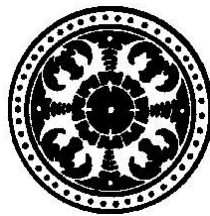


**KEAMANAN JARINGAN MENGGUNAKAN FIREWALL
DENGAN METODE RANDOM PORT KNOCKING
UNTUK KONEKSI SSH**

KOMPETENSI JARINGAN KOMPUTER

SKRIPSI



DANIE YOGA KRISTIANTO

NIM. 1108605024

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS UDAYANA
BUKIT JIMBARAN**

2015

SURAT PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan di bawah ini menyatakan bahwa naskah Skripsi dengan judul :

“Keamanan Jaringan Menggunakan Firewall Dengan Metode Random Port Knocking Untuk Koneksi SSH.”

Nama : Danie Yoga Kristianto
NIM : 11086050424
Program Studi : Teknik Informatika
E-mail : Daniyoga.bali@gmail.com
Nomor telp/HP : 081999131963
Alamat : Jl. Imam Bonjol no 128

Belum pernah dipublikasikan dalam dokumen skripsi, jurnal nasional maupun internasional atau dalam prosiding manapun, dan tidak sedang atau akan diajukan untuk publikasi di jurnal atau prosiding manapun. Apabila di kemudian hari terbukti terdapat pelanggaran kaidah – kaidah akademik pada karya ilmiah saya, maka saya bersedia menanggung sanksi-sanksi yang dijatuhkan karena kesalahan tersebut, sebagaimana diatur oleh Peraturan Menteri Pendidikan Nasional Nomor 17 Tahun 2010 tentang Pencegahan dan Penanggulangan Plagiat di Perguruan Tinggi.

Demikian Surat Pernyataan ini saya buat dengan sesungguhnya untuk dapat dipergunakan bilamana diperlukan.

Denpasar, 1 Oktober 2015

Yang membuat pernyataan,

(Danie Yoga Kristianto)

NIM. 1108605024

LEMBAR PENGESAHAN TUGAS AKHIR

Judul : Keamanan Jaringan Menggunakan *Firewall* Dengan
Metode *Random Port Knocking* Untuk Koneksi SSH.
Kompetensi : Jaringan Komputer
Nama : Danie Yoga Kristianto
NIM : 1108605024
Tanggal Seminar :

Disetujui Oleh :

Pembimbing I

Penguji I

I Komang Ari Mogi, S.Kom, M.Kom

NIP. 198409242008011007

Nama Penguji

NIP.

Pembimbing II

Penguji II

Drs I Wayan Santiyasa, M.Si

NIP. 196704141992031002

Nama Penguji

NIP.

Penguji III

Nama Penguji

NIP.

Mengetahui,

Jurusan Ilmu Komputer FMIPA UNUD

Ketua,

Drs. I Wayan Santiyasa, M.Si

NIP. 19670414 199203 1 002

Judul : Keamanan Jaringan Menggunakan *Firewall* Dengan Metode *Random Port Knocking* Untuk Koneksi SSH.
Nama : Danie Yoga Kristianto.
NIM : 1108605024
Pembimbing : 1. I Komang Ari Mogi, S.Kom, M.Kom.
2. Drs. Wayan Santiyasa, M.Si.

ABSTRAK

Integritas keamanan dewasa ini sangatlah penting untuk ditingkatkan, celah-celah keamanan yang terdapat pada jaringan dapat dilihat oleh orang yang tidak bertanggung jawab dan dapat menjadi ancaman yang patut diperhatikan.

Berhubungan dengan hal itu, *administrator* jaringan dituntut berkerja 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 *Secure Shell* (SSH). Prinsip dasar dari SSH yaitu membuka terus *port* (22) tempat SSH *server* berada, lalu administrator jaringan akan melakukan login kedalam *port* tersebut yang selanjutnya *port* SSH akan terbuka dan komunikasi dapat dilakukan antara *client* dengan *server*. *Port* SSH yang selalu terbuka merupakan suatu celah keamanan jaringan yang dapat digunakan oleh orang yang tidak bertanggung jawab untuk masuk kedalam *server*. Dengan menggunakan serangan *Brute force* yang sudah dimodifikasi dengan *multithreading*, maka seseorang dapat melakukan percobaan menebak *password* SSH sampai 1000 kali dalam sekali percobaan menebak.

Berfokus pada permasalahan tersebut, pada penelitian ini, *Random Port Knocking* merupakan cara yang tepat dan dapat dipakai untuk meningkatkan keamanan pada *port* SSH. Dengan *Random Port Knocking* maka *port* SSH akan dibuka sesuai dengan kebutuhan sehingga serangan *Brute force* dapat dihindari dan stabilitas keamanan jaringan dapat lebih ditingkatkan.

Kata Kunci : *Secure Shell, firewall, iptables, port-port dalam jaringan, Brute force, Random Port Knocking.*

Title : Keamanan Jaringan Menggunakan *Firewall* Dengan Metode *Random Port Knocking* Untuk Koneksi SSH.
Name : Danie Yoga Kristianto.
Registration : 1108605024
Supervisor : 1.I Komang Ari Mogi,S.Kom,M.Kom.
2. Drs. Wayan Santiyasa, M.Si.

ABSTRACT

Nowdays, safety integrity is essential for enhanced contents, vulnerabilities found on the network can be seen by people who are not responsible, and can be a threat noteworthy.

Associated with it, the network administrator is required to secure a work over computer networks management. One form of network security that is often used by a network administrator in the management server that is through remote login such as Secure Shell (SSH). The basic principle of the SSH *port* (22) is open continuously where SSH server is located, then the network administrator logged into the *port* furthermore SSH *port* will open and communication can be done between the client and server. SSH *port* that always open is a network security loopholes that can be used by people who are not responsible to entry into the server. By using the Brute force attack that has been modified with multithreading, then someone can experiment SHH password guessing until 1000 times in one experiment guessing.

Focusing on these problems, in this study, the Random *Port* Knocking is an appropriate way and possibly used to improve security in the SSH *port*. With Random *Port* Knocking then the SSH *port* will be opened in accordance with the needs that Brute force attack can be avoided and the stability of network security can be further improved.

Keywords:Secure Shell, firewall, iptables, ports in networking, Brute force, Random Port Knocking.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadapan Tuhan Yang Maha ESA, karena atas karuniaNya lah, penulis dapat menyelesaikan laporan tugas akhir“Keamanan Jaringan Menggunakan *Firewall* Dengan Metode *Random Port Knocking* Untuk Koneksi SSH” tepat pada waktunya.

Selama prosespenyusunantugas akhir ini , penulis telah banyak memperoleh bimbingan, pengarahan, petunjuk dan saran yang keseluruhannya membantu hingga akhir penyusunan laporan ini. Untuk itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada yang terhormat :

1. Bapak Drs. I Wayan Santiyasa, M.Si., selaku Ketua Jurusan Ilmu Komputer yang telah memberikan dukungan dalam penyelesaian tugas akhir ini.
2. Bapak I Komang Ari Mogi,S.Kom,M.Kom. selaku pembimbing I yang senantiasa membimbing dan mengarahkan penulis dalam guna menyempurnakan tugas akhir ini.
3. Bapak Drs. I Wayan Santiyasa, M.Si. selaku pembimbing II yang telah bersedia mengoreksi, memberi kritik dan saran dalam penyusunan dan penyempurnaan tugas akhir ini.
4. Keluarga dan rekan-rekan yang telah memberikan kontribusi dalam penyelesaian tugas akhir ini.

Akhir kata penulis berharap semoga laporan ini bermanfaat bagi semua pihak, dan penulis menyadari laporan ini masih jauh dari kesempurnaan, penulis mengharapkan kritik dan saran yang membangun demi kesempurnaan laporan ini.

Denpasar, September 2015

Penulis

Danie Yoga Kristianto

DAFTAR ISI

LEMBAR PENGESAHAN TUGAS AKHIR	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR TABEL	ix
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Batasan Masalah	3
1.5 Manfaat	3
1.6 Metodologi Penelitian	3
1.7 Identifikasi Dan Perumusan Masalah	4
1.8 Desain Penelitian	4
1.8.1 Skenario Pengujian	5
BAB II TINJAUAN PUSTAKA	7
2.1 <i>Port Knocking</i>	7
2.1.1 Pengertian <i>Port Knocking</i>	7
2.1.2 Mekanisme Pengetukan <i>Port</i>	7
2.2 <i>SSH (Secure Shell)</i>	10
2.3 <i>Firewall</i>	11
2.3.1 Fungsi <i>Firewall</i>	11
2.3.2 Karakteristik <i>Firewall</i>	12
2.4 <i>IPTables</i>	13
2.5 <i>Brute-Force Attack</i>	14
2.6 <i>NETCAT</i>	14
2.7 <i>Pseudo Random Number Generator</i>	14
2.8 <i>Linear Congruential Generator (LCG)</i>	15
2.9 <i>Random Port Knocking</i>	18

BAB III ANALISIS DAN PERANCANGAN SISTEM	21
3.1 Analisis Kebutuhan Sistem.....	21
3.2 Model Rancangan Eksperimental Penelitian.....	21
3.2.1 Topologi Jaringan	22
3.2.2 Pseudocode.....	22
3.2.3 <i>Flowchart</i>	25
3.2.4 Proses penentuan <i>Random Port Knocking</i>	27
BAB IV HASIL DAN PEMBAHASAN	29
4.1 Tahap Implementasi	29
4.1.1 Instalasi	29
4.1.2 Konfigurasi.....	30
4.2 Pengujian Pengacakan <i>Random Port</i>	31
4.3 Pengujian Sistem	37
BAB V PENUTUP.....	52
5.1 Kesimpulan.....	52
5.2 Saran	52
DAFTAR PUSTAKA	53
LAMPIRAN.....	55

DAFTAR GAMBAR

Gambar 2.1.2.1 Kondisi 1 <i>Port Knocsking</i>	8
Gambar 2.1.2.2 Kondisi 2 <i>Port Knocking</i>	9
Gambar 2.1.2.3 Kondisi 3 <i>Port Knocking</i>	9
Gambar 4.1.2.4 Kondisi 4 <i>Port Knocking</i>	10
Gambar 2.4.1 Diagram Perjalanan Paket data pada IPTables	13
Gambar 3.2.1.1 Topologi Jaringan	22
Gambar 3.2.3.1 <i>Flowchart Random Port Knocking</i>	25
Gambar 3.2.3.2 Flowcart Linier Congruential Generator	26
Gambar 3.2.4.1 Proses meminta port pada <i>Random Port Knocking</i>	27
Gambar 3.2.4.2 Proses pengetukan port dari sisi <i>client</i>	27
Gambar 3.2.4.3 <i>Port</i> SSH telah terbuka	28
Gambar 3.2.4.4 <i>Port</i> SSH telah terbuka	28
Gambar 4.1.2.1 Konfigurasi <i>Virtual Machine</i> pada Komputer 1	30
Gambar 4.1.2.2 Konfigurasi <i>Virtual Machine</i> pada Komputer 2	31
Gambar 4.3.1 Tampilan Awal Program <i>Server</i>	39
Gambar 4.3.2 Tampilan Awal Program <i>Daemon</i>	40
Gambar 4.3.3 Tampilan Awal Program <i>Client</i>	41
Gambar 4.3.4 Koneksi SSH Ditolak	42
Gambar 4.3.5 Port SSH Telah Tertutup	425
Gambar 4.3.6 <i>Request 3 Port random</i>	446
Gambar 4.3.7 Percobaan Koneksi SSH Kembali Gagal	457
Gambar 4.3.8 Proses Pengetukan 3 <i>Port random</i>	457
Gambar 4.3.9 Ketuk <i>Port</i> 1 Sukses	468
Gambar 4.3.10 Ketuk <i>Port</i> 2 Sukses	479
Gambar 4.3.11 Ketuk <i>Port</i> 3 Sukses	479
Gambar 4.3.12 Pengetukan Berhasil – <i>Port</i> SSH Terbuka Kembali	40
Gambar 4.3.13 Port SSH Terbuka Kembali	41
Gambar 4.3.14 Tutup SSH pada Client	42
Gambar 4.3.15 Tutup SSH pada Server	42

DAFTAR TABEL

Tabel 3.1 Tabel Spesifikasi Kebutuhan Sistem.....	21
---	----