Penerapan Stealth Monitoring Keamanan Jaringan Dengan Teknologi Open Source

Muhammad Rifqi Muwaffaq[1)], Irfan Syamsuddin[2)], Muh. Fajri Raharjo[3)]
[1]Teknik Komputer dan Jaringan, Teknik Elektro, Politeknik Negeri Ujung Pandang
muhrifqi3110@gmail.com
[2]Teknik Komputer dan Jaringan, Teknik Elektro, Politeknik Negeri Ujung Pandang
irfans@poliupg.ac.id
[3]Teknik Komputer dan Jaringan, Teknik Elektro, Politeknik Negeri Ujung Pandang
fajri_raharjo@poliupg.ac.id

Abstrak

Berbagai jenis serangan dapat terjadi pada jaringan internet, salah satu jenis ancaman dapat terjadi pada server yaitu serangan yang ditargetkan pada suatu port dalam kondisi terbuka. Terdapat metode yang dapat mengatasi masalah port dalam kondisi terbuka yaitu dengan menggunakan metode port knocking, dengan menggunakan port knocking maka port-port akan terlihat tertutup. Penelitian ini memberikan tingkat keamanan menggunakan model port knocking maka akan meningkatkan kerumitan penyerang dalam mengakses sebuah port yang terdapat pada server. Jika terdapat attacker melakukan serangan port scanning dengan adanya model port knocking pada server menjadi tidak efektif karena tidak dapat mengidentifikasi port yang terbuka.

Keywords: Sistem Keamanan, Firewall, Port Knocking

I. PENDAHULUAN

Terdapat jenis ancaman yang terjadi pada server yaitu serangan yang ditargetkan pada suatu port yang berada dalam kondisi terbuka, sehingga yang tidak memiliki hak akses dapat melakukan port scanning untuk menyusup kedalam server [1] . Portport dalam kondisi yang terbuka terdapat kemungkinan terjadi eksploitasi dari akses yang tidak diinginkan, oleh sebab itu dibutuhkan suatu sistem yang dapat menangkal masalah tersebut [2].

Berbagai cara telah diterapkan misalnya menggunakan firewall sebagai dinding penghalang pembatasan akses. Dalam penggunaan firewall sendiri masih terdapat kekurangan dikarenakan menutup semua akses tanpa memperhatikan siapapun yang sedang terkoneksi dalam jaringan. Suatu metode kemanan yang dapat menutup celah
dan masalah pembatasan hak akses berdasarkan firewall yaitu dengan menggunakan metode port knocking, metode ini dapat digunakan dalam proses mengamankan server (Linux dan Unix) dan melakukan monitoring jaringan melalui pembatasan akses blocking pada port yang terdapat dalam jaringan [3].

Port knocking adalah sebuah metode autentikasi yang dapat diterapkan untuk menyembunyikan service port, serta dapat juga diterapkan untuk membuka akses pada service port tertutup harus menggunakan ketukan port sequence [4]. Pada port knocking terdapat istilah knocking atau disebut autentikasi merupakan usaha untuk membuka port yang dalam kondisi tertutup dengan cara mengakses beberapa port komunikasi ketika beberapa port komunikasi diakses dengan kombinasi tertentu, maka akan terbuka sebuah port [5].

Dari berbagai uraian permasalahan keamanan serta cara penanganannya maka penelitian ini membahas masalah ini dengan mengusulkan kerangka kerja yang akan memberikan tingkat keamanan pada server dengan menerapkan port knocking. Kerangka kerja ini akan meningkatkan kerumitan penyerang dalam membuka sebuah port yang terdapat pada server karena dibutuhkan sebuah autentikasi tambahkan untuk membuka sebuah port.

Penelitian ini bertujuan untuk menerapkan port knocking sebagai teknologi open source [6] untuk melakukan stealth monitoring jaringan

II. KAJIAN LITERATUR

A. Firewall

Firewall didefinisikan sebagai sebuah komponen atau kumpulan komponen yang membatasi akses antara sebuah jaringan yang diproteksi dan internet, atau antara kumpulan-kumpulan jaringan lainnya. Firewall menciptakan solusi yang efektif dalam menanggulangi permasalahan keamanan di dalam lingkungan internet, yang mencakup perlindungan terhadap komputer dan jaringan yang sering kali terpapar oleh beragam jenis ancaman, baik yang berasal dari internal maupun eksternal [7].

B. Port scanning

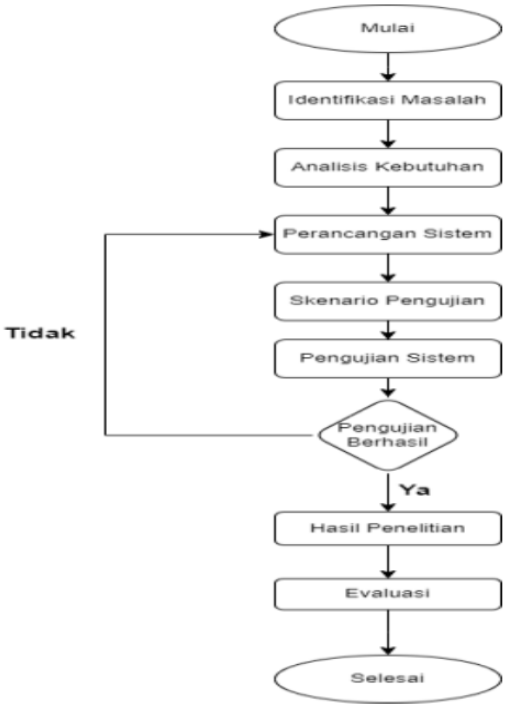
Port scanning merupakan metode yang digunakan untuk mendeteksi sebuah port yang aktif pada suatu computer. Oleh sebab itu serangan port scanning dianggap sebagai ancaman yang berbahaya bagi suatu jaringan, karena dapat mengeksploitasi kerentanan pada server untuk menjalankan tindakan yang merugikan [8].

C. Port Knocking

Metode yang dilakukan oleh port knocking adalah membuka akses ke port tertentu yang telah diblock. Koneksi pada port knocking dapat berupa TCP, UDP, maupun ICMP. Jika host telah mengirimkan koneksi yang telah sesuai dengan rule knocking, maka port yang sudah diblock akan diberikan akses secara dinamis oleh firewall [9]. *Port knocking* adalah teknik di mana serangkaian pengetukan dilakukan terhadap port-port komunikasi dalam sistem data. Pengetukan ini melibatkan kombinasi khusus yang dilakukan secara berurutan dalam interval waktu tertentu. Jika kombinasi pengetukan sesuai dengan yang ditentukan, port komunikasi yang dituju akan terbuka [8].

III. METODE PENELITIAN

Untuk membuat penelitian yang dapat mencakup semua tujuan penelitian dengan hasil yang baik maka perlu diterapkan sebuah prosedur penelitian atau sebuah kerangka kerja. Tahapan prosedur penelitian diperlukan agar penelitian dapat terstruktur sehingga hasil yang diperoleh sesuai dengan tujuan penelitian. Gambar 1 merupakan gambaran alur proses penelitian.



Gambar 1. Alur Prosedur Penelitian

1. Identifikasi Masalah

Pada tahap ini dilakukan identifikasi masalah sehingga dapat menentukan cakupan sistem yang akan dibuat. Permasalahan yang ada adalah keamanan pada suatu server saat melakukan knocking terdapat kemungkinan seseorang melakukan proses penyadapan maka perlu adanya tingkat keamanan tambahan di model port knocking yaitu dengan melakukan proses enkripsi pada sequence port.

2. Analisis Kebutuhan

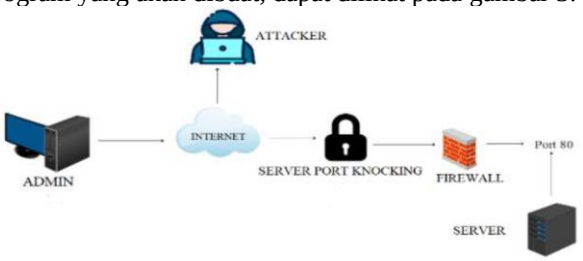
Dalam membangun sistem enkripsi pada port knocking dibutuhkan analisis kebutuhan. Pada tahap ini akan dilakukan analisis terhadap kebutuhan-kebutuhan sistem, kebutuhan perangkat keras (Hardwware) dan perangkat lunak (Software). Analisis ini bertujuan untuk mengetahui sistem seperti apa yang akan diterapkan, serta kebutuhan perangkat keras dan lunak yang sesuai pada pembuatan sistem.

3. Perancangan Sistem

Pada sistem perancangan ini dilakukan perancangan konseptual.

1. Arsitektur Program

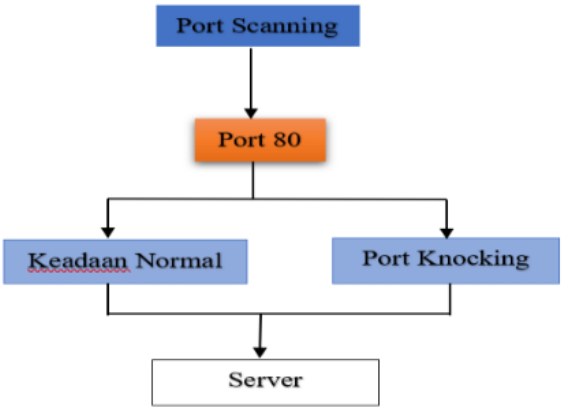
Arsitektur program merupakan penggambaran umum program yang akan dibuat, dapat dilihat pada gambar 3.



Gambar 2. Arsitektur Program

4. Skenario Pengujian

Skenario Pengujian merupakan penggambaran umum pengujian yang akan dibuat dapat dilihat pada gambar 3.



Gambar 3. Skenario Pengujian

5. Pengujian Sistem

Implementasi pada sistem ini akan dilakukan pada server dengan sistem operasi Ubuntu Server kemudian pada server tersebut telah terdapat port knocking untuk membuka dan menutup port pada saat admin melakukan remote server. Kemudian akan terdapat sebuah proses yang berjalan untuk mengenkripsi sequence port sebelum seorang admin melakukan remote terhadap server.

1. Pengujian Tidak Menerapkan Sistem Keamanan

   Tahap pengujian sistem yang akan dilakukan pada penelitian ini yaitu melakukan serangan sniffing dan port scanning dalam keadaan jaringan normal.

Gambar 4. Pengujian Tidak Menerapkan Sistem Keamanan

2. Pengujian Penerapan Port Knocking
   Tahap pengujian sistem yang akan dilakukan pada penelitian ini yaitu melakukan serangan sniffing dan port scanning dalam keadaan jaringan telah menerapkan Port knocking.

Gambar 5. Pengujian Penerapan Port Knocking

6. Hasil Penelitian

Setelah semua tahapan perancangan sistem, implementasi dan pengujian sistem telah selesai dilakukan maka pada tahap ini dilakukan pengambilan kesimpulan berdasarkan rumusan masalah terhadap hasil yang telah dicapai dari seluruh tahapan penelitian

7. Evaluasi

Pada tahap ini dilakukan perbaikan eror yang terjadi pada saat proses pengujian, serta melakukan perbaikan jika hasil belum sesuai dengan kebutuhan.

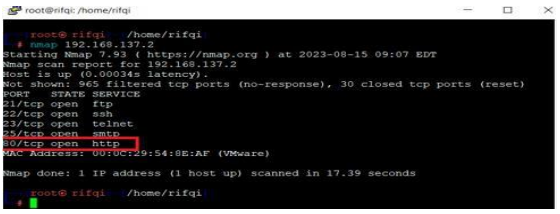
IV. HASIL DAN PEMBAHASAN

A. Pengujian Server Tidak Ada Sistem Keamanan

Melakukan percobaan untuk masuk ke server dengan mengakses port 80 (HTTP). Membuktikan bahwa server dapat dengan mudah diakses oleh orang yang tidak memiliki hak akses.

Gambar 6. HTTP Berhasil Diakses

Pada penelitian ini attacker melakukan peyadapan dengan menggunakan serangan *port scanning*.



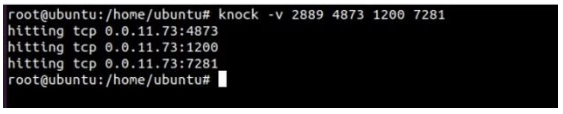
Gambar 7. Penyerangan *Port scanning*

Terlihat pada Gambar 8 bahwa *port* 80 (HTTP) pada *server* dalam keadaan terbuka sehingga *attacker* dapat mengetahui jika *admin* jaringan melakukan *remote server* pada bahwa *port* 80 (HTTP).

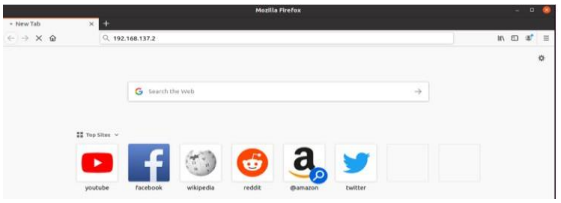
B. Pengujian Server Menerapkan Port Knocking

Metode *port knocking* dapat digunakan untuk menjaga semua *port* yang ditutup sampai pengguna melakukan autentikasi dengan *knock port.*

Admin melakukan percobaan untuk masuk ke *server* dengan mengakses *port* 80 (HTTP) menggunakan ketukan yang salah. Membuktikan bahwa *server* tidak dapat diakses menggunakan *port* 80 (HTTP) jika ketukan tidak sesuai sesuai dengan konfigurasi yang dilakukan di *server*.

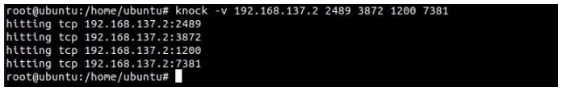


Gambar 8. Membuka HTTP Ketukan Salah



Gambar 9. HTTP Tidak Dapat Diakses

Admin melakukan percobaan untuk masuk ke *server* dengan mengakses *port* 80 (HTTP) menggunakan ketukan yang benar. Membuktikan bahwa *server* dapat diakses menggunakan *port* 80 (HTTP) jika ketukan yang sesuai dengan konfigurasi yang dilakukan di *server*.



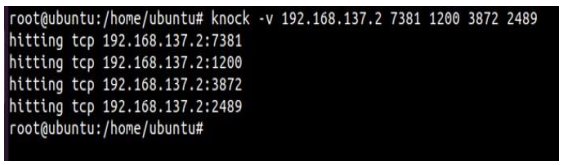
Gambar 10. Membuka HTTP Ketukan Benar

Gambar 11. HTTP Berhasil Diakses

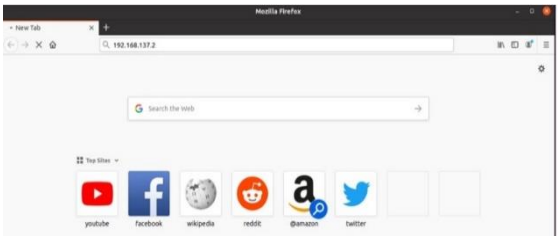
Admin melakukan percobaan untuk menutup *server* pad *port* 80 (HTTP) menggunakan ketukan yang salah maka *port* 80 (HTTP) masih dapat diakses.

Gambar 13. HTTP Masih Dapat Diakses

Admin melakukan percobaan untuk menutup *server* pad *port* 80 (HTTP) menggunakan ketukan diakses.



Gambar 14. Menutup HTTP Ketukan Benar



Gambar 15. HTTP Tidak Dapat DIakses

Pada penelitian ini attacker melakukan peyadapan dengan menggunakan serangan *port scanning*.

Gambar 16 Penyerangan *Port scanning*

Terlihat pada Gambar 12 bahwa setelah *server* menggunakan teknik *port knocking* menjadikan *port port* 80 (HTTP) dalam keadaan tertutup sehingga attacker tidak dapat mengetahui jika admin jaringan melakukan remote *server* pada *port* 80 (HTTP).

C. Tabel Pengujian Server

Tabel 1. Pengujian *Server*

Sistem Keamanan	**Tidak Ada Serangan**	***Port ScanningAttack***
Server Tidak Ada Keamnan	*Port* terbuka	*Attacker* **mendapatkan** informasi *port* kondisi terbuka
Server Port	*Port* Tertutup	*Attacker* **tidak mendapatkan** informasi *port* kondisi terbuka

V. KESIMPULAN

Berdasarkan implementasi dan pengujian yang dilakukan untuk maka dapat di simpulkan bahwa penerapan teknik *port knocking* meningkatkan keamanan *server* dengan mencegah akses yang tidak sah. Untuk mengakses *server* secara remote, maka harus mengetahui *sequence port* yang diaktifkan pada *server*. Serangan *port* scanning menjadi tidak efektif karena tidak dapat mengidentifikasi *port* yang terbuka.

UCAPAN TERIMAKASIH

Terimakasih kepada Tuhan Yang Maha Esa, orang Tua, kedua pembimbing, seluruh dosen, dan staf Teknik Elektro Porgram Studi Teknik Komputer dan Jaringan Politeknik Negeri Ujung Pandang.

REFERENSI

[1] A. S. S. Suhendar, H. Sajati, and Y. Astuti, "Perancangan Algoritma Anggi (Aa) Dengan Memanfaatkan Diffie-Hellman Dan Ronald Rivest (Rc4) Untuk Membangun Sistem Keamanan Berbasis *Port Knocking*," *Compiler*, vol. 2, no. 2, pp. 59–66, 2013, doi: 10.28989/compiler.v2i2.47.

[2] M. Iqbal, Arini, and H. Bayu Suseno, "Analysis and Simulation of Ubuntu *Server* Network Security Using *Port Knocking* , Honeypot , Iptables , Icmp," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 27–32, 2020.

[3] A. S. Andreatos, "Hiding the SSH *port* via smart *Port Knocking*," vol. 11, pp. 28–31,2017, [Online]. Available: ttps://www.researchgate.net/publication/315896859

[4] S. J. I. I. Devie Ryana Suchendra1, Alfian Fitra Rahman2, "Penerapan sistem pengamanan *port* pada layanan jaringan menggunakan *port knocking*," *J. Lpkia*, vol. 10, no. 2, pp. 45–50, 2017.

[5] S. B. U. Amrie, E. Tungadi, and I. Syamsuddin, "Teknologi Open Source Untuk Lomba Keamanan Jaringan Berbasis CTF," *Semin. Nas. Tek. …*, no. September, pp. 215–218, 2021, [Online].

Available: http://118.98.121.208/index.php/sntei/article/view/2890%0Ahttp://118.98.121.208/index.php/sntei/article/download/2890/2519

[6] M. V. a N. Basten, "Tugas jurnal jaringan komputer optimalisasi firewall pada jaringan skala luas," 2009.

[7] V. J. E. and D. M. W. P. Rodney R *Secur. Big Data, ISI 2017*, pp. 185–187, 2017, doi:10.1109/ISI.2017.8004906.

[8] B. H. Dimas Perdana , Jayanta, "Sistem deteksi keamanan jaringan pada *server* dapodik di smpn i muara kelingi terhadap serangan *sniffing*," pp. 57–65, 2023, doi: 10.31284/j.JREEC.2023.v31i.

[9] A. Saputro, N. Saputro, H. Wijayanto, and P. S. Informatika, "METODE DEMILITARIZED ZONE DAN *PORT KNOCKING* UNTUK DEMILITARIZED ZONE AND *PORT KNOCKING* METHODS FOR COMPUTER," vol. 3, no. 2, pp. 22–27, 2020.