

**IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN *PORT KNOCKING***

SKRIPSI



**Oleh:
Yuniaman Mendrofa
190210054**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023**

**IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN *PORT KNOCKING***

SKRIPSI

**Untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana**



**Oleh:
Yuniaman Mendrofa
190210054**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023**

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Yuniaman Mendrofa

Npm : 190210054

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan Bahwa “Skripsi” yang saya buat dengan judul:

IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING*

Adalah hasil karya sendiri dan bukan “duplikasi” dari karya orang lain. Sepengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau di terbitkan oleh orang lain, kecuali yang secara tertulis dikutip di dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah skripsi ini digugurkan dan gelar yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 2 Agustus 2023

Materai 10000



Yuniaman Mendrofa
190210054

**IMPLEMENTASI KEAMANAN JARINGAN
MENGUNAKAN *PORT KNOCKING***

SKRIPSI

**Untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana**

**Oleh:
Yuniaman Mendrofa
190210054**

**Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini**

Batam, 3 Agustus 2023


**Rahmat Fauzi, S.Kom., M.Kom
Pembimbing**

ABSTRAK

Perkembangan teknologi dari hari kehari semakin meningkat, dimana para ahli mengembangkan ilmu pengetahuannya baik dalam bidang industri, kesehatan, keamanan jaringan dan lainnya. PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto merupakan perusahaan air dibatam yang menjaga keamanan pengolahan air minum. Namun pada sistem yang digunakan oeh perusahaan masih terdapat Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadap keamanan data, selain itu dalam suatu sistem jaringan komputer terdapat bentuk ancaman baik dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya, Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus*, dan pemindaian *port. Port Knocking* memang merupakan salah satu metode keamanan yang digunakan untuk mengamankan akses ke port-port tertentu di sebuah perangkat jaringan, seperti server. Prinsip utama dari port knocking adalah bahwa akses ke port yang dibatasi hanya akan dibuka jika ada rangkaian permintaan koneksi yang tepat dari sumber yang sah. Selain Port Knocking, ada banyak metode keamanan lainnya yang dapat digunakan untuk melindungi jaringan, seperti penggunaan VPN, firewall yang dikonfigurasi dengan baik, dan manajemen hak akses yang ketat. Penting untuk mempertimbangkan kebutuhan keamanan dan fleksibilitas yang tepat untuk lingkungan jaringan tertentu saat memilih dan mengimplementasikan metode keamanan yang sesuai.

Kata kunci: Jaringan; Keamanan; *Port Knocking*

ABSTRACT

Technological developments are increasing day by day, where experts develop their knowledge both in the fields of industry, health, network security and others. PT Air Batam Hulu is a company whose address is Building A-WTP Moya Muka Kuning Jl. Letjend Supranto, which is a water company in Batam that maintains the security of drinking water management. However, in the system used by the company there are still parties who are not authorized to hack so that it is vulnerable to infiltration of data security, besides that in a computer network system there are forms of threats both physically and logically such as Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Cracker and others. One of the intrusions that are currently successfully hacked and are often carried out are UML sites, Malware, Trojans, Viruses, and port scanning. Port Knocking is a security system that aims to open or close block access to certain ports using a firewall on network devices by sending certain packets or connections. Connections in the form of TCP, UDP, and ICMP protocols. So to enter and use access to certain ports that have been restricted, the user must first tap by entering the rule which must be done first. Rules which are only known by the network provider (network administrator). A system must have a balance between security and flexibility. One way to achieve such a system is by using firewall access. By using a firewall, we can indirectly define trustworthy and untrusted users by using the IP device as a filter criterion.

Keywords: Network; Security; Port Knocking

KATA PENGANTAR

Atas berkat dan rahmat Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terimakasih kepada:

1. Ibu DR.Nur Elfi Husda,S.Kom.,M.Si Selaku Rektor Universitas Putera Batam;
 2. Bapak Welly Sugiyanto,S.T.,M.M Selaku Dekan Fakultas Teknik dan Komputer;
 3. Bapa Andi Maslan,S.T.,M.Si Selaku Ketua Program Studi Teknik Informatika;
 4. Bapak Sunarsan Sitohang, S.Kom., M.Kom Selaku Pembimbing Akademik pada Program Studi Teknik Informatika Universitas Putera Batam;
 5. Bapak Rahmat Fauzi, S.Kom., M.Kom Selaku Pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam;
 6. Dosen dan Staff Universitas Putera Batam;
 7. Selaku Kedua orang tua penulis yang selalu mendoakan dan memberikan dukungan sehingga skripsi ini dapat terselesaikan;
 8. Keluarga penulis yang selalu memberikan dukungan dan motivasi kepada penulis;
 9. Teman-teman seperjuangan yang bersedia membagi ilmu dan sharing pendapat;
 10. Semua pihak yang telah bersedia meluangkan waktu, tenaga dan pikiran dalam memberikan data dan informasi selama penulis membuat skripsi ini yang tidak dapat disebutkan satu persatu.
- Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan berkatNya, Amin.

Batam, 3 Agustus 2023



Yuniaman Mendrofa

DAFTAR ISI

Halaman

| | |
|---|-------------|
| HALAMAN SAMPUL | i |
| HALAMAN JUDUL | ii |
| SURAT PERNYATAAN ORISINALITAS | iii |
| ABSTRAK | v |
| ABSTRACT | vi |
| KATA PENGANTAR | vii |
| DAFTAR ISI | viii |
| DAFTAR GAMBAR | x |
| DAFTAR TABEL | xii |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Identifikasi Masalah..... | 4 |
| 1.3 Batasan Masalah..... | 4 |
| 1.4 Rumusan Masalah..... | 5 |
| 1.5 Tujuan Penelitian..... | 5 |
| 1.6 Manfaat Penelitian..... | 5 |
| 1.6.1 Manfaat Teoritis..... | 5 |
| 1.6.2 Manfaat Praktis..... | 6 |
| BAB II TINJAUAN PUSTAKA | |
| 2.1 Teori Dasar..... | 7 |
| 2.1.1 Pengertian Jaringan Komputer..... | 7 |
| 2.1.2 Standart Jaringan Komputer..... | 7 |
| 2.1.3 Jaringan Berdasarkan Area..... | 10 |
| 2.1.4 Perangkat Jaringan..... | 13 |
| 2.2 Teori Khusus..... | 14 |
| 2.2.1 Manfaat Jaringan Komputer..... | 14 |
| 2.2.2 Keamanan Jaringan..... | 15 |
| 2.2.3 <i>Firewall</i> | 16 |
| 2.2.4 Mikrotik..... | 17 |
| 2.2.5 <i>VirtualBox</i> | 19 |
| 2.2.6 <i>Port Knocking</i> | 20 |
| 2.3 Metode Network Development Life cycle (NDLC)..... | 21 |
| 2.4 <i>Tools/Software</i> Pendukung..... | 22 |
| 2.4 Penelitian Terdahulu..... | 25 |
| 2.5 Kerangka Pemikiran..... | 27 |
| BAB III METODE PENELITIAN | |
| 3.1 Desain Penelitian..... | 28 |
| 3.2 Metode Pengumpulan Data..... | 29 |
| 3.3 Tahap Analisis..... | 30 |
| 3.4 Lokasi dan Jadwal Penelitian..... | 32 |

| | |
|---|----|
| 3.4.1 Lokasi Penelitian..... | 33 |
| 3.4.2 Jadwal Penelitian..... | 33 |
| BAB IV HASIL DAN PEMBAHASAN | |
| 4.1 Hasil Penelitian..... | 35 |
| 4.1.1 <i>Implementasi Virtual box</i> | 35 |
| 4.1.2 <i>Simulasi dan prototype</i> | 40 |
| 4.1.2 <i>Setting firewall</i> | 42 |
| BAB V KESIMPULAN DAN SARAN | |
| 5.1 Kesimpulan | 46 |
| 5.2 Saran | 46 |
| DAFTAR PUSTAKA | |
| LAMPIRAN | |
| 1. Pendukung Penelitian | |
| 2. Daftar Riwayat Hidup | |
| 3. Surat Keterangan Penelitian | |
| 4. Turnitin Jurnal | |
| 5. Turnitin Skripsi | |

DAFTAR GAMBAR

Halaman

| | |
|--|----|
| Gambar 2. 1 Internet Engineering Task Force | 8 |
| Gambar 2. 2 International Telecommunications Union | 8 |
| Gambar 2. 3 Internasional Standards Organizations | 8 |
| Gambar 2. 4 American National Standart Insitute | 9 |
| Gambar 2. 5 Institute of Electrical and Electronics Engeeners | 9 |
| Gambar 2. 6 Electronic Industries Association | 10 |
| Gambar 2. 7 Federal Communications Commision | 10 |
| Gambar 2. 8 Personal Area Network..... | 11 |
| Gambar 2. 9 Local Area Network | 11 |
| Gambar 2. 10 Metropolitan Area Network..... | 12 |
| Gambar 2. 11 Wide Area Network..... | 12 |
| Gambar 2. 12 Firewall | 17 |
| Gambar 2. 13 Mikrotik | 17 |
| Gambar 2. 14 Virtual Box | 20 |
| Gambar 2. 15 Port Knocking..... | 21 |
| Gambar 2. 16 Leptop | 22 |
| Gambar 2. 17 Kabel UTP | 23 |
| Gambar 2. 18 Rj45..... | 23 |
| Gambar 2. 19 Switch | 24 |
| Gambar 2. 20 Modem..... | 24 |
| Gambar 2. 21 Winbox | 25 |
| Gambar 2. 22 Kerangka Pemikiran | 27 |
| Gambar 3. 1 Desain Penelittian | 28 |
| Gambar 3. 2 Desain | 31 |
| Gambar 3. 3 Desain jaringan | 31 |
| Gambar 3. 4 Desain jaringan | 32 |
| Gambar 3. 5 Lokasi Penelitian | 33 |
| Gambar 4. 1 Instal OS..... | 36 |
| Gambar 4. 2 Hasil instal OS | 36 |
| Gambar 4. 3 Jumlah memory | 37 |
| Gambar 4. 4 Pada finish | 37 |
| Gambar 4. 5 Setting Microtik..... | 38 |
| Gambar 4. 6 Setting reboot..... | 38 |
| Gambar 4. 7 Tutup OS..... | 39 |
| Gambar 4. 8 Tampilan OS..... | 39 |
| Gambar 4. 9 Open winbox..... | 40 |
| Gambar 4. 10 Pilih..... | 40 |
| Gambar 4. 11 Konfigurasi..... | 41 |
| Gambar 4. 12 Setting IP adress | 41 |
| Gambar 4. 14 setting firewall | 42 |
| Gambar 4. 15 setting firewall | 42 |

| | |
|--|----|
| Gambar 4. 16 setting firewall | 43 |
| Gambar 4. 17 setting firewall | 43 |
| Gambar 4. 18 setting firewall | 44 |
| Gambar 4. 19 setting firewall | 44 |
| Gambar 4. 20 setting firewall | 45 |
| Gambar 4. 21 setting firewall | 45 |

DAFTAR TABEL

| | |
|--|---------|
| | Halaman |
| Tabel 3. 1 Jadwal Penelitian..... | 33 |