Analisa Kinerja Metode *Hybrid Port Knocking* pada Sistem Operasi *Linux*

SKRIPSI

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Komputer

Monica Sabrina Jusuf

08110210014

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2014

HALAMAN PENGESAHAN

ANALISA KINERJA METODE *HYBRID PORT KNOCKING* PADA SISTEM OPERASI *LINUX*

Oleh

Nama : Monica Sabrina Jusuf
NIM : 08110210014
Fakultas : Teknologi Informasi dan Komunikasi
Program Studi : Sistem Komputer

Bahwa telah diujikan pada hari Jumat tanggal 24 Oktober 2014 pukul 13.00-15.30 di

Universitas Multimedia Nusantara, Tangerang

Dosen Pembimbing

Hargyo T. N. I., S.Kom, M.Sc

Dosen Penguji

Kanisius Karyono, S.T, M.T

Ketua Sidang

Dr. Hugeng, S.T.,M.T

Mengetahui:

Ketua Program Studi Sistem Komputer

Kanisius Karyono, S.T, M.T

LEMBAR PERNYATAAN

TIDAK MELAKUKAN PLAGIAT

Dengan ini saya:

Nama : Monica Sabrina Jusuf

NIM : 08110210014

Fakultas : Teknologi Informasi dan Komunikasi

Program Studi : Sistem Komputer

Menyatakan bahwa skripsi yang saya buat untuk memenuhi persyaratan kelulusan pada Fakultas Teknologi Informasi dan Komunikasi, Jurusan Sistem Komputer Universitas Multimedia Nusantara dengan judul **ANALISA KINERJA METODE *HYBRID PORT KNOCKING*PADA SISTEM OPERASI *LINUX*** adalah karya ilmiah sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka.

Tangerang, 24 Oktober 2014

(Monica Sabrina Jusuf)

ABSTRAK

Hybrid port knocking(HPK) merupakan pengembangan metode *port knocking*yang menggunakan tiga konsep yaitu *port knocking*, steganografi, dan *mutual authentication* untuk meningkatan keamanan jaringan. Pada penelitian ini, dilakukan pengujian kinerja *hybrid port knocking*[4] berbasis enkripsi GnuPG menggunakan RSA and RSA *public key algorithm*, DSA and ElGamal *public-key algorithm* serta DSA and RSA *public key algorithm*. Hasil uji coba menunjukkan bahwa *HPK server* dan *client* script berbasis *DSA and ElGamal public key algorithm* memerlukan waktu dan konsumsi memori paling banyak, diikuti dengan *HPK server* dan *client script* berbasis *DSA and RSA public key algorithm* lalu *HPK server* dan *client* script berbasis *RSA and RSA public key algorithm*. Perbedaan ini terjadi karena algoritma ElGamal melakukan enkripsi dengan menggunakan perhitungan logaritma diskrit sehingga memerlukan waktu lebih lama dalam pemrosesannya dibandingkan dengan RSA yang melakukan enkripsi dengan memfaktorkan angka dalam jumlah besar.

Kata kunci: *Port knocking,* HPK, *Firewall, kriptografi, steganografi, mutual authentication*

ABSTRACT

Hybrid port knocking(HPK) is another form of port knockingtechnique that utilizes three concepts, these are port knocking, steganography, and mutual authentication, to improve network security. In this research, the performance of HPK[4] *with RSA and RSA public-key algorithm, DSA and ElGamal public-key algorithm, DSA and RSA public-key algorithm was analized to know how fast are HPK server and client script running, how much memory are consumed. The experiment result shows that HPK server and client script with DSA and ElGamal public key algorithm needs more time and memory than the others, followed by HPK server and client script with DSA and RSA public key algorithm, then HPK server and client script with RSA and RSA public key algorithm. The difference is caused by the computation complexity such as ElGamal algorithm that uses complex discrete logartihm for encryption so that it needs more processing time than RSA that use large number factorization.*

Keyword: Port knocking, HPK, firewall, cryptography, steganography, mutual authentication

KATA PENGANTAR

Puji dan syukur dipanjatkan kepada Tuhan Yang Maha Esa karena atas berkat dan penyertaan-Nya maka laporan skripsi berjudul " Analisa Kinerja Metode *Hybrid Port Knocking* pada Sistem Operasi *Linux*". Laporan ini menjelaskan analisa kinerja *hybrid port knocking*yang meliputi berapa lama waktu yang diperlukan untuk meng-*execute* HPK *server script* dan *client script* juga berapa banyak penggunaan memori yang digunakan oleh HPK *server script* dan *client script.* Skripsi ini dibuat dalam rangka menyelesaikan studi dan sebagai syarat kelulusan di Universitas Multimedia Nusantara.

Penyelesaian laporan skripsi ini tidak lepas dari bantuan beberapa pihak, sehingga penulis ingin mengucapkan terima kasih kepada:

1. Ibu Yohanna, mama dari penulis yang selalu mendoakan dan mendukung kebutuhan baik materi maupun moril.
2. Bapak Hargyo Tri Nugroho, S.Kom, M.Sc, selaku pembimbing tugas akhir yang telah mengarahkan, mendidik, dan membantu penulis hingga proses akhir.
3. Ibu Hira Meidia, B.Eng, PhD, selaku pembimbing akademik penulis.
4. Bapak Kanisius Karyono, S.T, M.T, selaku kepala program studi
5. Bapak Dr. Hugeng, S.T, M.T, selaku ketua sidang
6. Oma Setiati Soetjipto dan oma Tabitha Soetjipto yang selalu mendoakan penulis
7. Daniel Franco Cecilia, yang mendukung dan memotivasi selama proses pengerjaan skripsi, *"muchas gracias por todo, Dan"*.
8. Inez, yang selalu menyemangati penulis.

9. Teman-teman seperjuangan SK 2008 khususnya Vania Utami yang senantiasa mendukung dan memberi semangat, Linda, Stenley, Gani, Firdaus, Ersa, dan Felix.
10. Tante Paula Van Bekkum dan dedek Nidya yang selalu mendoakan serta mendukung penulis
11. Chendy J.B dan Permata Karina yang menemani dan menyemangati penulis.
12. Tante Sarmalina, ibunda dari Vania yang juga menyemangati.
13. Saudara-saudara penulis yang mendoakan
14. Pihak-pihak yang tidak dapat disebutkan satu per satu.

Dalam penyusunan skripsi ini, penulis mengakui bahwa masih belum sempurna. Oleh karena itu, saran dan kritik yang membangun ke arah yang lebih baik akan sangat diterima. Mudah-mudahan skripsi ini dapat membantu dan bermanfaat bagi pembaca dan pihak-pihak yang membutuhkannya.

Tangerang, Oktober 2014

Monica Sabrina

DAFTAR ISI

JUDUL : ANALISA KINERJA KEAMANAN JARINGAN MENGGUNAKAN METODE *HYBRID PORT KNOCKING* PADA SISTEM OPERASI *LINUX*

HALAMAN PENGESAHAN.....i

LEMBAR PERNYATAAN TIDAK MELAKUKAN PLAGIAT.....ii

ABSTRAK iii

ABSTRACT iv

KATA PENGANTAR.....v

DAFTAR ISI.....vii

DAFTAR GAMBAR..... ix

DAFTAR TABEL.....xi

DAFTAR RUMUS xiii

BAB I PENDAHULUAN.....1

1.1 Latar Belakang.....1

1.2 Tujuan dan Manfaat 2

1.3 Rumusan Masalah 3

1.4 Batasan Masalah 3

1.5 Sistematika Laporan 3

BAB II DASAR TEORI.....5

2.1 Firewall 5

2.2 Kriptografi 9

2.2.1 *Public-key Algorithms*.....11

2.2.1.1 RSA.....13

2.2.1.2 ElGamal.....14

2.2.1.3 DSA.....15

2.3 Steganografi.....16

2.4 *Mutual authentication*.....17

2.5 Penelitian sebelumnya.....17

BAB III METODOLOGI PENELITIAN.....22

3.1 Gambaran Umum Penelitian 22

3.2 Metode Penelitian.....22

3.3 Spesifikasi umum sistem 23

3.4 *Flow Chart* 25

3.5 Pembangunan Lingkungan Uji coba.....29

3.6 Struktur Navigasi Aplikasi.....30

3.7 Metode Pengujian.....33

BAB IV UJI COBA DAN PEMBAHASAN.....35

4.1 Spesifikasi Perangkat.....35

4.2 Implementasi.....36

4.2. 1 Implementasi metode *Hybrid port knocking*.....36

4.2.2 Kinerja Sistem.....43

BAB V KESIMPULAN DAN SARAN.....58

5.1 Kesimpulan 58

5.2 Saran 59

Daftar Pustaka.....60

DAFTAR GAMBAR

Gambar 2.1 Penggunaan *firewall* pada umumnya[8]..... 5

Gambar 2.2 *Packet Filtering Firewall*[8].....7

Gambar 2.3 *iptables* untuk *hybrid port knocking*.....8

Gambar 2.4 Skema kriptografi [6].....9

Gambar 2.5 Model enkripsi simetris[8].....10

Gambar 2.6 GnuPG key di sisi *server*.....12

Gambar 2.7 GnuPG key di sisi *client*.....12

Gambar 2.8 Algoritma RSA[7].....14

Gambar 2.9 Proses Algoritma ElGamal[7].....15

Gambar 2.10 Proses DSA[9] 15

Gambar 2.11 Proses Steganografi [10].....16

Gambar 2.12 Cara kerja *port knocking*[2].....18

Gambar 3.1 Hybrid *port knocking flowchart*[3].....27

Gambar 3.2 *Server* melakukan *monitoring*[3].....25

Gambar 3.3 *Server* meng-*capture payload* yang berisi gambar[3].....26

Gambar 3.4 *Server* meminta *firewall* untuk membuka *port* bagi *client*[3].....26

Gambar 3.5 *Server* memenuhi *client's request*[3].....28

Gambar 3.6 Penutupan *port* [3].....29

Gambar 3.7 Lingkungan Uji Coba *Hybrid port knocking*.....29

Gambar 3.8 *Server Configuration*.....31

Gambar 3.9 *Client configuration*.....31

Gambar 3.10 command untuk *execute server script* melalui terminal.....32

Gambar 3.11 *command execute client's request* untuk membuka *port* 22.....33

Gambar 3.12 Ilustrasi aplikasi *hybrid port knocking*.....33

Gambar 4.1 Client mengirimkan request untuk membuka port 22.....37

Gambar 4.2 Respons *server* terhadap *client's request* untuk membuka *port* 22 37

Gambar 4.3 Client berhasil melakukan login ssh.....38

Gambar 4.4 Client mengirimkan echo message ke server.....38

Gambar 4.5 Server menerima echo message.....39

Gambar 4.6 Client's request untuk me-restart layanan yang disediakan oleh server.....39

Gambar 4.7 Respon server terhadap client's request untuk me-restart layanan.....40

Gambar 4.8 *Client* melakukan *port knock* dengan *port sequence* yang salah.....40

Gambar 4.9 Respon *server* saat *client* melakukan *port knock* dengan *sequence port* yang salah 41

Gambar 4.10 *Client* melakukan *port knock* yang benar namun *sequence port*-nya salah.....42

Gambar 4.11 Respon *server* saat *client* melakukan *port knock* pada *port* yang benar namun dengan *sequence yang* salah 42

Gambar 4.12Grafik konsumsi waktu HPK *server script* berbasis *RSA and RSA public-key algorithm*.....47

Gambar 4.13 Grafik konsumsi waktu HPK *client script* berbasis *RSA and RSA public-key algorithm*.....47
Gambar 4.14 Grafik konsumsi waktu HPK *server script* berbasis *DSA and ElGamal public-key algorithm*.....48
Gambar 4.15 Grafik konsumsi waktu HPK *client script* berbasis *DSA and ElGamal public-key algorithm*.....48
Gambar 4.16 Grafik konsumsi waktu HPK *server script* berbasis *DSA and RSA public-key algorithm*.....49
Gambar 4.17 Grafik konsumsi waktu HPK *client script* berbasis *DSA and RSA public-key algorithm*.....49

DAFTAR TABEL

Tabel 4.1 Konsumsi waktu *hybrid port knocking server script* berbasis *RSA and RSA public-key algorithm* 44

Tabel 4.2 Konsumsi waktu *hybrid port knocking client script* berbasis *RSA and RSA public-key algorithm* 44

Tabel 4.3Konsumsi waktu *hybrid port knocking server script* berbasis *DSA and ElGamal public-key algorithm*.....45

Tabel 4.4 Konsumsi waktu *hybrid port knocking client script* berbasis *DSA and ElGamal public-key algorithm*.....45

Tabel 4.5 Konsumsi waktu *Hybrid port knocking server script berbasis DSA and RSA public-key algorithm*.....46

Tabel 4.6 Konsumsi waktu *Hybrid port knocking client script* berbasis *DSA and RSA public-key algorithm* 46

Tabel 4.7 Konsumsi memori *Hybrid port knocking server script* berbasis *RSA and RSA public key algorithm*.....51

Tabel 4.8 Konsumsi memori *Hybrid port knockingclient script* berbasis *RSA and RSA public key algorithm*.....51

Tabel 4.9 Konsumsi memori *Hybrid port knockingserver script* berbasis *DSA and ElGamal public key algorithm*.....52

Tabel 4.10 Konsumsi memori *Hybrid port knocking client script* berbasis *DSA and ElGamal public key algorithm*.....52

Tabel 4.11 Konsumsi memori *Hybrid port knockingserver script* berbasis *DSA and RSA public key algorithm*.....53

Tabel 4.11 Konsumsi memori *Hybrid port knocking client script* berbasis *DSA and RSA public key algorithm*.....53

DAFTAR RUMUS

Rumus 2.1 Enkripsi dan Dekripsi untuk beberapa blok *plaintext* M dan blok *ciphertext* C [7].....3