



**PENGAMANAN *SERVER* DENGAN METODE *PORT KNOCKING* DAN
KEY AUTHENTICATION PADA LAYANAN *SECURE SHELL* (SSH)**

SKRIPSI

TUBAGUS MUHAMMAD FAWWAZ RASYID

1710511033

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021

PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut :

Nama : Tubagus Muhammad Fawwaz Rasyid
NIM : 1710511033
Program Studi : Informatika
Judul Tugas Akhir : Pengamanan *Server* Dengan Metode *Port Knocking* Dan *Key Authentication* Pada Layanan Secure Shell (SSH)

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



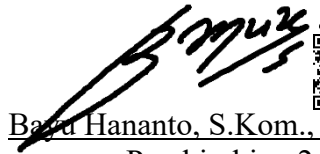
Henki Bayu Seta, S.Kom., MTI
Ketua Penguji



Bambang Tri Wahyono, S.Kom, M.Si.
Anggota Penguji


REVISI_2021

Jayanta, S.Kom., M.Si.
Pembimbing 1



Batu Hananto, S.Kom., M.Kom.
Pembimbing 2



Dr. Ermatita, M.Kom.
Dekan



Yuni Widiastiwi, S.Kom., Msi.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 7 Juli 2021



PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Tubagus Muhammad Fawwaz Rasyid

NIM : 1710511033

Tanggal : 7 juli 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Tangerang Selatan, 7 Juli 2021

Yang Menyatakan,



(Tubagus Muhammad Fawwaz Rasyid)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Tubagus Muhammad Fawwaz Rasyid

NIM : 1710511033

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti NonEksklusif (Non-Exclusive Royalty Free Right) atas karya ilmiah saya yang berjudul:

PENGAMANAN *SERVER* DENGAN METODE *PORT KNOCKING* DAN *KEY AUTHENTICATION* PADA LAYANAN *SECURE SHELL* (SSH)

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di :Tangerang Selatan

Pada Tanggal : 7 Juli 2021

Yang Menyatakan,



(Tubagus Muhammad Fawwaz Rasyid)

PENGAMANAN *SERVER* DENGAN METODE *PORT KNOCKING* DAN *KEY AUTHENTICATION* PADA LAYANAN *SECURE SHELL* (SSH)

Tubagus Muhammad Fawwaz Rasyid

ABSTRAK

Penerapan keamanan lebih pada *server* untuk mengamankan data dari orang yang tidak bertanggung jawab dengan metode *port knocking* dan *key authentication* pada layanan *secure shell* (ssh). Metode *port knocking* adalah metode autentikasi dengan memasukan pola yang telah ditentukan. Metode *key authentication* adalah metode autentikasi dengan menggunakan kunci publik dan kunci privat. Hasil pengujian pengamanan *server* tanpa metode *port knocking* dan *key authentication* dengan pengamanan *server* dengan metode *port knocking* dan *key authentication* berbeda dan pengamanan *server* dengan metode *port knocking* dan *key authentication* tidak dapat direntas dengan metode *sniffing* dan *brute force*. Pengamanan *server* lebih baik menggunakan metode *port knocking* dan *key authentication* dibandingkan dengan tidak memakai pengamanan lebih

Kata Kunci: *port knocking*, *key Authentication*, *secure shell*, keamanan.

SERVER SECURITY WITH PORT KNOCKING METHOD AND KEY AUTHENTICATION IN SECURE SHELL (SSH) SERVICE

Tubagus Muhammad Fawwaz Rasyid

ABSTRACT

Implementation of more security on the server to secure data from irresponsible people by using port knocking and key authentication methods in the secure shell (ssh) service. The port knocking method is an authentication method by entering a predetermined pattern. Key authentication method is an authentication method using a public key and a private key. The results of testing server security without port knocking and key authentication methods with server security using port knocking and key authentication methods are different and server security using port knocking and key authentication methods cannot be hacked by sniffing and brute force methods. Server security is better using port knocking and key authentication methods than not using more security.

Keywords: port knocking, key Authentication, secure shell, security.

KATA PENGANTAR

Pertama saya panjatkan puji dan syukur kepada Allah SWT atas rahmatnya penulis diberikan kesempatan untuk menyelesaikan skripsi tugas akhir dengan judul:” pengamanan *server* dengan metode *port knocking* dan *key authentication* pada layanan *secure shell* (ssh)” yang menjadikan syarat penulis untuk lulus menyelesaikan studi Sarjana Pendidikan Strata Satu Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Tidak lupa penulis berterima kasih atas doa, dukungan, dan bimbingan dari berbagai pihak yaitu:

1. Ibu dan Bapak yang telah mendukung sepenuhnya dan doa-doa yang membuat penulis semangat menyelesaikan laporannya.
2. Bapak Jayanta, S.Kom., M.Si yang telah membimbing saya untuk memperkuat pola pikir dan mental penulis untuk siap-siap pada sidang skripsi yang akan diadakan.
3. Bapak Bayu Hananto, S.Kom., M.Kom yang telah membantu penulis dalam menulis, menyusun, dan memberikan solusi pada BAB 4 yang ditulis.
4. Bapak/Ibu dosen Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan pengetahuan dibidang informatika sehingga penulis mengerti dengan topik yang diambilnya.
5. Teman-teman satu angkatan dan grup Naqos yang telah membantu penulis memberikan informasi yang membantu untuk menyelesaikan skripsi tugas akhir pada tepat waktu.

DAFTAR ISI

PENGESAHAN.....	ii
PERNYATAAN ORISINALITAS.....	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN.....	xiv
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	2
1.3. Batasan masalah.....	3
1.4. Tujuan	3
1.5. Manfaat	3
1.6. Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	5
2.1. Jaringan Komputer.....	5
2.1.1. Jenis Jaringan.....	5
2.2. TCP/IP	6
2.3. <i>Secure Shell</i>	6
2.3.1. <i>Authentication</i> dan RSA.....	8
2.3.2. <i>Public key</i> dan <i>Private key</i>	8
2.3.3. <i>Encryption</i> dan <i>Integrity</i>	8
2.4. Ubuntu dan Kali Linux	9
2.5. Client dan Server	9
2.6. <i>Port knocking</i>	10
2.6.1. Knockd	10

2.7.	<i>Brute force Attack</i> dan Hydra.....	11
2.8.	<i>Sniffing</i> dan ARP <i>poisoning</i>	11
2.9.	<i>Virtual Machine</i> dan VirtualBox.....	11
2.10.	<i>Port</i>	12
2.11.	<i>Firewall</i> dan ASCII	12
2.12.	Wireshark	14
2.13.	Penelitian Terkait.....	14
BAB 3 METODOLOGI PENELITIAN		16
3.1.	Kerangka Pikir	16
3.1.1.	Identifikasi Masalah	16
3.1.2.	Studi literatur	16
3.1.3.	Perancangan Sistem	17
3.1.3.	Pengujian Sistem	21
3.1.4.	Dokumentasi	22
3.2.	Alat Bantu Penelitian	22
3.3.	Jadwal Penelitian	22
BAB IV HASIL DAN PEMBAHASAN		24
4.1.	RSA.....	24
4.2.	Pengujian <i>Server</i> Tanpa Pengamanan	26
4.2.1.	Pengujian <i>Sniffing</i>	26
4.2.2.	Pengujian <i>Brute force</i>	29
4.3.	Implementasi Keamanan <i>Server</i>	33
4.4.1.	<i>Key Authentication</i>	33
4.4.2.	<i>Port Knocking</i>	36
4.4.3.	Administrator melakukan <i>login</i>	39
4.4.	Pengujian <i>Server</i> Dengan Keamanan	41
4.4.1.	Pengujian <i>Sniffing</i>	42
4.4.2.	Pengujian <i>Port Knocking</i> dan <i>Brute force</i>	42
4.5.	Hasil Pengujian	45
BAB V PENUTUP		48
5.1.	Kesimpulan	48
5.2.	Saran	48
DAFTAR PUSTAKA		49

RIWAYAT HIDUP	52
LAMPIRAN.....	53

DAFTAR GAMBAR

Gambar 1. SSH Client dan Server	7
Gambar 2. SSH Authentication	8
Gambar 3. Firewall.....	13
Gambar 4. ASCII	13
Gambar 5. ASCII Extended.....	14
Gambar 6. Kerangka Pikir	16
Gambar 7. Rancangan Keamanan	18
Gambar 8. Flowchart port knocking.....	18
Gambar 9. port 1	19
Gambar 10. port 2	20
Gambar 11. port 3	20
Gambar 12. port 4	20
Gambar 13. Key Authentication.....	21
Gambar 14. Sniffing Attack	26
Gambar 15. Tampilan Tool Ettercap	27
Gambar 16. Serangan ARP Poinsoning.....	28
Gambar 17. Hasil Wireshark.....	29
Gambar 18. gambaran brute force.....	29
Gambar 19. hasil brute force wordlist 1 tanpa pengamanan lebih	30
Gambar 20. hasil brute force wordlist 2 tanpa pengamanan lebih	31
Gambar 21. hasil brute force wordlist 3 tanpa pengamanan lebih	32
Gambar 22. Login Dengan Hasil Dari Brute force	33
Gambar 23. Generate Key	34
Gambar 24. Menyalin Public Key Ke Server	34
Gambar 25. Command Mengedit Configuration	35
Gambar 26. Mengubah Yes Menjadi No	35
Gambar 27. Command Untuk Restart SSH	35
Gambar 28. Command Untuk Menambahkan Expired Pada Key	35
Gambar 29. Scrip Untuk Menghemat Waktu	36
Gambar 30. Command Untuk Install Tool Knockd	36
Gambar 31. Menyesuaikan Ethernet Yang Digunakan	37
Gambar 32. Command Untuk Melihat Ethernet Yang Digunakan	37
Gambar 33. Mengkonfigurasi Pola Yang Akan Digunakan	37
Gambar 34. Pola Yang Digunakan Untuk Membuka Firewall	39
Gambar 35. Command Untuk Memulai Knockd	39
Gambar 36. Command Knock Untuk Membuka Port Pada Server	39
Gambar 37. Log pada Server Menunjukan Firewall Menambahkan Rule.....	39
Gambar 38. Mengecek Status Firewall	40
Gambar 39. Administrator melakukan Login Pada SSH	40
Gambar 40. Command Knock Untuk menutup Port Pada Server	40
Gambar 41. Log pada Server Menunjukan Firewall Menghapus Rule.....	41
Gambar 42. Mengecek Status Firewall	41
Gambar 43. Pola Yang sudah Digunakan Untuk Membuka Firewall.....	41
Gambar 44. Tampilan Hasil Dari Wireshark	42

Gambar 45. Brute force wordlist 1 dengan pengamanan lebih	43
Gambar 46. Brute force wordlist 2 dengan pengamanan lebih	43
Gambar 47. Brute force wordlist 3 dengan pengamanan lebih	44
Gambar 48. Perbandingan Login Berhasil.....	45
Gambar 49. Perbandingan Waktu Serangan Brute Force.....	45

DAFTAR TABEL

Tabel 1. Penelitian Terkait.....	15
Tabel 2. Jadwal Kegiatan Penelitian	23
Tabel 3. pengujian brute force wordlist 1 tanpa pengamanan lebih.....	30
Tabel 4. pengujian brute force wordlist 2 tanpa pengamanan lebih.....	31
Tabel 5. pengujian brute force wordlist 3 tanpa pengamanan lebih.....	32
Tabel 6. pengujian brute force wordlist 1 dengan pengamanan lebih	43
Tabel 7. pengujian brute force wordlist 2 dengan pengamanan lebih	43
Tabel 8. pengujian brute force wordlist 3 dengan pengamanan lebih	44
Tabel 9. Hasil Percobaan Serangan <i>Sniffing</i> Dan <i>Bruteforce</i>	46

DAFTAR LAMPIRAN

Lampiran 1 percobaan brute force wordlist 1 sebelum pengamanan lebih.....	54
Lampiran 2 Percobaan brute force wordlist 2 sebelum pengamanan lebih.....	57
Lampiran 3 Percobaan brute force wordlist 2 sebelum pengamanan lebih.....	62
Lampiran 4 Percobaan brute force wordlist 1 dengan pengamanan lebih	67
Lampiran 5 Percobaan brute force wordlist 2 dengan pengamanan lebih	69
Lampiran 6 Percobaan brute force wordlist 3 dengan pengamanan lebih	71
Lampiran 7. Turnitin skripsi	73