MENINGKATKAN MEKANISME KEAMANAN OTORISASI *PORT* DENGAN METODE *SIMPLE PORT KNOCKING TUNNELING*

EdyHaryanto[1)], Widyawan[2)], Dani Adhipta[3)],
[1)]Universitas Gadjahmada, [2)]Universitas Gadjahmada, [3)]Universitas Gadjahmada
Edy.haryanto.mti13@mail.gmail.com[(1)], widyawan@ugm.ac.id[(2)], dani@ugm.ac.id[(3)]

Abstrak

Port knocking merupakan teknik pertahanan yang digunakan untuk mencegah penyerang melakukan scanning guna mendapatkan informasi tentang kelemahan service yang berpotensi dieksploitasi. Port knocking merupakan sebuah metode otorisasi user berdasarkan firewall untuk melakukan komunikasi melalui port yang tertutup. Akan tetapi port knocking masih memiliki beberapa kelemahan seperti TCP replay, port scanning dan lain-lain. Penelitian ini mengusulkan sebuah metode menggunakan tunneling untuk meningkatkan keamanan, dan source port sequence untuk menyederhanakan proses otorisasi port knocking yang akan menghasilkan metode Port Knocking baru yang lebih sederhana dan lebihaman

Kata Kunci: *Port Knocking; Source Port Sequence; Tunneling*

1. PENDAHULUAN

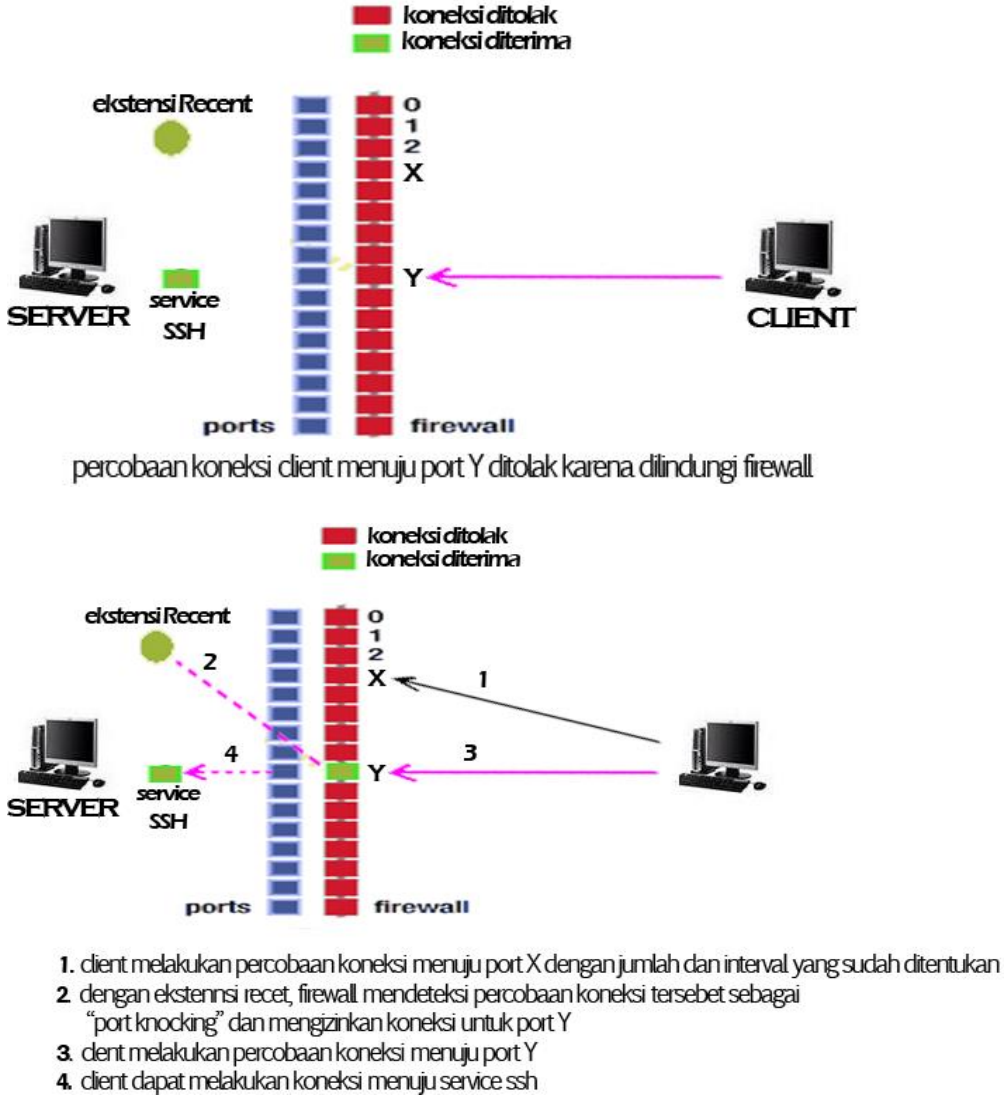
Keamanan jaringan computer telah menjadi perhatian selama bertahun-tahun. Internet merupakan sekumpulan *node* jaringan yang luas dan dihubungkan bersama untuk memberikan layanan yang berbeda. Masalah yang timbul adalah bagaimana melindungi sistem agar aman di saat yang bersamaan dapat diak sesoleh pihak yang sah secara online (Atani, 2012).

Cara yang paling mudah untuk membatasi akses adalah dengan mengharuskan pengguna untuk mengotentikasi dirinya sebelum memberikannya akses, tetapi tetap saja banyak kasus serangan yang dilaporkan (Srivastava, 2011).

Padaumumnya langkah pertama yang dilakukan penyerang adalah mencari informasi lengkap tentang korbanya, seperti layanan yang berjalan, *port* yang terbuka dan versi dari *software* untuk menemukan kelemahan yang belum di-*Patch* bahkan*Zero-Day* (Karzywinski, 2009). *Port Knocking* adalah sebuah metode yang dapat menyembunyikan *service* dari penyerang dengan cara mentransmisikan data melalui *port* yang tertutup.

Padadasarnya *Port Knocking* merupakan sebuah mekanisme keamanan jaringan yang tertanam dalam *Firewall* pada *Secure Computer System*(A Khan, 2011). Pada referensi lain mengatakan bahwa *Port Knocking* adalah sebuah metode otorisasi *user* berdasarkan *firewall* untuk melakukan komunikasi melalui *port* yang tertutup (Ali, 2012). *Port Knocking* merupakan teknik pertama yang diperkenalkan untuk mencegah penyerang melakukan *Discovery* dan *Exploitasi* terhadap layanan-layanan yang berpotensi diserang

pada jaringan komputer korban (Manzanares, 2005). Ilustrasi konsep kerja*Port Knocking* dapat dilihat pada gambar di bawahini.

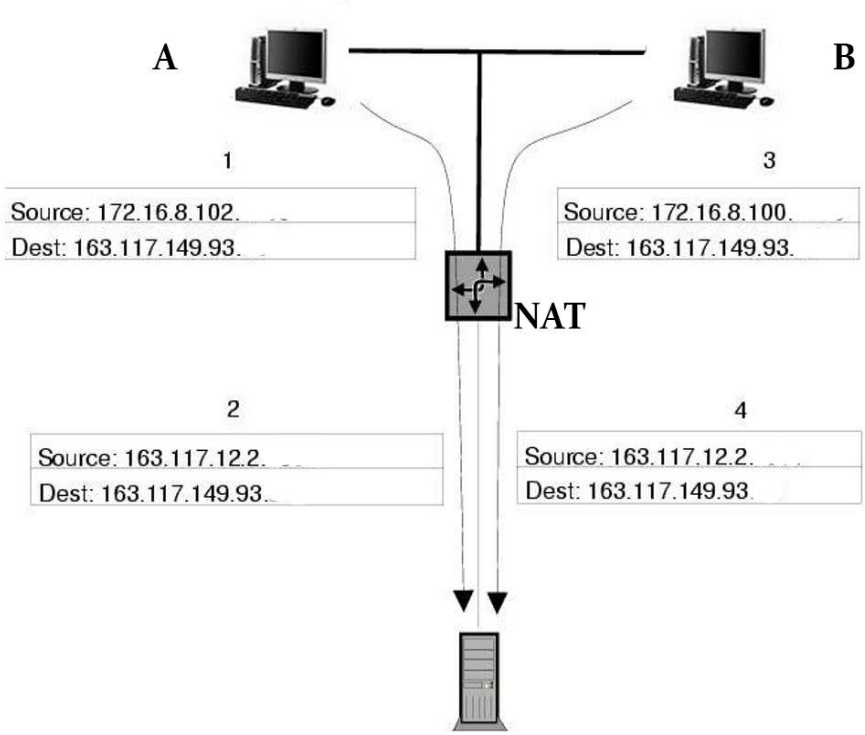


Gambar1.1 Konsepkerja Port Knocking

Port knocking masih rentan terhadap beberapa jenis serangan walaupun di satu sisi dapat memebuat proses otorisasi menjadi lebih aman dari sebelumnya. *DOS-Knocking* dan *NAT-Knocking* adalah beberapa jenis serangan yang umum menyerang*Port Knocking*.

Seperti yang telah di jelaskan sebelumnya, *Port Knocking* akan membuka *port* untuk klien yang telah melakukan valid *Knock Sequnece. Port Knocking* mengidentifikasi *Knock Sequnece* klien berdasarkan *network address* klien. Masalah muncul ketika beberapa klien memiliki *network address* yang sama, contohnya pada kasus *Network Address Translation*

(NAT). ketika beberapa klien mengirimkan paket keluar, dimana klien-klien tersebut berada dalam NAT yang sama, maka semua paket tersebut akan menggunakan *source address* yang sama yaitu *Public address* dari NAT tesebut.



Gambar 1.2 NAT

Seperti gambar diatas, klien A dan B menggunakan *IP Public* yang sama karena mereka harus menggunakan NAT untuk melakukan koneksi keluar *network*. Paket 1 milik klien A akan dirubah menjadi paket 2, dimana *source address* akan dirubah menjadi *public address* milik NAT. Hal yang sama juga terjadi pada paket 3 milik klien B, sehingga bila dilihat dari luar NAT, sangat sulit untuk menentukan paket mana yang berasal dari klien mana yang menggunakan *address* yang mana.

NAT-Knocking terjadi ketika *server* tidak bisa membedakan antara *user* yang valid dan tidak. Hal ini terjadi bila *Network Address Translation* (NAT) diugnakan pada jaringan tersebut, sehingga semua klien pada NAT yang sama akan memiliki *Address* yang sama diluar *local network*. Sehingga jika seorang *user* telah menyelesaikan proses *Port Knocking* dan mendapat akses ke *server*, semua klien pada NAT yang sama dapat mengakses *server* ersebut.

Untuk bekerja optimal, *Port Knocking server* harus mengontrol semua percobaan koneksi yang masuk untuk menganalisa *knock sequence* yang sah

dan membuka *port* untuk klien yang sah dan hal ini harus dilakukan secara *real time.*

Proses analisa ini membutuhkan alokasi memori untuk percobaan koneksi dari setiap klien yang berbeda guna mengidentifikasi *knock sequence*. Jikapenyerangmengirimkanbanyakpaketdengan*random source address*, *portk nocking server* harus mengalokasikan memori untuk setiap *source address* tersebut.

DOS-Knocking terjadi ketika penyerang mengirim paket secara trus-menerus dengan *random fake network address* kepada *server*. Server harus mengalokasikan memori untuk mencatat *log* pengiriman paket untuk setiap *fake network address* tersebut. Hal ini menyebabkan meningkatny apenggunaan memori secara signifikan dan dapat mengakibatkan server *Overload* [13].

Penelitian yang berjudul "*SPKT Secure Port Knock-Tunneling, an enhanced port security authentication mechanism*" menambahkan *text pass parses* pada setiap *knock sequence* untuk mengatasi *DOS-Knocking*. Pada penelitian ini akan menyederhanakan proses *knock sequence* dengan menggunakan *source port* sebagi otorisasinya dan sekaligus untuk mengatasi *DOS-Knocking.*

Pada penelitian juga ini akan menggunakan VPN sebagai *tunneling*. Setelah klien menyelesaikan proses *Port Knocking*, klien tersebut harus melakukan koneksi melalui *tunneling* VPN tersebut, sehingga hanya klien yang sah yang dapat mengakses *server*. Hal ini dapat mengatasi serangan *NAT-Knocking.*

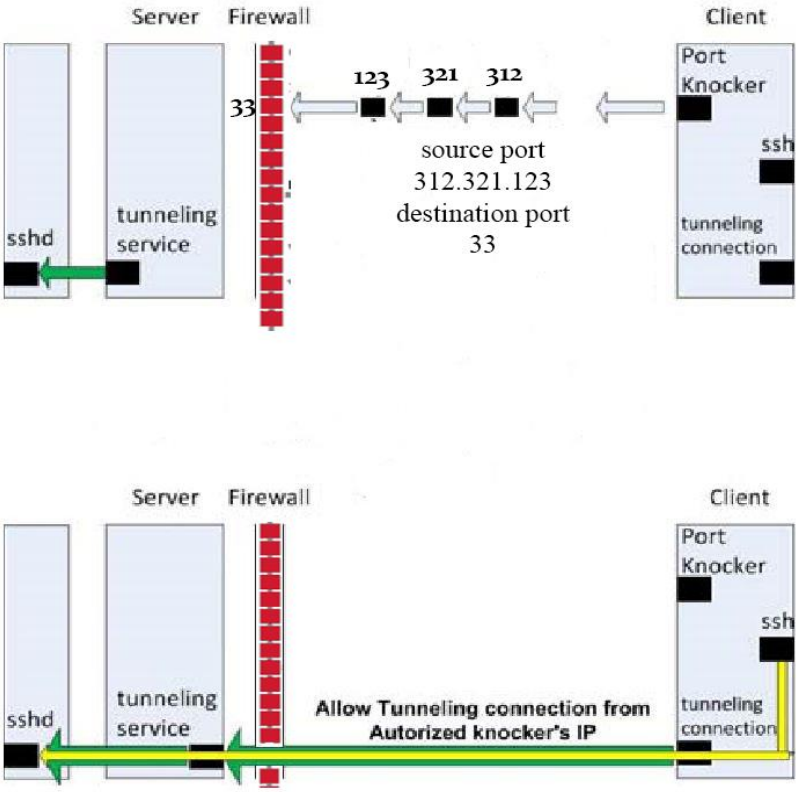
Penelitan ini bertujuan untuk merancang sebuah metode *port knocking* baru yang lebih sederhana menggunakan *source port* dan juga dapat meningkatkan sisi keamanan dari *port knocking* itu sendiri menggunakan *tunneling*.

2. METODE PENELITIAN

Metode *port knocking* pada penelitan ini terdapat dua proses utama untuk mengamankan proses otorisasi klien, yang pertama adalah menyederhanakan *port knocking* dengan menggunakan *source port* dan yang kedua adalah *tunneling* menggunakan VPN

Proses pertama adalah metode *port knockin* menggunakan *source port* yang sudah ditentukan menuju *port server* yang sudah ditentukan juga. Jika *source port* valid dan *destination port* juga valid maka *firewall* akan membuka *port* yang dituju dan *mentrigger* VPN pada koneksi tersebut.

Pada proses *tunneling*, klien harus melakukan koneksi SSH melalui *tunnel* tersebuts ehingga penyerang akan susah melakukan *scanning*, *replay attack* bahkan *NAT-Knocking*.



Gambar 2.1 Port Knocking Tunneling

Sumber :SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism, 2012

Dari gambar di atas terlihat klien melakukan porcobaan koneksi menuju *port* 33 dengan *sourceport* 312, 321,123. Bila *port* yang dituju benar dan *source port* benar maka server akan mengizinkan klien mengakses SSH melalui *tunneling service*, bila tidak paket akan langsung di *drop* sehingga bila penyerang mengirimkan *fake random source paket*, server tidak akan mengalokasikan memori untuk paket tersebut sehingga serangan *DOS-Knocking* dapat diatasi.

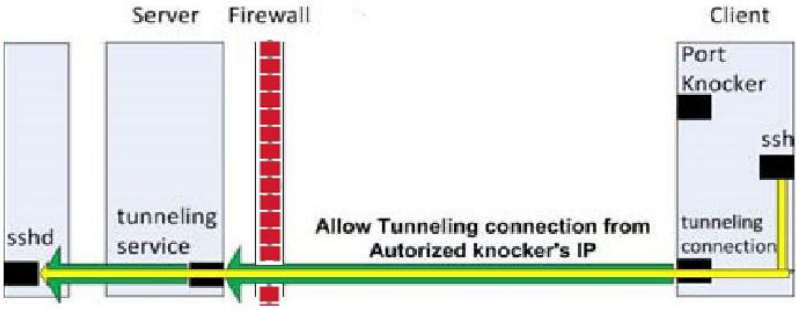
Klien sah yang sudah menyelesaikan proses *Port Knocking*, harus melakukan koneksi SSH melalui *tunneling server*. Klien harus melakukan otentikasi untuk mengakses koneksi VPN, sehingga serangan *NAT-Knocking* dapat diatasi.

Metode pengambilan data pada penelitan ini akan dilakukan dengan cara membandingkan langsung *step* dan waktu yang dibutuhkan untuk menyelesaikan sebuah proses *Port Knocking* antara *Port Knocking* standar dengan *Simple Port Knocking Tunneling*.

Metode pengambilan data selanjutnya adalah denga cara melakukan percobaan serangan *DOS Knocking* dan *NAT Knocking* pada *Simple Port Knocking Tunneling*.

3. HASIL PENELITIAN DAN PEMBAHASAN

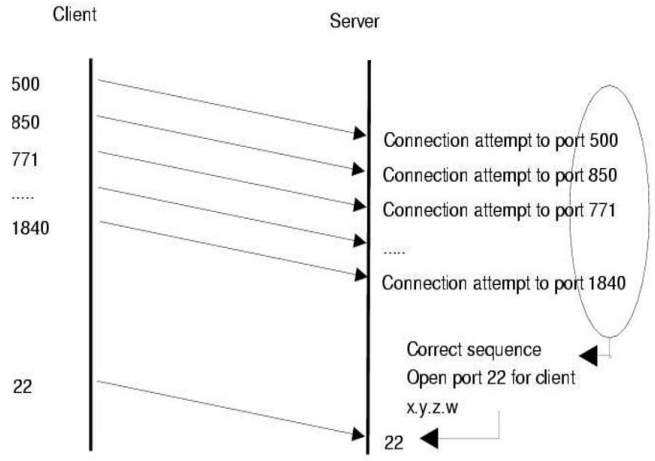
Karena penelitian masih berjalan sehingga data lengkap belum dapat kami paparkan. Harapannya Metode *port knocking* sederhana menggunakan *Tunneling* ini dapat mengatasi serangan *DOS-Knocking* dan *NAT-Knocking* dimana metode *port knocking* standar masih rentan terhadap dua serangan ini.



Gambar 3.1 Port Knocking menggunakan Tunneling
Sumber : SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism, 2012

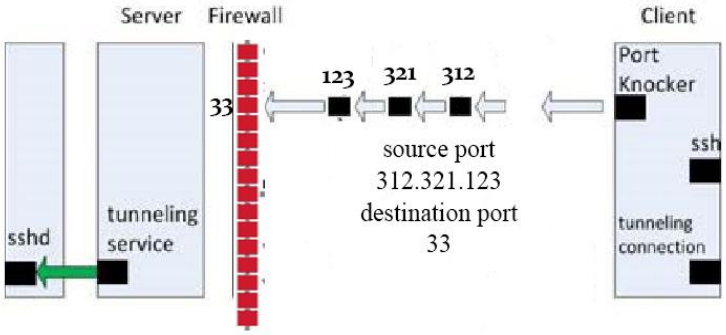
Bila klien telah selesai melakukan *Port Knocking*, klien tersebut harus mengakses *server* melalui *tunneling* eperti gambar diatas. Hal ini mengharuskan klien untuk melakukan otentikasi agar dapat mengakses *tunneling* tersebut, sehingga tidak semua klien dapat mengakses *server* walaupun memiliki *IP Public* yang sama atau berada dalam NAT yang sama.

Selain meningkatkan sisi keamanan, penelitian ini juga diharapkan dapat membuat proses *port knocking* ini menjadi lebih sederhana, membutuhkan alokasi memori yang lebih sedikit dan membutuhkan waktu yang lebih sedikit dalam proses otorisasinya.



Gambar 3.1 Standar Port Knocking

*Sumber :*Simple Port Knocking Method: Against TCP Replay Attack and Port Scanning



Gambar 3.2 Port Knocking dengan Source Port
Sumber : SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism, 2012

Terlihat pada gambar di atas, standar *Port Knocking* membutuhkan lebih dari satu kali proses validasi dengan cara melakukan lebih dari satu kali *knock sequence*. Hal ini akan membutuhkan banyak proses, waktu yang lebih lama dan alokasi memori yang lebih banyak sehingga rentan terhadap serangan *DOS-Knocking*.

Berbeda halnya dengan *Port Knocking* menggunakan *source port*, hanya membutuhkan satu kali validasi, sehingga proses otorisasinya lebih sederhana dengan waktu yang lebih sedikit dan juga alokasi memori yang sedikit sehingga dapat mengatasi *DOS-Knocking.*

4. SIMPULAN

Jaringan computer sangat rentan terhadap serangan terutama ketika mengakses komputer lain dalam jaringan. Karena itu lah dibutuhkun *port knocking* untuk dapat mengurangi resiko serangan tersebut. Akan tetapi*Port knocking* sendiri masih rentan terhadap serangan *DOS-Knocking* dan *NAT-Knocking* dan juga proses otorisasi yang masih rumit.

Penggunaan *source port* dapat menyederhanakan proses otentikasi dan mempersingkat waktunya karna hanya butuh satu kali validasi dimana standar *port knocking* masih menggunakan *knock sequence* yang membutuhkan lebih dari satu kali validasi sehingga membutuhkan proses dan waktu yang lebih lama.

DOS-Knocking dapat diatasi dengan penggunakan *source port*, karena *server* tidak akan mengalokasikan memori untuk percobaan koneksi yang

tidak valid. Setelah menyelesaikan proses *port knocking*, tidak semua klien yang berada pada NAT yang sama dapat mengakses *server*, karena *server* hanya dapat diakses melali *tunneling* VPN, sehingga serangan *NAT-Knocking* dapat diatasi.

5. DAFTAR PUSTAKA

A. I. Manzanares, J. T. Marquez, J. M. Estevez-Tapiador, J. Cesar Hern´andez Castro. (2005) "Attacks on port knocking authentication mechanism,", Computational Science and Its Application, ICCSA 2005, pp. 1292-1300.

Ali, F.H.M. , Yunos, R. , Alias, M.A.M. (2012). " Simple Port Knocking Method: Against TCP Replay Attack and Port Scanning ", Cyber Warfare and Digital Forensic (CyberSec).

Atani, Reza Ebrahimi,.Boroumand, Laleh,.Pourvahab, Mehran., "SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism"IEEE Symposium on Computer & Informatics, 2012

M. Krzywinski, "Port Knocking Implementations," Port Knocking, [Online] 3 Nov 2009, [2009 Dec 14] Available:http://www.portknocking.org/view/implementations

S. Jeanquier. (2006). "An Analysis of Port Knocking and Single Packet Authorization," master's thesis, Information Security Group, Royal Holloway College, Univ. of London.

Srivastava, V. (2011). "Advanced port knocking authentication scheme with QRC using AES" Emerging Trends in Networks and Computer Communications (ETNCC).

Z, A Khan, N. Javaid, M. H. Arshad. (2012). " Performance Evaluation of Widely used Portknocking Algorithms". IEEE 14th International Conference on High Performance Computing and Communications.