JIMP - Jurnal Informatika Merdeka Pasuruan
Vol 3 No1 Maret 2018
ISSN 2503-1945

PORT KNOCKING DAN HONEYPOT SEBAGAI KEAMANAN JARINGAN PADA SERVER UBUNTU VIRTUAL

Wilman[1], Iskandar Fitri[2], Novi Dian Nathasia[3]
[1,2,3] Jurusan Teknik Informatika, Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional 2017
e-mail: [1]**Wilman313@gmail.com**, [2] tektel2001@yahoo.com,
[3]novidian@civitas.unas.ac.id

Abstrak

Sistem keamanan terhadap akses data harus ditingkatkan seiring dengan perkembangan teknologi dan organisasi maka organisasi tersebut harus semakin waspada terhadap orang-orang yang tidak bertanggung jawab dan tidak memiliki hak akses tentang data rahasia perusahaan yang ada pada server. Server merupakan suatu wadah utama untuk data – data penting suatu organisasi. Server Virtual dengan OS Linux sangat disarankan bagi pemula, karena mudah untuk dipelajari karena server bersifat krusial, maka server perlu diberikan suatu keamanan untuk melindungi data - data atau memblokir jalan dari intruder (penyusup) menuju server dengan cara member lebih dari satu metode keamanan yang berbeda untuk mengelabuhi intruder. Keamanan jaringan port knocking merupakan metode untuk menutup dan membuka port tertentu yang diamankan oleh administrator dengan menggunakan beberapa key atau kode untuk dapat membuka dan menutup port. Metode yang kedua suatu keamanan jaringan dapat dengan menggunakan honeypot. Dimana honeypot merupakan server tipuan untuk intruder agar dia seolah – olah berhasil masuk ke dalam server sungguhan. Dalam pengetesan kedua metode keamanan jaringan tersebut menggunakan putty dan mobaxtrem Mengkombinasikan kedua metode firewall yaitu port knocking dan honeypot.

Kata kunci *— linux ubuntu, port knocking, honeypot*

Abstract

System security against data access should be improved along with the development of technology and organization of the Organization must then increasingly wary of people who are not responsible and do not have the right of access of confidential data companies that exists on the server. Server is a container for important data of an organization. The Virtual Server with the Linux OS is highly recommended for beginners, because it is easy to learn because the crucial nature of the server, then the server will need to be given a security to protect data or block the way from the intruder (intruder) to server by giving more than one different security methods to confuse intruder. Network security of port knocking is a method for closing and opening certain ports which are secured by the administrator by using some key or code to be able to open and close ports. The second method is a network security can use honeypot. Where is a honeypot server trickery to intruder that he seems though managed to get into a real server. In the second method of testing the network security using putty and mobaxtremcombines both methods i.e. firewall port knocking and honeypot.

Keywords— *linux ubuntu, port knocking, honeypot*

1. PENDAHULUAN

Perkembangan Teknolologi jaringan terutama system keamanan jaringan yang semakin berkembang menuntut agar system keamanan untuk berkembang, terutama pada keamanan *server* yang merupakan salah satu tugas pokok dari system administrator. Hal ini didasarkan pada karakteristik umum dari jaringan komputer yang pada dasarnya adalah tidak aman untuk diakses secara bebas. Terbukanya *port* untuk layanan yang bersifat public maupun bersifat *privat*, memiliki kemungkinan resiko yang tinggi untuk diserang oleh para *attacker*. Untuk mengatasi hal tersebut maka dibutuhkan sebuah keamanan yang dapat menjaga jaringan *server* dari *attacker*.

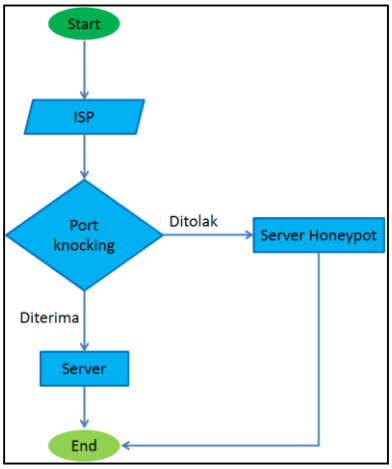
Sebelum adanya metode *port knocking* dan *honeypot* keamanan *server* hanya menggunakan *firewall*, akan tetapi untuk saat ini *firewall* masih banyak kelemahan. Untuk mengatasinya maka dibutuhkan pengembangan dari *firewall* yaitu dengan mengimplementasikan *port knocking* dan *honeypot* pada jaringan *server*. Dimana *port knocking* dapat mengontrol layanan *port* terbuka dan *port* tertutup[1]. Selain menggunakan metode *port knocking* dibutuhkan

honeypot untuk mengalihkan *attacker* kedalam *server* tiruan dan mendeteksi serangan apa saja yang dilakukan oleh *attacker/intruder* pada *server*[2]. Pada penelitian sebelumnya *port knocking* belum dikombinasikan dengan *honeypot*, *port knocking* hanya digunakan untuk menyembunyikan *port*, dan dapat berjalan dengan baik pada Virtual Debian Versi 6.0.1[3].

Pada penelitian lainnya *honeypot* digunakan untuk keamanan jaringan *wireless*[4]. *Honeypot* mampu untuk memberikan data informasi palsu terhadap *attacker*, seolah – olah *server* utama yang berhasil disusupi oleh *attacker*, padahal penyerang tidak masuk ke *server* sebenarnya, tetapi masuk ke sistem yang palsu.[5].

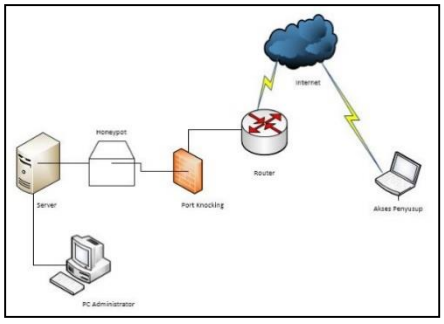
2. METODE DAN ANALISIS PERANCANGAN

Dalam penelitian ini dirancang untuk mengimplementasikan port knocking dan honeypot untuk keamanan sebuah server. Seperti dikatakan pada bab sebelumnya bahwa pada dasarnya port knocking dapat didefinisikan sebagai suatu metode komunikasi antara dua computer, sedangkan honeypot sebagai pengalihan penyusup seolah – olah sudah masuk ke sever utama. Flowchart proses Perancangan Implementasi Port Konocking dan Honeypot. Sebagai keamanan Jaringan pada server Ubuntu Virtual.



Gambar 1. *Flowchart* Implementasi *Port Konocking* dan *Honeypot*. Sebagai keamanan Jaringan pada *server* Ubuntu *Virtual*.

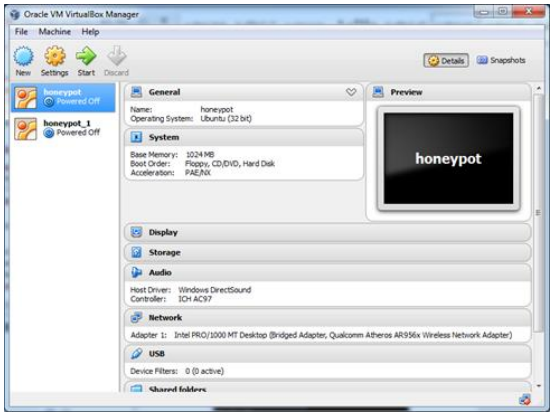
Flowchart ini sebagai gambaran untuk member penjelasan proses berjalannya Implementasi Port Konocking dan Honeypot Sebagai keamanan Jaringan pada server Ubuntu *Virtual*. Dari *Flowchart* Menjelaskan pada tahap awal intruder masuk kemudian mencoba untuk menyusup ke server, yang kemudian dialihkan ke *server* palsu. Dengan adanya *honeypot* dan *port knocking* yang dapat difungsikan atau tidak oleh administrator.



Gambar 2. Topologi *Honeypot* dan *Port Knocking*

Pada gambar 2. Diatas merupakan rancangan dari *implementasi Port Konocking* dan *Honeypot*, Sebagai keamanan Jaringan pada *server Ubuntu Virtual*, dari perancangan tersebut *intruder* tidak bias mengakses ke *server*. Pada implementasi ini perangkat yang digunakan untuk penilitian Laptop dengan spesifikasi *Processor Intel*® Core™ i3-4030U CPU @ 1.90 GHz dengan RAM

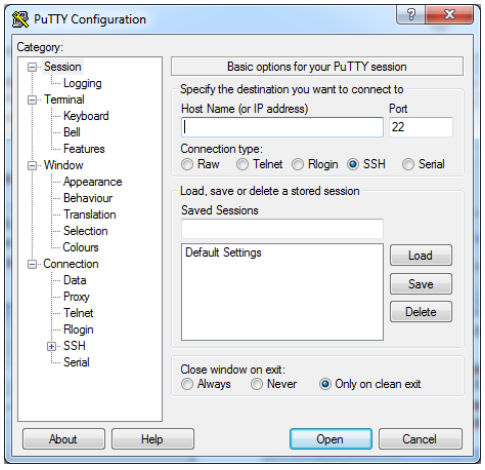
4GB sedang untuk operasi *system* yang digunakan ada Ubuntu *Server* pada *VM VirtualBox*. Beberapa tools dan utility yang digunakan untuk konfigurasi dalam Implementasi *Port Konocking* dan *Honeypot*. Sebagai keamanan Jaringan pada server Ubuntu *Virtual*, *tools* yang digunkan pada penelitian ini mengunakan *virtual* dari Oracle *VM Virtualbox*.



Gambar 3. Tampilan utama *Oracle VM Virtualbox*.

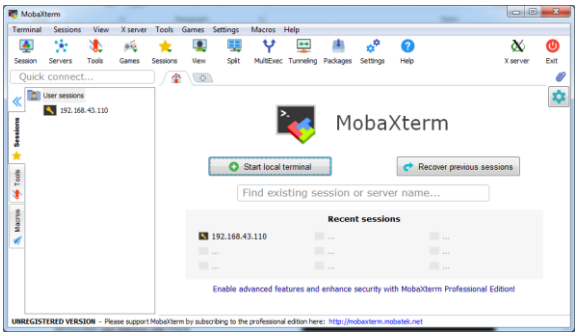
Virtualbox termasuk suatu alat perangkat lunak secara Virtualisasi,yang dapat megoprasikan/menginstal beberapa *System* operasi pada *system* utama. Fungsi ini sangat penting bagi seseorang yang ingin melakukan pengujian dan melakukan simulasi suatu *system* tanpa harus menghapus *system* yang ada. Aplikasi dengan fungsi yang sama adalah *VM Ware* dari perusahaan *VM Ware Inc.*

Selain menggunakan aplikasi Virtualbox penulis juga menggunakan beberapa aplikasi untuk melakukan pengujian dari hasil implementasi keamanan *Server* dengan mengkobinasikan *Port Knocking* dan *Honeypot*, aplikasi yang digunakan adalah Putty dan Mobaxtreme.



Gambar 4. Tampilan Utama Putty

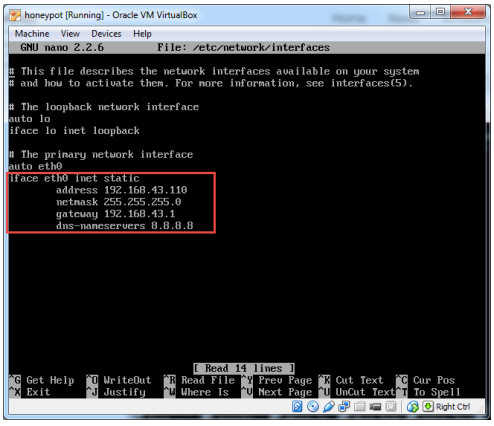
Putty adalah aplikasi yang bersifat open source yang dapat digunakan untuk melakukan protocol jaringan SSH,Telnet dan Rlogin. Aplikasi lain yang digunakan untuk pengujian dari hasil penulisan yaitu Mobaxtrem.



Gambar 5. Tampilan Utama MobaXtrerm.

2.1 Konfigurasi Ip Address pada Server Ubuntu

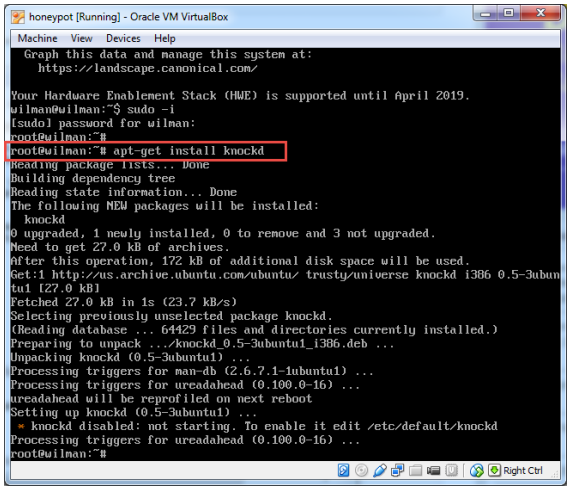
Pada penelitian ini penulis menggunakan konfigurasi internet *static*. Dan langkah untuk konfigurasi *IP Address* yaitu dengan mengedit file interfaces yang lokasinya ada pada "*etc/network/interfaces*" untuk mengedit file tersebut ketikan perintah nano. *etc/network/interfaces.*



Gambar 6. Tampilan Konfigurasi *IP Address*.

2.2 Konfigurasi *Port knocking* pada*Server* Ubuntu.

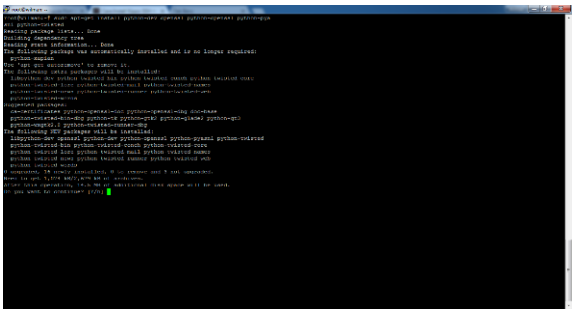
Untuk konfigurasi port knocking penulis menggunakan program *knocd* dari *Slackbuilds.org.*dan untuk install *knocd* ketikan perintah *apt-get install knocd.*



Gambar 7. Tampilan Knocd sudah terinstall

2.3 Konfigurasi *Honeypot* pada *Server Ubuntu.*

Untuk Konfigurasi *Honeypot* ketikan perintah *apt-get install python-dev openssl python-openssl python-pyasn1 python-wisted.*



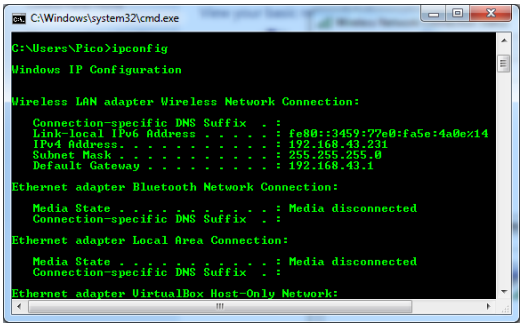
Gambar 8. Tampilan Honeypot

3. HASIL DAN PEMBAHASAN

Dalam penulisan ini dirancang untuk mengimplementasikan keamanan *server* dengan menggunakan metode *Port knocking* dan *Honeypot*. *Port knocking* dapat didefinisikan sebagai suatu komunikasi antara dua komputer, sedangkan *honeypot* sebagai pengalihan agar intruder (penyusup) masuk ke *server* tiruan, dengan *honeypot* bias melihat *log*/aktivitas yang dikerjakan oleh *intruder* terhadap *server*. Pada implementasi ini dilakukan dengan installasi *server* pada *VM Virtualbox*. Dan untuk tahap pengujian penulis menggunakan dua aplikasi yaitu *Putty* dan *MobaXtreem*.

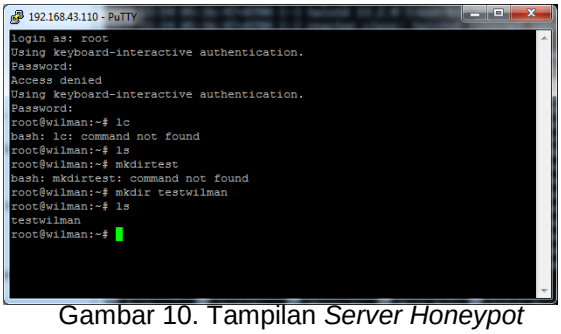
3.1 Pengujian Keamanan Server

Pada pengujian pertama dengan menggunakan aplikasi *putty* didapati instruder berhasil dialihkan ke *server* banyangan. Pada pengujian ini *intruder*/penyusup mencoba meremot dengan menggunakan *port* 22,8000, dan 9000 dengan menggunakan *IP Address* 192.168.43.231.



Gambar 9. Tampilan *IP Address* pengujian pertama

Pada pengujian ini *intruder*/penyusup berhasil dialihkan ke *server* banyangan atau server honeypot. Pada *server honeypot* ini *intruder*/penyusup mencoba *log in* dengan *user root* dan seolah – olah penyusup berhasil masuk ke *server* utama.

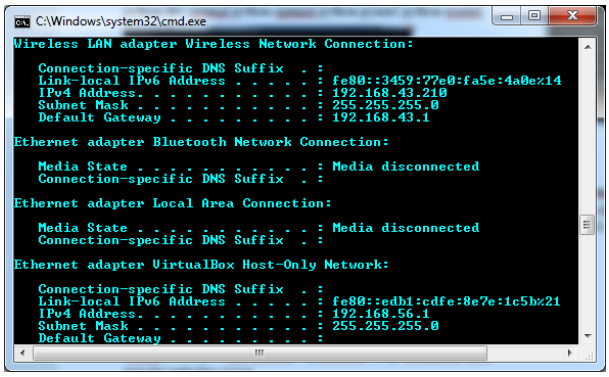


Gambar 10. Tampilan *Server Honeypot*

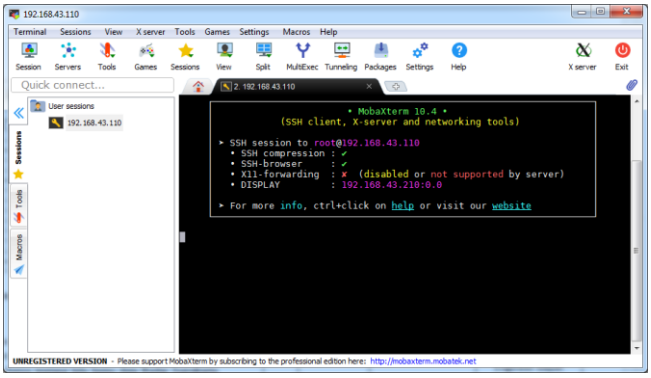
Gambar 10. Menunjukan bahwa *intruder*/penyusup membuat folder pada *server honeypot.*

3.2 Pengujian Kedua

Pada pengujian kedua menggunakan aplikasi MobaXtreme, pada pengujian ini intruder mencoba masukke server dengan *IP Address* 192.168.43.210.



Gambar 11. Tampilan *IP Address* pengujian kedua



Gambar 12. Tampilan *Server Honeypot* pada Aplikasi *MobaXtreme*

Pada pengujian yang kedua intruder/penyusup berhasil dialihkan ke server *honeypot.* Dari hasil pengujian diatas,maka dapat ditarik tabel 1

Tabel 1. Tabel Perbandingan

Aplikasi	IP Address	Port	Keterangan	
			Gagal	Berhasil
Putty	192.168.43.231	9000.8000.22	-	√
MobaXtreme	192.168.43.210	9000.8000.22	-	√

Pada tabel 1 menjelaskan dari hasil pengujian dengan dua aplikasi didapati hasil sesuai dengan harapan, penyusup berhasil dialihkan ke server bayangan dengan metode *honeypot*.

4. KESIMPULAN & SARAN

4.1 Kesimpulan

Berdasarkan hasil implementasi *Port Knocking* dengan *Fitur Limit per-IP connection Rate* dan *honeypot* sebagai keamanan jaringan pada *Server* Ubuntu Virtual mampu mengamankan *server* dengan cara mengalihkan penyusup dan seolah – olah penyusup sudah masuk ke *server* utama, selain itu dengan adanya *honeypot* bias memonitoring yang dilakukan penyusup selama berada di server banyangan dan bias dijadikan sebagai acuan untuk memperkuat system keamanan.

4.2 Saran

Sebaiknya kita tetap terus monitoring untuk monitoring intruder dan terus mempelajari semua metode yang terupdate baik dari segi firewall maupun segi penyusup.

DAFTAR PUSTAKA

[1] Fakariah Hani Mohd Ali, Rozita Yunos, Mohd Azuan Mohamad Alias, *"Simple Port Knocking Method"*, IEEE Software, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA 2013.

[2] Luigi Catuogno, Aniello Castiglione, Francesco Palmieri, *"A Honeypot System with Honeyword-driven Fake Interactive Sessions"*, IEEE Software, Department of Computer Science, University of Salerno 2015.

[3] Mariam Khader, Ali Hadi, Amjad Hudaib, *"Covert Communication Using Port Knocking"*, IEEE Software, Computer Science, Princess Sumaya University of Technology Amman, Jordan, 2016.

[4] Hibatul Wafi, Andrew Fiade, Nashrul Hakiem, Rizal Broer Bahaweres, *"Honeypot Honey Network on Wireless Networks"*, IEEE Software, Deptartment of Informatics, Faculty of Science and Technology, UIN Syarif Hidayatullah Jakarta, Indonesia, 2017.

[5] Muh Masruri Mustofa, Eko Aribowo, *"Penerapan Sistem Keamanan Honeypot Dan IDS Pada Jaringan Nirkabel (HOTSPOT)"*, Universitas Ahmad Dahlan, 2013.