# PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN RANDOM PORT KNOCKING BERBASIS RASPBERRY PI YANG DIKIRM MELEWATI TELEGRAM

**Iga Revva Princiss Jeinever[1)],Abdul Rasyid[2)],Nugroho Suharto[3)]**
[1,2,3)] Program Studi Jaringan Telekomunikasi Digital, Teknik Elektro, Politeknik Negeri Malang
Email: igarevva@gmail.com

**Abstrak**

Intergritas keamanan sistem komputer atau jaringan dewasa isi sangatlah penting untuk ditingkatkan. Jaringan computer pada dasarnya tidak aman untuk diakses secara bebas celah-celah keamanan yang terdapat pada jaringan dapat dilihat oleh orang yang tidak bertanggung jawab dengan berbagai teknik. Membuka port untuk akses memiliki resiko yang tinggi untuk kemungkinan diserang oleh attacker.

Berhubungan dengan hal itu, *administrator* jaringan dituntut bekerja lebih untuk dapat mengamankan jaringan komputer yang dikelolanya. Salah satu bentuk keamanan jaringan yang sering digunakan oleh seorang administrator jaringan dalam pengelolaan *server* yaitu melalui *remote login* seperti port pada telnet,SSH dll. *Port* yang selalu terbuka merupakan suatu celah keamanan jaringan yang dapat digunakan oleh orang yang tidak bertanggung jawab untuk masuk kedalam *server*.

Berfokus pada permasalahan tersebut, pada penelitian ini, *Random PortKnocking* merupakan cara yang tepat dan dapat dipakai untuk meningkatkankeamanan jaringan. Dengan *Random Port Knocking* maka *port* akandibuka sesuai dengan kebutuhan , juga port akan secara otomatis berganti ketika gagal melakukan login lebih dari tiga kali dan otomatis IP akan diblok serta akses tidak akan berlanjut sehingga serangan pada jaringan dapat dihindari danstabilitas keamanan jaringan dapat lebih ditingkatkan.

Hasil akhir pada penelitian menunjukkan bahwa untuk metode yang diterapkan dalam penelitian kali ini membuat serveraman. Karena pengacakan port dan block IP membuat pihak yang tidak bertanggung jawab akan berusaha lebih keras untuk menembus dinding firewall.

Kata Kunci : *RandomPort Knocking*, *remote login, server, Port, IP, SSH*..

## I. PENDAHULUAN

Jaringan (network) adalah sebuah sistem operasi yang terdiri atas sejumlah komputer dan perangkat jaringan lainnya yang bekerja bersama-sama untuk mencapai suatu tujuam yang sama atau suatu jaringan kerja yang terdiri dari titik-titik (nodes) yang terhubung satu sama lain, dengan atau tanpa kabel. Masing-masing nodes berfungsi sebagai stasiun kerja (workstations). Salah satu nodes sebagai media jasa atau server, yaitu yang mengatur fungsi tertentu dari nodes lainnya. Pada dasarnya teknologi jaringan komputer itu sendiri merupakan perpaduan anatara tenologi komputer dan juga teknologi komunikasi.

Sistem Keamanan Jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer.Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang.

Dalam perkembangan jaman, seorang hacker dapat menggunakan multithreading program untuk melakukan penyerangan terhadap jaringan contohnya program brute-force password yang dalam setiap detiknya saja dapat melakukan 1000 kali percobaan penebakan username dan password.

Banyak jenis gangguan keamanan jaringan yang di terapkan oleh orang-orang yang tidak bertanggung jawab

oleh sebab itu, penulisan skripsi ini bertujuan untuk memberikan solusi yang tepat terhadap permasalahan jaringan komputer guna keamanan dan kestabilan jaringan dapat tetap terjaga. Metode yang digunakan dalam skripsi ini menggunakan random port knocking yakni dimana *Random Port Knocking* ini akan memberikan keamanan lebih kepada*server* karena sistem pengetukan *port* yang dilakukan secara random sehingga*port* yang diketuk untuk membuka *port* utama tidak akan mudah untuktermonitoring. Dengan mengacak beberapa *port* yang yang akan diketuk padametode *Random Port Knocking* ini maka setiap *port* yang diketuk pada setiapsesinya akan berbeda – beda sehingga integiritas keamanan dapat lebihditingkatkan.

### 1.2 Rumusan Masalah

Dari latar belakang yang telah dikemukakan, dapat dirumuskan sebagai berikut:

1. Bagaimana merancang sistem kemanan jaringan menggunakan metode random port knocking ?
2. Bagaimana performansi pengacakan port ?
3. Bagaimana melakukan proses pengiriman data hasil ke telegram ?

## II. TINJAUAN PUSTAKA

### A. Port

Dalam protokol jaringan TCP/IP, sebuah port adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. Port dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, port juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam server.

### B. Port Knocking

Port Knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protocol TCP, UDP maupun ICMP. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule knocking yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah diblock.

### C. Firewall

Pengertian *Firewall* adalah sebuah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internet. Untuk mencegah berbagai serangan yang tidak diinginkan, firewall bekerja dengan mengontrol baik itu melacak, mengendalikan dan memutuskan suatu perintah bahwa jaringan ini boleh lewat (pass), perlu dijatuhkan (drop), perlu ditolak (reject), melakukan enkripsi serta mencatat history atau aktivitas data.

### D. Wireshark

Wireshark adalah program Network Protocol Analyzer alias penganalisa protokol jaringan yang lengkap. Program ini dapat merakam semua paket yang lewat serta menyeleksi dan menampilkan data tersebut sedetail mungkin, misalnya postingan komentar kamu di blog atau bahkan Username dan Password.Wireshark utamanya dibuat untuk Administrator Jaringan untuk dapat melacak apa yang terjadi didalam jaringan miliknya atau untuk memastikan jaringannya bekerja dengan baik, serta tidak ada yang melakukan hal hal buruk pada jaringan itu.

### E. Raspberry Pi 3 Model B

Raspberry Pi 3 Model B adalah generasi ketiga dari Raspberry Pi. Jenis *credit-card* yang kuat ini berukuran tunggal board komputer dan dapat digunakan untuk banyak aplikasi dan menggantikan *the original* Raspberry Pi Model B + dan Raspberry Pi 2 Model B. Untuk mempertahankan format *board* populer, Raspberry Pi 3 Model B

membawakan prosesor yang lebih kuat, 10x lebih cepat dari generasi pertama Raspberry Pi. Selain itu, menambah konektivitas LAN &*bluetooth* nirkabel menjadikannya solusi ideal untuk desain koneksi yang kuat.

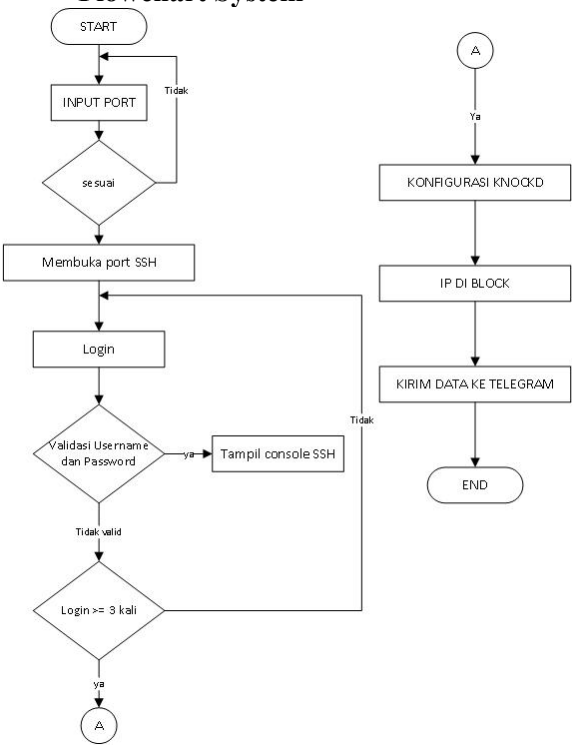
### F. Telegram

Telegram adalah Aplikasi pesan chatting yang memungkinkan pengguna untuk mengirimkan pesan chatting rahasia yang dienkripsi end-to-end sebagai keamanan tambahan. Dengan Telegram, Xplorer juga dapat berbagi lebih dari sekedar gambar dan video, tapi Telegram juga memungkinkan Xplorer mentransfer dokumen atau mengirim lokasi Xplorer saat ini ke teman dengan mudah.

## III. ETODE PENELITIAN

### A. Model Sistem

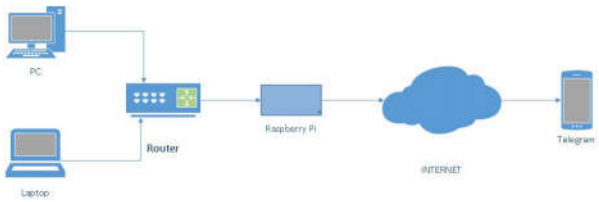
- **Flowchart System**




1. User akan melakukan knock terlebih dahulu untuk bisa masuk ke port SSH
2. Jika sudah berhasil melakukan knocking maka selanjutnya user akan melakukan login pada port SSH
3. Login dengan cara memasukkan username dan password, saat login kurang <= 3 kali berhasil maka akan tampil console SSH (berhasil).
4. ketika login melakukan percobaan login lebih dari 3 kali maka port akan berganti dan IP akan diblock.
5. Data IP yang diblock dan port yang berganti secara acak tersebut akan dikirim ke telegram, sebagai control *administrator* jaringan

- **B**

**lok Diagram Perangkat**




**Gambar 3.3** Blok Diagram Perangkat

Gambar 3.3 menjelaskan blok diagram perangkat yang terdiri dari perangkat. Dari gambar diatas terdapat 3 sistem utama yaitu blok input,blok proses dan blok output, berikut merupakan keterangan dari masing-masing blok diatas :

**Blok Input** Pada blok input terdiri dari PC dan Laptop yang terhubung dengan AP/Router. Inputan berupa port, username,password dan IP yang digunakan untuk masuk dan mengakses SSH.

**Blok Proses** Pada blok proses ini terdiri dari atas sebuah Raspberry Pi 3 B yang bertugas mengolah data hasil dari proses blok input serta berfungsi sebagai pengatur jalannya sistem.

**Blok Output**Pada blok outout sistem terdiri dari telegram yang mendukung proses pengambilan data, menampilkan data hasil pemrosesan pada blok output. Disini telegram berfungsi sebagai tools dari administrator jaringan yang memberikan informasi terkait perubahan port dan IP.

### 3.4 Perancangan Akses Login SSH

Dalam perancangan knock untuk menghindari layanan servis remote login orang yang tidak bertanggung jawab, langkah pertama membuat ID login untuk melakukan monitoring server beserta fungsinya, seperti table 3.6 berikut ini :

**Tabel 3.1 Pembuatan ID Login SSH**

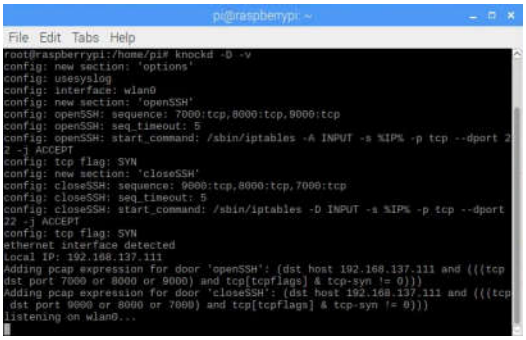
| No | Username | Password |
|---|---|---|
| 1 | Pi | Raspberry |

selanjutnya melakukan perancangan service remote login via knock dijelaskan untuk blok knock dimana aplikasi untuk melakukan knocking pada server terlebih dahulu. Untuk blok knock merupakan port yang dikirim secara acak dengan waktu akses yang berbeda-beda setiap blok knocknya. Untuk blok selanjutnya apabila client sukses melakukan knock diperbolehkan untuk melakukan akses service remote login terhadap port SSH dengan software putty atau yang lain

Pengguna melakukan knocking dengan cara menuliskan alamat ip dan port tujuan, contoh penulisan yang dimaksud seperti 198.162.10.1 2300 4000 6000. Apabila client sukses melakukan knock secara otomatis Port SSH akan terbukadan client dapat melakukan login port SSH.

### 3.5 Konfigurasi KnockD

Konfigurasi knockD disini adalah melakukan pengaturan pada system secara keseluruhan meliputi proses knocking (pengetukan / buka tutup port), proses pergantian port secara random dan proses pemblokiran IP. Berikut adalah perintah yang digunakan unutk menjalankan knockD .

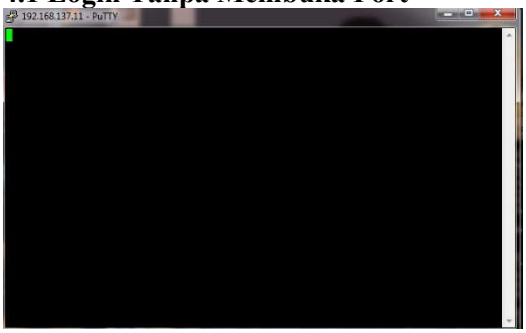



Pada proses tersebut dapat diketahui nilai port yang terbuka dan port yang digunakan untuk menutup kembali, dapat dilihat pula adanya alamat IP yang tertulis, hal ini mengartikan bahwa proses knockd sedang berjalan pada IP tersebut.

## IV. H ASIL DAN PEMBAHASAN

### A. H asil Pengujian Knocking

#### 4.1 Login Tanpa Membuka Port




**Gambar 4.1** kondisi tanpa proses knocking terlebih dahulu

Pada gambar diatas terlihat bahwa tidak ada perintah atau lebih tepatnya blank. Hal ini terjadi karea client tidak melakukan pengetukan port terlebih dahulu. Sehingga tidak bisa menuliskan perintah untuk akses kedalam port server yang dituju.

#### 4.2 Login Dengan Membuka Port

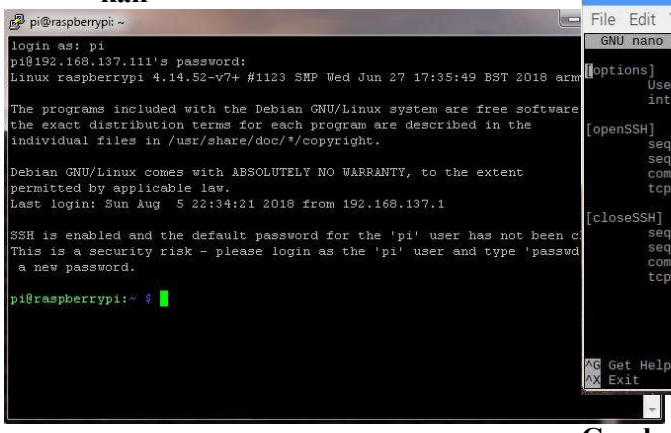

**Gambar 4.2** kondisi port terbuka

Gambar diatas merupakan hasil ketika sebelumnya kita sudah melakukan pengetukan port dengan benar. Dimana akan diteruskan ke halaman login SSH. Pada halaman tersebut kita akan diminta mengisikan username dan password terlebih dahulu.

### 4.3 Hasil Pengujian Knockd

Pada pengujian kali ini ada dua keadaan yakni keadaan dimana client berhasil melakukan login kurang dari tiga kali dan lebih dari tiga kali. Berikut hasil pengujiannya :

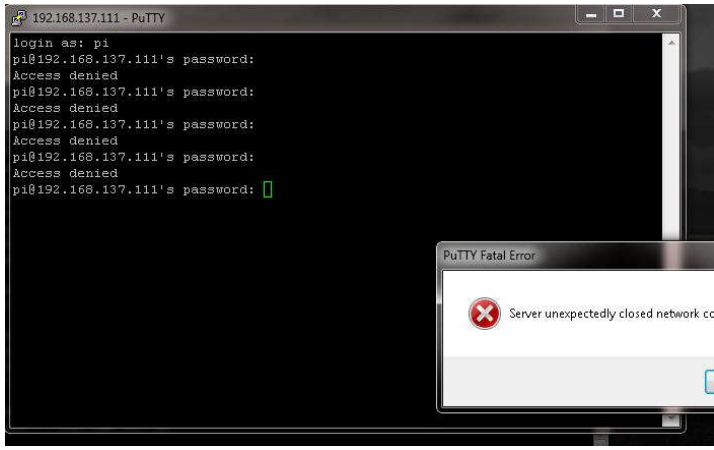
#### 4.3.1 Hasil Pengujian Login<= 3 kali




**Gambar 4.3** hasil pengujian login <= 3 kali

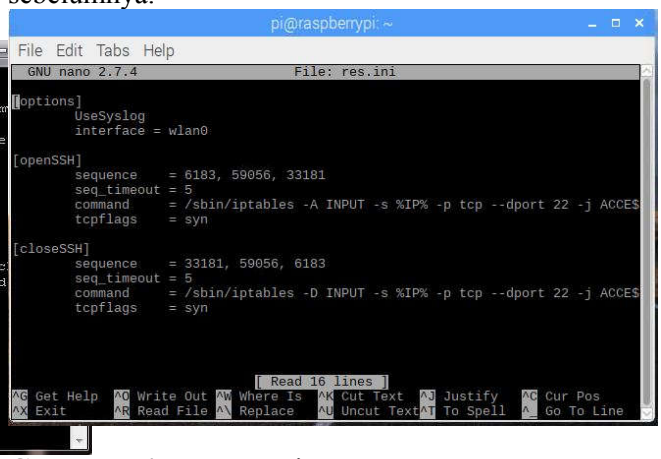
Dalam gambar diatas dapat diketahui bahwa ketika kita berhasil melakukan login maka secara otomatis kita akan masuk ke halaman console SSH, dimana kondisi tersebut menunjukkan bahwa kita bisa melakukan akses terhadap port SSH dan menujukkan bahwa port SSH telah terbuka.

#### 4.3.2 Hasil Pengujian Login Lebih dari tiga kali




**Gambar 4.4** Login lebih dari tiga kali

Pada gambar diatas merupakan hasil unutk kesalahan saat login yang lebih dari tiga kali, dimana secara otomatis IP akan diblok dan tidak bisa melakukan akses apapun. Selanjutnya selain pengamanan dalam segi IP disini juga port akan kembali berganti secara acak, sehingga pengguna yang awal tidak akan bisa membuka port dengan port yang sebelumnya.




**Gambar 4.5** Pergantian Port Baru secara Acak

Port yang sebelumnya 7000 8000 9000 terlah berganti menjadi port seperti pada gambar diatas, hal ini diakibatkan karena kesalahan login yang lebih dari tiga kali tersebut. Berikut merupakan table hasil proses knokcd

## V.PENUTUP

### 5.1 Kesimpulan

Berdasarkan hasil penelitian Penerapan Sistem Keamanan

Jaringan Menggunakan Random Port Knocking Berbasis Raspberry Pi Yang Dikirm Melewati Telegram yang telah dijelaskan dan diuraikan pada bab sebelumnya dalam skripsi ini, dapat disimpulkan bahwa :

1. Dengan metode pengacakan port yang dilakukan orang lain tidak bisa menggunakan port awal untuk masuk.
2. Metode random port knocking ini bekerja dengan baik, sebab pergantian port terjadi ketika login gagal > 3 kali.

**5.2 Saran**

Beberapa saran yang digunakan guna pengembangan lebih lanjut antara lain :

1. Pada penelitian selanjutnya bisa diimplementasikan ke jaringan yang lebih kompleks seperti LAN dll.
2. Random port knocking ini dapat di integrasikan dengan beberapa metode pengamanan jaringan yang lain contohnya dengan honeypot dll.

**DAFTAR PUSTAKA**


1. http://www.portknocking.org/ diakses pada tanggal 3 juli 2018 pukul 10:38 WIB
2. https://keamanan-informasi.stei.itb.ac.id/category/firewall/ diakses pada tanggal 3 juli 2018 pukul 10:53 WIB
3. https://media.neliti.com/media/publications/67747-ID-analisa-dan-implementasi-sistem-keamanan.pdf diakses pada tanggal 3 juli 2018 pukul 11:30 WIB
4. Zainal dan Syaifudin "Implementasi Authentication System Pada Port Knocking Ubuntu Server Menggunakan Knockd Dan Python" *Jurnal SISTEMASI, Volume 7, Nomor 2, Mei 2018 : 169 – 175*
5. Awan, Awan. "Memberikan Akses Legal Terhadap Port Tertentu Yang Telah Ditutup oleh Firewall dengan Metode Port Knocking." *Jurnal Ilmiah CORE IT* 2.1 (2017).
6. Rika dan Reza " membandingkan analisa trafik data pada jaringan computer antara wireshark dan Nmap" Konferensi Internasional Sistem Informasi 2011
7. Richard dan Helmy "Rancang Bangun Pendeteksi Gerak Menggunakan Metode Image Subtraction Pada Single Board Computer (Sbc)" Jurnal Stikom (2018)
8. Triasanti, Dina. 2001. Konsep Dasar Phyton. Jakarta.
9. Wilman dkk, "Port Knocking Dan Honeypot Sebagai Keamanan Jaringan Pada Server Ubuntu Virtual" Jurnal Informatika (2018)
10. Puji Aprianto "Implementasi Simple Port Knocking Pada Dynamic Routing (Ospf) Menggunakan Simulasi Gns3" Jurnal Informatika (2016)
11. Efendi Zulham " Implementasi Port Knocking Pada Sistem Keamanan Informasi Menggunakan Bahasa C" Tugas Akhir 2016
12. Teza Lesmana "Sistem Keamanan Pada Static Port Dalam Jaringan Menggunakan Port Knocking" jurnal teknologi Informasi (2017)

13. Nasrulloh Hasby Meningkatkan Sistem Keamanan Port Service Remote Login Pada Server MEnggunakan Metode Port Knocking" Skripsi JTd (2015)