Gambar 3.19 | <i>Rules Drop (2)</i> | 42 |
| Gambar 3.20 | <i>Rules Drop (3)</i> | 42 |
| Gambar 4.1 | Grafik Pengujian <i>Throughput</i> | 44 |
| Gambar 4.2 | Grafik Pengujian <i>Packet Loss</i> | 46 |
| Gambar 4.3 | Grafik Pengujian <i>Delay</i> | 48 |
| Gambar 4.4 | Grafik Pengujian <i>Jitter</i> | 50 |