PJSE: PERWIRA JOURNAL OF SCIENCE & ENGINEERING
E-ISSN: 2775-8486
Volume 02 No 01 (2022)

IMPLEMENTASI LOW INTERACTION HONEYPOT DAN PORT KNOCKING UNTUK MENINGKATKAN KEAMANAN JARINGAN

Riyan Dwi Yulian Prakoso[1],
[1,] Program Bisnis Digital , Institut Teknologi Bisnis Muhamadiyah Purbalingga.
Jl. Letjen S Parman No.95, Bancar, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah, Indonesia

Email: riyandwwi@itbmp.ac.id

Abstrak

Seiring dengan pesatnya perkembangan teknologi tentu akan berdampak pada segala aspek kehidupan, walaupun memberikan dampak yang positif dalam menyediakan dan mendapatkan informasi, namun disisi negatifnya perlu adanya upaya untuk pencegahan ancaman, pencurian data dan perusakan data pada sebuah jaringan. Salah satu cara dengan mengimplementasikan Port Knocking dan HoneyPot pada jaringan server. Suatu metode kemanan yang dapat menutup celah dan dan mengalihkan akses dari firewall. Dimana Port Knocking dapat mengontrol layanan port terbuka dan port tertutup. HoneyPot untuk mengalihkan attacker kedalam server tiruan dan mendeteksi serangan apa sajayang dilakukan oleh attacker/intruder pada server. Dalam pengetesan penggabungan kedua metode keamanan jaringan tersebut menggunakan Nmap,

Kata Kunci : Keamanan Jaringan, HoneyPot, Port Knocking,

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi tentu akan berdampak pada segala aspek kehidupan, walaupun memberikan dampak yang positif dalam menyediakan dan mendapatkan informasi, namun disisi negatifnya perlu adanya upaya untuk pencegahan. Ada faktor dimana kita tidak menyadari akan adanya ancaman, pencurian data dan perusakan data pada sebuah jaringan.. Di dalam upaya perlindungan data dalam jaringan komputer memiliki beberapa cakupan penting yang menjadi penting untuk dimiliki oleh perusahaan. Aspek pertama adalah pengamanan secara fisik. Pengamanan secara fisik ini termasuk ke dalam salah satu aspek palling sederhana yang bisa dilakukan oleh perusahaan agar komputer yang dimilikinya tidak diakses oleh orang lain. Minimal dengan menampatkan komputer perusahaan di sebuah tempat yang memiliki sistem keamanan yang tinggi. Banyak cara sudah diterapkan seperti menggunakan firewall sebagai dinding penghalang pembatasan akses. Penggunaan firewall sendiri masih kurang efektif dikarenakan menutup semua akses tanpa memperdulikan siapapun yang sedang terkoneksi dalam jaringan

Untuk mencegah kejadian tersebut di butuhkan sebuah sistem keamanan untuk menjaga server dari attacker. Salah satu cara mengatasinya dengan mengimplementasikan Port Knocking dan HoneyPot pada jaringan server. metode ini digunakan dalam membantu mengamankan server (Linux dan Unix) dan monitoring jaringan melalui pembatasan dan pengalihan akses blocking pada port pada server yang terdapat dalam jaringan

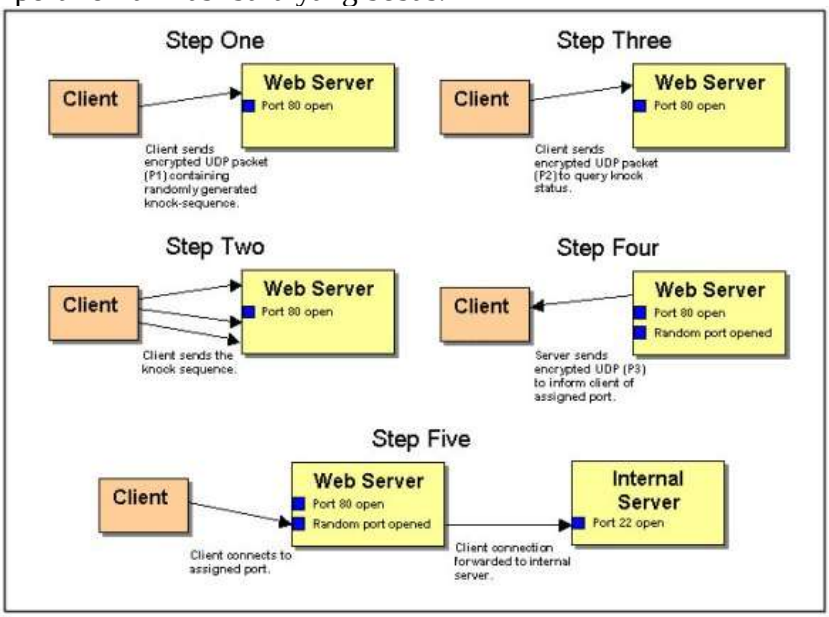
Dimana Port Knocking dapat mengontrol layanan port terbuka dan port tertutup [1] . Selain menggunakan metode Port Knocking dibutuhkan HoneyPot untuk mengalihkan attacker kedalam server tiruan dan mendeteksi serangan apa sajayang dilakukan oleh attacker/intruder pada server [2]. Pada penelitian sebelumnya Port Knocking belum dikombinasikan dengan HoneyPot dan jenis HoneyPot yang di gunakan adalah honeyd. Port Knocking hanya digunakan untuk menyembunyikan port, dan dapat berjalan dengan baik pada Virtual Ubuntu 12.4

2. TINJAUAN PUSTAKAN

2.1 Port Knocking

Metode Port Knocking digunakan untuk dapat akses secara remote dengan tidak mengijinkan port dalam kondisi terbuka sehingga dapat melindungi server dari port scanning dan serangan scripts kiddies. Dengan user diberikan akses untuk mengakses port dan diakhiri dengan menutup port agar firewall menghapus rule yang ditulis sebelumnya untuk membuka port [3]

Kunci dari sistem port knocking adalah port- port komunikasi itu sendiri. Cara membuka kuncinya adalah dengan mengakses dengan sengaja beberapa port komunikasi yang memang tertutup. Ketika beberapa port komunikasi tadi diakses dengan kombinasi tertentu, maka akan terbuka sebuah port komunikasi baru yang bebas.

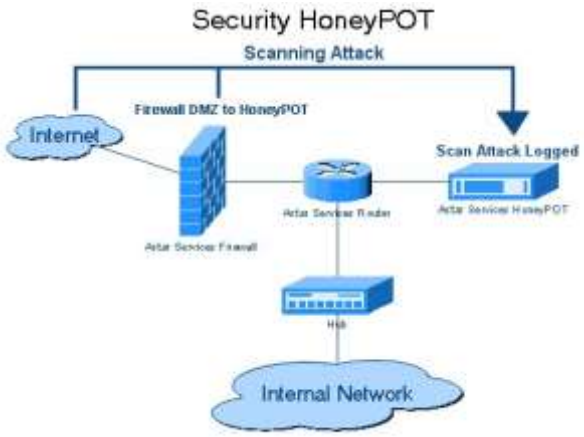


Gambar 1 Porses Kerja Port Knocking

2.2 HoneyPot

Honeypot adalah sistem yang terhubung dengan jaringan yang ditetapkan sebagai umpan untuk memikat penjahat cyber dan untuk mendeteksi, membelokkan atau mempelajari upaya peretasan untuk mendapatkan akses tidak sah ke sistem informasi. Fungsi honeypot adalah untuk mewakili dirinya di internet sebagai target potensial bagi penyerang. HoneyPot memberi kontribusi terhadap keamanan namun tidak secara langsung mencegah serangan dan dapat mengurangi intensitas serangan penyusup ke server. HoneyPot menurut tingkat interaksi (aktivitas penyerangan) dapat dikategorikan menjadi [4] :

1. Low Interaction HoneyPot Didesain untuk mengemulasikan service (layanan) layaknya ke server yang asli, namun penyerang hanya mampu terkoneksi dan memeriksa satu atau beberapa port.
2. Medium Interaction HoneyPot Penyerang dapat menyisipkan worm akan digunakan untk melakukan data analissi yang tertera pada payload worm dari penyerang.
3. High Interaction HoneyPot Metode ini penyerang dapat berinteraksi langsung dan tidak ada batasan sehingga jika sudah dapat mengakses root maka akan dapat berinteraksi secara penuh.



Gambar 2 Cara Kerja Honeypot

Sebelum penyerang masuk ke dalam sistem utama maka dia akan masuk terlebih dahulu ke sistem honeypot. Kemudian sistem ini akan mencatat apapun jejak yang ditinggalkan oleh penyerang.

Jenis HoneyPot yang di gunakan adalah Honeyd. HoneyD adalah program komputer open source yang dibuat oleh Niels Provos yang memungkinkan pengguna untuk mengatur dan menjalankan beberapa host virtual di jaringan Komputer, Dan bersifat Low Interaction

Kelebihan dari Low Interaction Honey poy :

1. Mudah di install, dikonfigurasi, deployed, dan dimaintain
2. Mampu mengemulasi suatu layanan seperti http, ftp, telnet, dsb.
3. Difungsikan untuk deteksi serangan, khususnya pada proses scanning atau percobaan.

Kekurangan dari Low Interaction Honeypot :

1. Layanan yang di berikan hanya berupa emulasi, sehingga penyerang tidak dapat berinteraksi secara penuh dengan layanan yang diberikan atau sistem operasinya secara langsung
2. Informasi yang bisa kita dapatkan dari penyerang sangat minim.
3. Apabila serangan dilakukan oleh "real person" bukan "automated tools" mungkin akan segera menyadari bahwa yang sedang dihadapi merupakan mesin honeypot, karena keterbatasan layanan yang bisa diakses.

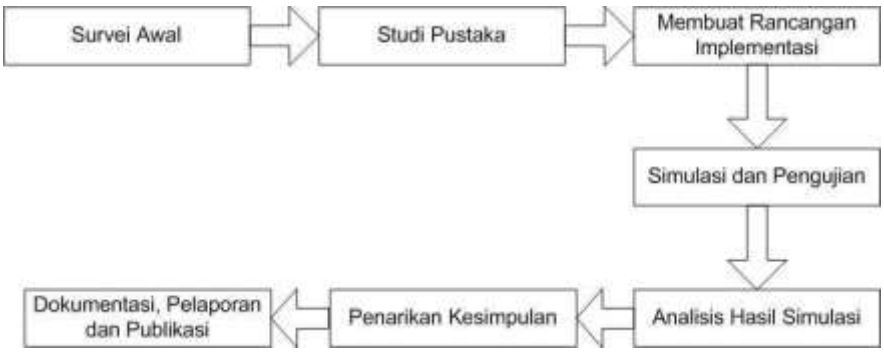
3. METODE

3.1 Metode Penelitian

Pendekatan pada penelitian ini adalah melalui pendekatan kualitatif, dengan mengumpulkan data bukan dalam nilai angka-angka, namun data yang didapatkan melalui pencatatan di lapangan atau laporan resmi lainnya. Metode kualitatif adalah metode yang menentukan peneliti untuk melakukan pengumpulan data yang bersifat gabungan, hasil penelitian kualitatif ini lebih mengarah pada generalisasi

3.2 Tahapan Penelitian

Penelitian ini terdiri dari beberapa tahap yaitu studi pustaka dan literature,
Analisis Data, Metode dan Pemodelan Desain, Implementasi, Pengujian, kesimpulan dan publikasi.



Gambar 3 Tahapan Penelitian

3.2 Pengumpulan Data

1. Data Publik

Metode ini dimaksudkan untuk mendapatkan data publik yaitu data konfigurasi Honeypot dan Port Knocking pada Ubuntu

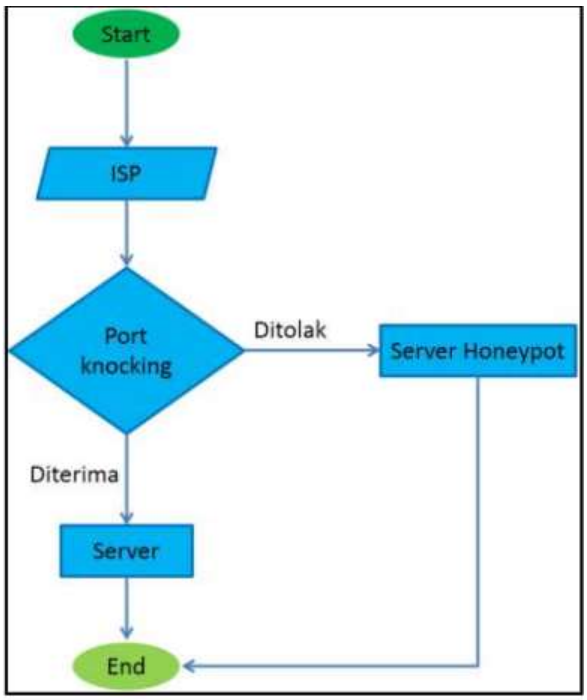
2. Sudi Pustaka

Melakukan penelurusan melalui dokumen-dokumen yang berhubungan baik dalam bentuk media cetak ataupun elektronik sebagai acuan dalam melakukan penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Perancangan System

Dalam penelitian ini dirancang untuk mengimplementasikan Port Knocking dan HoneyPot untuk keamanan sebuah server



Gambar 1 Flowchat implementasi Port Knocking dan HoneyPot

Pada implementasi ini perangkat yang digunakan untuk penilitian Laptop dengan spesifikasi Processor Intel core 15-4210U CPU @ 2.7 GHz dengan RAM 8 GB. 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 2 Tampilan Virtual Box

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 Nmap

Gambar 3 Tampilan Namp

Namp adalah aplikasi yang bersifat open source yang dapat digunakan untuk melakukan protocol jaringan SSH,Telnet dan Rlogin.

Langkah pertama install beberapa program di ubuntu server dengan perintah apt-get install python-dev openssl pythonopenssl python-pyasn1 python-wisted

```
root@honeyd-VirtualBox:~# apt-get install python-dev openssl py
thon-openssl python-pyasn1 python-twisted
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-pyasn1 is already the newest version.
python-twisted is already the newest version.
openssl is already the newest version.
python-dev is already the newest version.
python-openssl is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 325 not upgraded
.
root@honeyd-VirtualBox:~#
```

Gambar 4 Tampilan instalasi Program pendukung HoneyPot

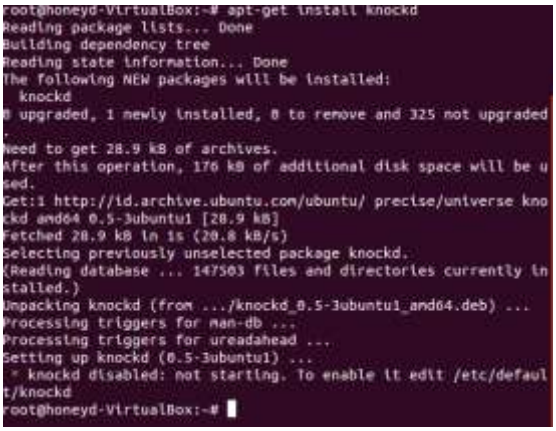
Langkah selanjutnya install honeyd denagn perintan apt-get install honeyd

Gambar 5 tampilan instalasi Honey Pot

Tahap terakhir lakukan konfigurasi pada honeyd.cong dengan perintah gedit honeyd.conf

Gambar 6 konfigurasi Honeyd

Selanjutnya untuk meinstall Port Knocking lakukan isntalasi dengan menggunakan perintah apt-get install knocked

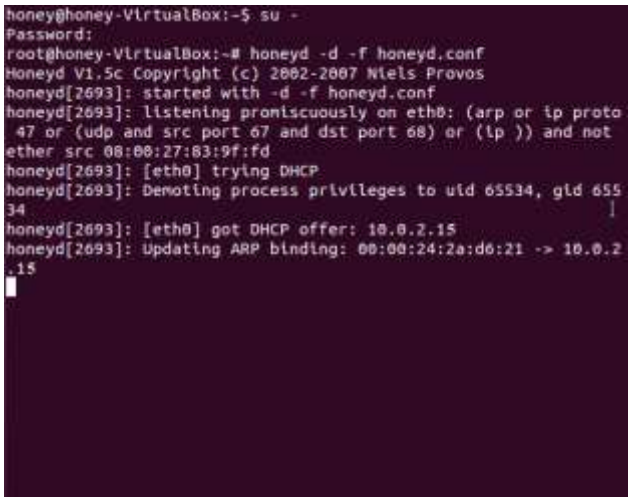


Gambar 7 Tampilan Instalasi Knockd

3.2 . Pengujian Sistem

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, Pada implementasi ini dilakukan dengan installasi server pada VM Virtualbox. Dan untuk tahap pengujian penulis menggunakan aplikasi Namp

Pada pengujian pertama dengan menggunakan aplikasi Nmap didapati Server bayangan dapat di lacak. Pada pengujian ini intruder/penyusup mencoba meremot dengan menggunakan IP Address 10.0.2.15

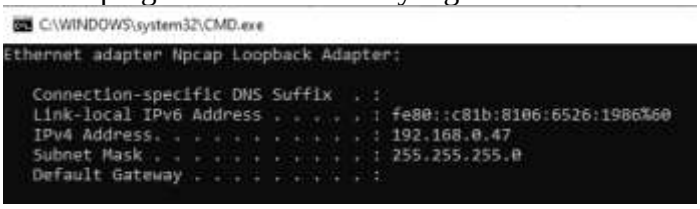


Gambar 8 tampilan ip address HoneyPot

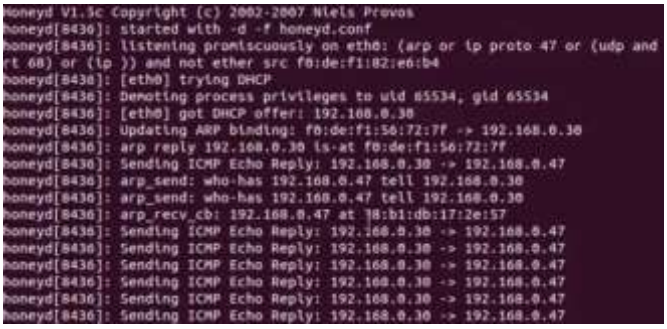
Pada pengujian Mencoba untuk masuk kedalam server banyangan atau server HoneyPot..

Gambar 9 Hasil pengujian Mengguanakan Nmap

Pengujian ke dua mencoba ping kedalam server bayangan



Gambar 10 Tampilan Ip Addres



Gambar 11 Tampilan hasil Ping

Dari hasil pengujian diatas maka didapati hasil sesuai dengan harapan, bahwa server bayangan dapat terditeksi dan di akses .

4 **KESIMPULAN DAN SARAN**

4.1 Kesimpulan

Berdasarkan dari hasil analisa dan simulasi kami menghasilkan :

1. Port Knocking dapat mencegah penyerang dari pemindai sistem seperti service SSH dengan melakukan port scanning, sehingga service SSH tidak mudah dilacak dan diakses orang lain.
2. Sistem yang rancang telah mampu untuk menambah keamanan dalam proses autentikasi ke server, karena port tidak terbuka secara bebas ke publik.
3. Dengan menggunakan HoneyPot dapat mencegah dari upaya seseorang untuk scanning port dan brute force, maka yang akan tampil pada aplikasi scan adalah fake port

3.2 Saran

Meningkatkan keamanan remote server menggunakan metode port knocking dan Honeypot ini tentu tidak terlepas dari beberapa kekurangan. Oleh sebab itu, untuk pengembangan selanjutnya yang lebih baik, penulis menyarankan beberapa hal diantaranya adalah:

1. Dilakukan Pengujian lagi dengan metode yang berbeda untuk mencari kekurangan dan kelemahan dalam sistem
2. Diharapakan untuk penerapan keamanan yang lebih tinggi menggunakan high interaction honeypot
3. Untuk kedepan nya metode Port Knocking menggunakan VPN tunneling .

DAFTAR PUSTAKA

[1] F. H. Mohd Ali, R. Yunos, and M. A. Mohamad Alias, “Simple Port Knocking method: Against TCP replay attack and port scanning,” in *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, 2012.

[2] L. Catuogno, A. Castiglione, and F. Palmieri, “A HoneyPot system with honeyword-driven fake interactive sessions,” in *Proceedings of the 2015 International Conference on High Performance Computing and Simulation, HPCS 2015*, 2015.

[3] FAJRI, M.S.H. SUHATMAN, R., & PUTRA, Y.E. 2013. Analisa Port Knocking Pada Sistem Operasi Linux Ubuntu Server 12.04 LTS. Vol 2 No 2 (2013)

[4] W. Wilman, I. Fitri, and N. D. Nathasia, “PORT KNOCKING DAN HONEYPOT SEBAGAI KEAMANAN JARINGAN PADA SERVER UBUNTU VIRTUAL,” *J I M P - J. Inform. Merdeka Pasuruan*, 201

[5] WAFI, H (2016). Implementasi Sistem Keamanan HoneyPot dengan Modern Honeynetwork Pada Jaringan Wireless. Skripsi Teknologi Informasi. Perpustakaan FST UIN Jakarta, 0356 TI 2016