JIKSTRA *Vol. 03, No. 01, April 2021*
p-ISSN:2715-887X
e-ISSN:2747-2485

PERBANDINGAN KINERJA IPCOP DENGAN HONEYPOT DALAM MENGAMANKAN SERVER LINUX DARI SERANGAN HACKER

Burju Manik[1], Imran Lubis[2]
[1,2]Program Studi Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan.
[1]manikburju8@gmail.com, [2]Imranloebismedan@gmail.com

ABSTRAK

Penelitian untuk melakukan pemasangan IPCop dan honeypot pada komputer server dan mengimplementasikan,IPCop dengan cara melakukan konfigurasi untuk melindungi server dari pihak yang tidak berkepentingan. Perangkat lunak yang digunakan adalah IPCop, Manjaro Linux, Shootpress, Windows 10, dan Virtual Box. Hasil penelitian ini menunjukkan bahwa implementasi IPCop sebagai sistem keamanan pada server dapat dilakukan dan dapat berjalan dengan baik. IPCop mampu melindungi server dari serangan hacker dengan sangat baik, bahkan menggunakan IPCop hacker tidak mampu melakukan ping pada server, sehingga hacker tidak dapat mengetahui informasi mengenai server yang menjadi target. Implementasi honeypot sebagai sistem keamanan pada server linux dapat dilakukan dan dapat berjalan dengan baik. Honeypot mampu melindungi server dari serangan hacker dengan baik melalui server virtual yang dimilikinya. Sehingga hacker tidak mengetahui mana server asli dan hacker hanya akan menyerang server virtual dari honeypot dan berpikir seolah-olah server tersebut adalah server yang sebenarnya. Dalam hal ini IPCop lebih baik dibandingkan dengan honeypot dalam sistem keamanan server.

Kata Kunci: IPCop, Windows, Honeypot, Manjaro Linux, Shootpress

ABSTRACT

Research to install IPCop and honeypot on server computers and implement IPCop by way of configuration to protect the server from unauthorized parties. The software used in this research is IPCop, Manjaro Linux, Shootpress, Windows 10, and Virtual Box. The results of this study indicate that the implementation of IPCop as a security system on the server can be done and can run well. IPCop is able to protect servers from hacker attacks very well, even using IPCop hackers are not able to ping the server, so hackers cannot find out information about the target server. Honeypot implementation as a security system on a linux server can be done and can run well. Honeypot is able to protect the server from hacker attacks well through its virtual server. So that hackers do not know where the original server is and the hacker will only attack the virtual server from the honeypot and think as if the server is the real server. In this case IPCop is better than the honeypot in the server security system.

Keywords*: IPCop, Windows, Honeypot, Manjaro Linux, Shootpress*

I. PENDAHULUAN

Dalam suatu sistem komputer, khususnya pada sistem jaringan komputer, keamanan merupakan hal yang sangat urgen untuk diperhatikan.Hal ini sebab semua telah paling dimudahkan seiring pertumbuhan teknologi dan tidak tidak banyak mereka beranggapan bahwa semua kegiatan telah aman dari serangan peretas. Sehingga kelalaian tersebut dimanfaatkan oleh tidak sedikit peretas guna dapat meretas jaringan suatu server.

Linux memang telah menjadi pilihan banyak orang maupun perusahaan untuk menjadi sebuah sistem operasi yang menjalankan server jaringan yang besar dan luas. Hal ini karena salah satu kelebihan linux yang open sources sehingga banyak pengembang yang mendukung keamanan serta pembaruan perangkat tersebut secara gratis. Namun dibalik hal tersebut terdapat pula banyak celah yang dapat disusupi peretas. Hal ini juga sering terjadi dengan server linux yang dibangun dengan tujuan penggunaan pribadi atau individual.

Alasan beberapa orang membangun server linux untuk penggunaan pribadi dikarenakan besarnya biaya sewa server yang disediakan oleh jasa-jasa penyedia layanan tersebut. Sehingga untuk meminimalisir biaya mereka, terutama yang sudah menguasai jaringan lebih memilih membangun server sendiri dengan berbasiskan linux. Namun kebanyakan dari mereka tidak memperhatikan keamanan server yang telah mereka bangun karena mereka membangun server secara pribadi mereka berpikir tidak akan ada orang lain atau pihak ketiga yang dapat mengakses server mereka. Padahal jika ditelusuri lebih jauh, server dengan kriteria seperti ini sangat rentan terhadap serangan, apalagi jika kurangnya pengetahuan pemilik untuk melakukan maintanance pada server linux.

Ketika jaringan mendapat serangan dan terjadi kehancuran sistem, maka akan tidak sedikit biaya yang harus dibebankan untuk mengerjakan perbaikan sistem. Untuk tersebut setiap empunya server mesti lebih memperhatikan ketenteraman jaringan server mereka guna mencegah kehancuran dari ancaman serangan yang ketika ini semakin beragam.

Salah satu cara yang bisa dilakukan ialah dengan memakai IPCop. IPCop adalahsalah satu penyaluran linux yang menyeluruh dan spesial untuk mengayomi jaringan. Dengan merealisasikan teknologi baru yang terdapat dan pemrograman ketenteraman yang praktis IPCop tetap menjadi penyaluran linux yang diperlukan untuk mengawal jaringan komputer dengan aman. IPCop bertolak belakang dengan Mikrotik yang cepat berkembang dan memiliki keunggulan pada pembagian rasio bandwith. IPCop sebagai sistem operasi linux, guna menjadi firewall dan memiliki kemudahan untuk menyaring konten dan squid yang dapat dipasang bersamaan atau pada komputer yang berbeda.

2. METODE PENELITIAN

Penelitian ini menggunakan sejumlah metode yang bisa diuraikan sebagai berikut:

1. Literatur dan Kajian Pustaka

Metode ini dipakai untuk menemukan data yang dibutuhkan melalui buku, jurnal dan internet

2. Eksperimen
   Merupakan metode dengan mengadakan eksperimen atau pembuatan alat seperti instalasi dan konfigurasi pada layanan yang diterapkan
3. Pengujian
   Metode ini merupakan uji coba terhadap keamanan jaringan yang menggunakan IPCop

3. HASIL DAN PEMBAHASAN

Jaringan Komputer

Jaringan komputer terbagi sekian banyak jenis jaringan, yang mengasingkan menurut lokasi atau skala dan terbagi menjadi 3 unsur yaitu [1]:

1. *Local Area Network (LAN)*
   Local lokasi network adalah jaringan lokal yang dibikin pada lokasi terbatas. Misalkan dalam satu gedung atau satu ruangan. Kadangkala jaringan lokal di sebut pun jaringan individu atau private. Lan dapat di pakai pada skala kecil yang memakai sumber secara bersamaan, seperti pemakaian printer bersama, memakai media penyimpanan secara bersamaan, dan sebagainya.
2. *Metropolitan Area Network (MAN)*
   Metropolitan lokasi network memakai metode yang sama dengan LAN namun wilayah lebih luas ,daerah cakupan. MAN dapat satu RW kantor yang berada dalam satu komplek yang sama, satu/beberapa desa, satu/beberapa kota. Dapat disebutkan MAN pengembangan dari LAN.
3. *Wide Area Network (WAN)*
   Wide lokasi network memakai area yang lebih luas dari pada MAN. memakai MAN mencakup satu kawasan, satu Negara, satu pulau, bahkan satu dunia, cara yang dipakai WAN sama laksana yang di pakai LAN dan MAN. Umumnya WAN terhubung dengan jaringan telepon digital. Namun media transmisi beda pun bisa digunakan.

Ada sejumlah prinsip utama dalam ketenteraman informasi. Hal ini akan membicarakan prinsip-prinsip itu secara singkat. Adapun hal-hal yang lebih mendetail dan teknis, contohnya bagaimana mengimplementasikan aspek keamanan, akan dibicarakan pada bab ini [2].

Ketika anda bicara tentang ketenteraman informasi, maka yang anda bicarakan terdapat tiga urusan yaitu; confidentiality, integrity, dan availability. Ketiganya tidak jarang disebut dengan istilah CIA, yang merupakan campuran huruf depan dari ucapan-ucapan tersebut. Di samping* ketiga urusan* tersebut, masih terdapat* aspek aspek ketenteraman* lainnya.

Confidentiality atau kerahasiaan adalah aspek yang dapat dipahami mengenai keamanan. Aspek *confidentiality* mengaku bahwa data melulu dapat diakses atau disaksikan oleh orang yang berhak. Biasanya aspek ini yang sangat mudah dicerna

oleh orang orang, Jika berhubungan dengan data pribadi, aspek ini pun dikenal dengan istilah privacy.

Serangan terhadap aspek confidentiality bisa berupa penyadapan data (melalui jaringan), memasang keylogger guna menyadap apa-apa yang diketikkan di keyboard, dan pencopetan fisik mesin/disk yang dipakai untuk menyimpan data.

Perlindungan terhadap aspek confidentiality dapat dilaksanakan dengan memakai kriptografi, dan memberi batas akses (segmentasi jaringan) integrity. Aspek integrity menuliskan bahwa data jangan berubah tanpa ijin dari yang berhak. Sebagai contoh, andai kita mempunyai sebuah pesan atau data transaksi inilah ini (transfer dari tabungan 12345 ke tabungan 6789 dengan nilai transaksi teretentu), maka data transaksi itu tidak dapat diolah seenaknya. Serangan terhadap aspek integrity dapat dilaksanakan oleh man-in the-middle, yaitu menciduk data di tengah jalan lantas mengubahnya dan meneruskannya ke tujuan. Data yang hingga di destinasi (misal software di web server) tidak tahu bahwa data sudah diolah di tengah jalan. Perlindungan guna aspek integrity dapat dilaksanakan dengan memakai message authentication code.

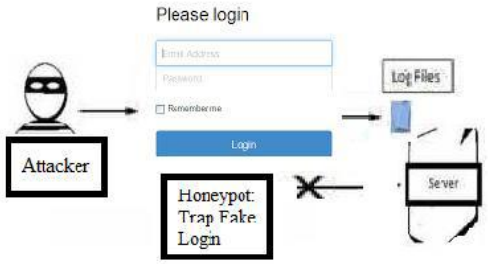
Firewall

Firewall ialah sebuah perlengkapan / aplikasi di dalam jaringan yang dapat mengerjakan pemantauan kemudian lintas jaringan, menciptakan pemisah antara jaringan yang terpercaya dan tidak terpercaya. Firewall menampik semua kemudian lintas yang tidak terpercaya supaya jaringan menjadi aman dari serangan dan memperbolehkan lalu lintas yang terpercaya guna masuk ke dalam jaringan. Firewall adalah garis pertahanan kesatu dalam mengayomi jaringan dan data-data yang terdapat di dalamnya [3].

Honeypot

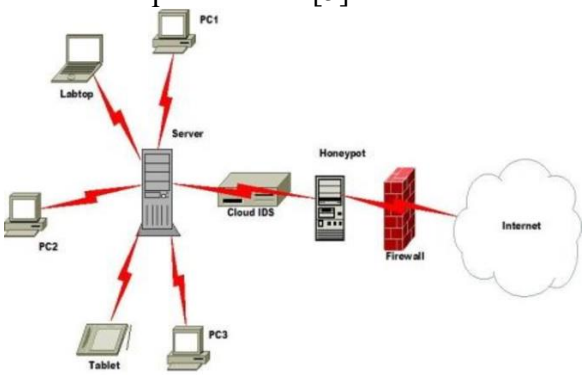
Honeypot adalah security resource yang sengaja diciptakan untuk diselidiki, diserang, atau dikompromikan. Pada lazimny honeypot berupa komputer, data, atau website jaringan yang terlihat laksana bagian dari jaringan, tapi sebetulnya terisolasi dan dimonitor. Jika disaksikan dari kacamata hacker yang bakal menyerang, honeypot terlihat laksana layaknya sistem yang patut guna diserang [4].

Ini dapat dimanfaatkan oleh Administrator Jaringan sebagai input untuk menambal sistem yang sebenarnya, mengkonfigurasi segmen jaringan asli untuk pencegahan dini [4]. Gambar honeypot sebagai berikut.



Gambar 1. Mekanisme Penyerangan

Honeypot adalah sistem komputer di Internet yang dapat mengatur untuk menarik dan menjebak orang yang mencoba menembus sistem komputer lain. Honeypot adalah aplikasi forensik yang dipasang di server yang khusus dirancang untuk memantau aktivitas potensial untuk menyerang dan mengamati penyusup bagaimana mereka masuk ke sistem komputer server [5].



Gambar 2. Security Honeypot

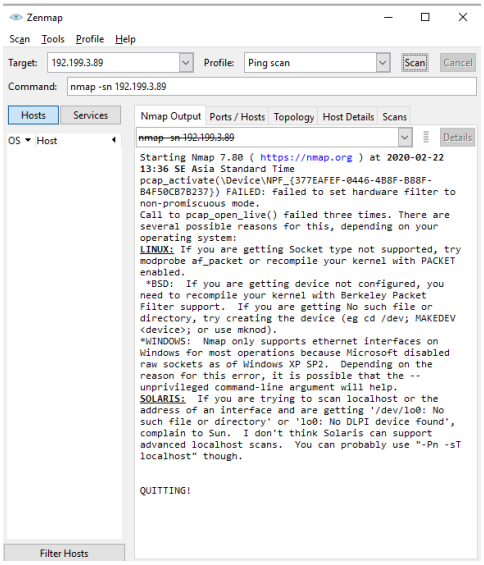
IPCop

IPCop Linux merupakan penyaluran software yang bertujuan guna menyediakan teknik yang gampang dalam menata firewall berbasis perlengkapan keras PC. IPCop adalahsalah satu firewall yang di bina mengunakan kerangka Linux Netfilter. Distro ini tadinya dikembangkan oleh kesebelasan yang mengembangkan Smoothwall Linux firewall, pertumbuhan selanjutnya, IPCop dikembangkan dengan bebas,atau cuma-cuma dan terpisah. IPCop paling sederhana, dan mempunyai fitur user-managed guna mekanisme pembaharuan keamanan, serta mudah dicerna untuk semua pemula, dan handal guna yang telah berpengalaman [6].

Network interface IPCop terdefinisi atas empat macam yakni RED, GREEN, BLUE dan ORANGE yaitu inilah ini [7]:

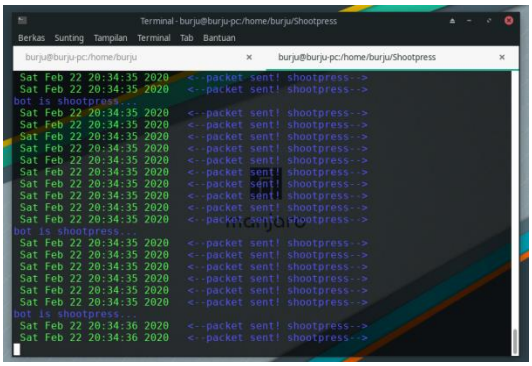
1. RED Network Interface
   Network ini ialah interface internet atau untrusted network. Pada dasarnya yang dibentengi oleh IPCop ialah network GREEN, BLUE dan ORANGE dari traffic yang berasal dari network RED.
2. GREEN Network Interface
   Interface ini melulu terhubung ke komputer yang dibentengi oleh IPCop atau lebih dikenal dengan istilah local network. Traffic ke interface ini ditunjukkan lewat LAN card yang terpasang di IPCop firewall.
3. BLUE Network Interface
   Interface ini ialah interface opsi (digunakan andai dibutuhkan) yang dapat dipakai untuk koneksi perlengkapan wireless di network yang bertolak belakang dari local network. Komputer dibawah interface ini tidak bisa terhubung dengan komputer yang berada pada interface GREEN kecuali dikontrol memakai “pinholes” atau via koneksi VPN. Traffic ke interface ini juga ditunjukkan lewat LAN card yang terpasang di IPCop firewall.
4. ORANGE Network Interface
   Interface ini pun adalah interface opsi yang dipakai untuk menanam server yang boleh diakses oleh network yang berbeda.

Adapun hasil pengujian dari penelitian ini dapat diuraikan sebagai berikut.



Gambar 3. Hasil Uji Ping IPCop

Berdasarkan hasil uji ping pada Gambar 3 dapat dilihat bahwa client tidak dapat melakukan ping ke server IPCop, sehingga client tidak akan bisa mengetahui jaringan dan port yang terbuka pada server. Oleh karena itu server akan aman dari serangan pihak yang tidak bertanggungjawab.



Gambar 4. Output Hasil Serangan

Berdasarkan Gambar 4 dapat dilihat bahwa serangan dapat dilakukan pada server virtual yang dibangun oleh honeypot. Namun serangan ini adalah serangan semu yang tidak akan mengenai atau berdampak terhadap server aslinya. Melalui server virtual honeypot ini penyerang akan merasa bahwa telah berhasil menembus pertahanan server dengan mudah.

Tabel 1. Perbandingan Hasil Uji Keamanan

Jenis Pengujian	Hasil Pengujian	
	IPCop	**Honeypot**
Ping	Tidak dapat melakukan ping ke server IPCop, sehingga penyerang tidak dapat melihat apakah server aktif atau tidak.	Berhasil melakukan ping ke server honeypot, sehingga penyerang dapat mengetahui bahwa server yang akan diserang dalam keadaan aktif.
Port Scanner	Tidak dapat dilanjutkan karena tahap pertama gagal.	Berhasil mengetahui port mana saja yang terbuka pada server honeypot, sehingga dapat melanjutkan serangan pada server.
Shootpress	Tidak dapat dilanjutkan karena tahap pertama gagal.	Berhasil melakukan serangan *shootpress* pada server honeypot melalui IP 10.0.0.08 menggunakan port 22, 53, 23, dan 80.

Untuk mengetahui lebih rinci mengenai kemampuan lebih dan kurangnya dari masing-masing sistem keamanan yang dianalisis dapat dilihat dari kinerja masing-masing sistem keamanan dalam penelitian ini. Untuk melihat perbandingan kinerja tersebut ditunjukkan pada Tabel berikut.

Tabel 2. Perbandingan Kinerja

Kinerja	IPCop	Honeypot
Membuat IP Virtual	x	√
Memblokir IP Tidak Dikenal	√	x
Membatasi Pengguna	√	x
Tidak Dapat di Ping	√	x
Tidak Dapat Melihat Port yang Terbuka	√	x
Kebal Terhadap Serangan Shootpress	√	√

Berdasarkan hasil perbandingan kinerja pada Tabel 2 dapat dilihat bahwa IPCop lebih unggul dibandingkan dengan honeypot sehingga dapat disimpulkan bahwa dalam penelitian ini IPCop merupakan sistem keamanan jaringan yang paling baik dibandingkan dengan honeypot.

4. KESIMPULAN

Kesimpulan

Implementasi IPCop sebagai sistem keamanan pada server dapat dilakukan dan dapat berjalan dengan baik.

IPCop mampu melindungi jaringan dari serangan hacker dengan sangat baik, bahkan menggunakan IPCop, hacker tidak mampu melakukan ping pada server, sehingga hacker tidak dapat mengetahui informasi mengenai server yang menjadi target.

Implementasi honeypot sebagai sistem keamanan pada server linux dapat dilakukan dan dapat berjalan dengan baik.

Honeypot mampu melindungi jaringan dari serangan hacker dengan baik melalui server virtual yang dimilikinya. Sehingga hacker tidak mengetahui mana server asli dan hacker hanya akan menyerang server virtual dari honeypot dan berpikir seolah-olah server tersebut adalah server yang sebenarnya.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih untuk Fakultas Teknik dan Komputer Universitas Harapan Medan yang sudah memberi sokongan financial terhadap riset ini

DAFTAR PUSTAKA

[1] I. Sofana, *Membangun Jaringan Komputer: Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux*. Bandung: Informatika, 2017.

[2] Binus University, "Port (Jaringan Komputer)," 2019. https://socs.binus.ac.id/2019/11/06/port-jaringan-komputer/ (accessed Jun. 14, 2020).

[3] Comer, *Computer Networks And Internets*. New Jersey: Prentice Hall, 2014.

[4] B. Rahardjo, *Keamanan Informasi*. Jakarta: budi.rahardjo.id, 2017.

[5] E. Maiwald, *Fundamentals of Network Security*. New York: McGraw-Hill, 2014.

[6] H. Anggeriana, "Perancangan Keamanan Cloud Computing Melalui Honeypot Sistem," *E-Journal*, vol. Vol. 12, 2015.

[7] T. M. Diansyah, "Analysis Of Using Firewall And Single Honeypot In Training Attack On Wireless Network," 2017.