JURNAL

SISTEM KEAMANAN *HONEYPOT* PADA JARINGAN NIRKABEL (*HOTSPOT*) DI UNIVERSITAS NUSANTARA PGRI KEDIRI

Oleh:

KHOIRUL ANAM

12.1.03.03.0138

Dibimbing oleh :

1. **Fatkur Rhohman, M. Pd**
2. **Rini Indriati, S. Kom., M. Kom**

SISTEM INFORMASI

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2017

Artikel Skripsi
Universitas Nusantara PGRI Kediri

SURA TPERNYATAAN
ARTIKEL SKRIPSI TAHUN 2017

Yang bertanda tangandibawahini:

Nama Lengkap	: Khoirul Anam
NPM	: 12.1.03.03.0138
Telepun/HP	: 085755897808
Alamat Surel (Email)	: kakhoirul66@gmail.com
Judul Artikel	: Sistem Keamanan *Honeypot* pada Jaringan Nirkabel (*Hotspot*) di Universitas Nusantara PGRI Kediri
Fakultas – Program Studi	: Fakultas Teknik – Sistem Informasi
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: JL. K.H. Achmad Dahlan No. 76 Tel. : (0354) 771576, 771503, 771495 Kediri

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;
b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila dikemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 30 Januari 2017
Pembimbing I	Pembimbing II	Penulis,
Fatkur Rhohman, M. Pd NIDN. 0728088503	Rini Indriati, S. Kom., M. Kom NIDN. 0725057003	Khoirul Anam NPM. 12.1.03.03.0138

Khoirul Anam | 12.1.03.03.0138
Fakultas Teknik – Sistem Informasi
simki.unpkediri.ac.id
|| 1||

SISTEM KEAMANAN *HONEYPOT* PADA JARINGAN NIRKABEL (*HOTSPOT*) DI UNIVERSITAS NUSANTARA PGRI KEDIRI

Khoirul Anam
12.1.03.03.0138
Fakultas Teknik–Sistem Informasi
Email : kakhoirul66@gmail.com
Fatkur Rhohman, M.Pd dan Rini Indriati, S. Kom., M. Kom
UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Keamanan merupakan salah satu aspek terpenting pada sebuah sistem informasi. Keamanan jaringan komputer menjadi salah satu faktor pendukung terpenting pada sebuah jaringan komputer, agar jaringan komputer dapat berjalan sebagai mana mestinya. Sehingga dibutuhkan suatu sistem keamanan yang dapat membantu menyelesaikan permasalahan yang terjadi pada suatu jaringan komputer.

Permasalahan pada penelitian ini adalah bagaimana cara pendeteksian jenis serangan yang terjadi pada jaringan nirkabel di Universitas Nusantara PGRI Kediri, dengan menggunakan metode *Honeypot*. Kemudian cara menjalankan beberapa *tools* pendukung untuk mendapatkan hasil informasi tentang *port* yang terbuka yang dapat diambil alih oleh para *hacker*. Semua permasalahan tersebut akan diminimalisir dengan beberapa cara yang terdapat pada sistem.

Honeypot merupakan sebuah sistem yang sengaja "dikorbankan" untuk menjadi target serangan dari *hacker*. Metode ini ditujukan agar administrator dari *server* yang akan diserang dapat mengetahui trik penetrasi yang dilakukan *hacker* serta bisa melakukan antisipasi dalam melindungi *server* yang sesungguhnya. Setiap tindakan yang dilakukan oleh penyusup yang mecoba melakukan koneksi ke *honeypot*, maka *honeypot* akan mendeteksi dan mencatatnya.

Kesimpulan dari penelitian yang dilakukan dapat memunculkan beberapa informasi tentang *port* yang terbuka yang dapat diambil alih oleh *hacker*. *User* dapat mengetahui terjadinya serangan yang dilakukan oleh *hacker*, sehingga *user* dapat mengambil tindakan pengamanan untuk mengamankan *server*.

Dengan adanya penelitian ini, diharapkan kedepanya ada yang mengembangkan kinerja dari metode *honeypot*. Supaya metode ini dapat dioptimalakan kinerjanya. Seperti dapat menambahkan identifikasi pola serangan, mengetahui *software* dan metode yang digunakan *hacker*, mengetahui lokasi *hacker* dan melakukan serangan balik kepada *hacker*, mengetahui kelemahan *hacker* dan menginfeksikan virus ke *hacker*.

KATA KUNCI : Sistem Keamanan Jaringan, *Honeypot, Hacker, BackOfficer Friendly*.

I. LATAR BELAKANG

Masalah keamanan merupakan salah satu aspek terpenting pada sebuah sistem informasi. Terkadang untuk permasalahan sistem informasi masih dipandang sebelah mata. Padahal aspek tersebut cukup vital dalam pengembangan infrastruktur suatu organisasi yang memiliki ketergantungan akan dunia IT, khususnya pengembangan sistem informasi itu sendiri. Banyak hal untuk melakukan pengamanan, yaitu diperlukan perangkat yang mendukung serta sumber daya manusia yang mampu dalam

menyelesaikan setiap masalah keamanan dari sistem informasi (Pranajaya, 2011).

Keamanan jaringan komputer dibagi menjadi dua bagian, yaitu keamana secara fisik dan keamana secara non-fisik. Keamanan secara fisik merupakan keamanan yang cenderung lebih memfokuskan segala sesuatunya berdasarkan sifat fisiknya. Dalam hal ini misalnya pengamanan komputer agar terhindar dari pencurian dengan rantai sehingga fisik komputer tersebut tetap pada tempatnya. Sedangkan keamanan non-fisik adalah keamanan dimana suatu kondisi keamanan yang menitikberatkan pada kepentingan secara sifat, sebagai contoh yaitu pengamanan data, misalnya data sebuah perusahaan yang sangat penting (Borut, 2011).

Keamana fisik ataupun keamanan non-fisik keduanya sangat penting, namun yang terpenting adalah bamputer tersebut terhindar dari gangguan. Gangguan tersebut dapat berupa gangguan dari dalam (*internal*) ataupun gangguan dari luar (*eksternal*). Ganguan internal merupakan gangguan yang berasal dari lingkup dalam jaringan infrastruktur tersebut, dalam hal ini adalah gangguan dari pihak-pihak yang telah mengetahui kondisi keamanan dan kelemahan jaringan tersebut. Gangguan eksternal adalah gangguan yang memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada. Gangguan eksternal biasa lebih sering terjadi pada jaringan eksternal seperti web-server, telnet, FTP, SSH-server (Borut, 2011).

Sehubung dengan diperlukannya sebuah keamanan jaringan pada jaringan nirkabel (*hotspot*) di area Universitas Nusanatara PGRI Kediri dipilihlah sebuah judul yakni “Sistem Keamanan *Honeypot* Pada Jaringan Nirkabel (*Hotspot*) di Universitas Nusantara PGRI Kediri ”. *Honeypot* sendiri merupakan komputer duplikat dari *server* yang digunakan untuk menjebak *hacker*/*cracker*. Dengan adanya *Honeypot* masalah yang terjadi di Universitas Nusantara PGRI Kediri bisa diminimalisir. Sistem keamanan ini diharapkan bisa menjaga keamanan pada jaringan nirkabel (*hotspot*) dan tidak mudah diretas oleh para *hacker*/*cracker*.

II. METODE

Adapun metode pada penelitian ini adalah sebagai berikut :

1. Subyek Penelitian

Subyek yang akan dibahas pada tugas akhir ini adalah "Rancang Bangun Sistem Keamanan *Honeypot* Pada Jaringan Nirkabel (*Hotspot*)" dengan studi kasus di Universitas Nusantara PGRI Kediri. Diharapkan dengan adanya sistem keamanan pada jaringan *hotspot* yang berupa *Honeyd* dapat mengurangi resiko penyerangan, baik terhadap *server* maupun *user*.

2. Metode Pengumpulan Data

Metode yang dilakukan bertujuan agar hasil dari penelitian dan analisa lebih terarah serta data yang diperoleh lebih akurat. Kelengkapan data yang diperoleh dapat memberikan konstribusi dalam proses penyusunan skripsi ini, dan memberikan waktu yang lebih singkat. Metode yang dilakukan dalam pengumpulan data terdiri dari :

a. Studi Pustaka

Metode pengumpulan data dengan cara membaca berdasarkan kepustakaan dari buku, jurnal maupun makalah yang mana dimaksudkan untuk mendapatkan konsep teori yang mengenai masalah yang ingin ditelitiserta mencari sumber data dari internet.

b. Metode Observasi

Pengumpulan data dengan pengamatan secara langsung pada obyek yang diteliti untuk memperoleh informasi yang tepat dan sistematis. Meliputi *instalasi*, *konfigurasi*, *tool* yang dipakai dan pengujian koneksi terhadap internet.

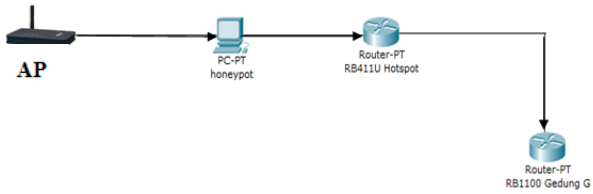
III. HASIL DAN KESIMPULAN

A. HASIL

Desain sistem adalah tahap berupa penggambaran, perencanaan dan pembuatan dengan menyatukan beberapa elemen terpisah kedalam satu kesatuan yang utuh untuk memperjelas bentuk sebuah sistem. Yang terdiri dari :

1. Desain *Output*

Rancangan penerapan keamanan pada topologi yang telah tersedia dapat digambarkan sebagai berikut.



Gambar 5.1 Topologi Rancangan Penerapan Keamanan

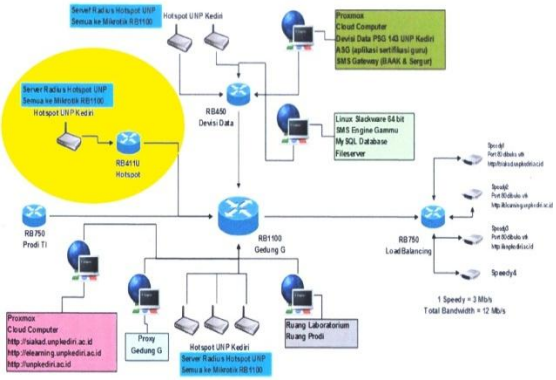
Keterangan.

Gambar diatas menerangkan bahwa tempat untuk meletakkan komputer keamanan yaitu seletah AP (*access point*). Dimana jika terjadi penyerangan oleh *hacker* tidak

akan langsung menuju *server* asli, melainkan akan masuk kedalam duplikat *server*. Sehingga dapat meminimalisir terjadinya pencurian data pada *server* pusat yang dilakukan oleh *hacker*.

2. Desain *Input*

Pemilihan lokasi yang terdapat pada topologi yang telah ada digambarkan sebagai berikut.



Gambar 5.2 Penentuan Lokasi Penelitian

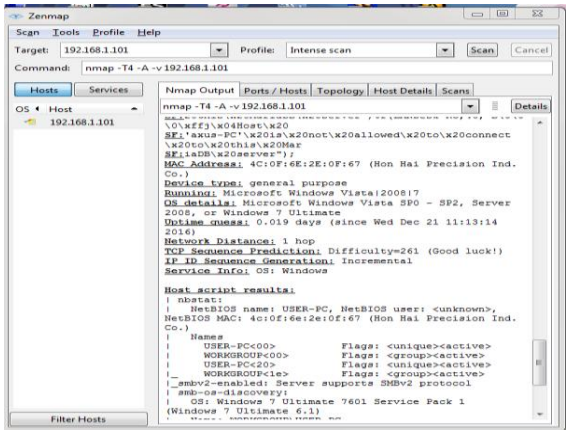
Keterangan.

Pemilihan lokasi untuk melakukan penelitian ditetapkan pada bagian topologi yang ditandai dengan warna kuning. Pada area tersebut, penerapan keamanan jaringan akan dilakukan.

3. Modul Program

Pada modul program ini akan dibahas hasil dari simulasi percobaan penyerangan dan simulasi hasil dari pendeteksian penyusup. Yang akan ditunjukkan pada Gambar 5.21 Simulasi penyeranangan terhadap komputer *server* dan pada Gambar 5.22 Simulasi pendeteksian penyusup dari komputer *server*.

a. Simulasi penyerangan terhadap komputer *server*

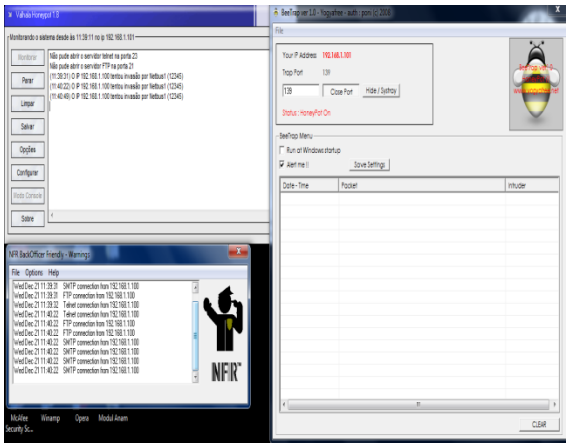


Gambar 5.21 Simulasi penyerangan terhadap komputer *server*

Keterangan.

Pada simulasi penyerangan tersebut yang dilakukan dengan menggunakan *Nmap* ditujukan kepada komputer yang memiliki ip address 192.168.1.101 dengan Intense scan. Dan penyerang tersebut berhasil memasuki ip address dari komputer target.

b. Simulasi pendeteksian penyusup dari komputer *server*



Gambar 5.22 Simulasi pendeteksian penyusup dari komputer *server*

Keterangan.

Pada simulasi pendeteksian tersebut yang menangkap adanya serangan adalah *valhala honeypot* dan *backOfficer friendly*, sedangkan *beetrap* tidak melakukan respon. Pada kedua *tools* tersebut muncul *ip address* dari penyusup yang terdeteksi. Kemudian akan dilakukan pemberhentian serangan tersebut.

B. KESIMPULAN

Berdasarkan penelitian yang dilakukan dengan menggunakan metode *Honeypot* dapat ditarik kesimpulan :

1. Pendeteksian serangan menghasilkan informasi tentang *ports* yang terbuka yang bisa diserang oleh *hacker* yang terjadi dalam jaringan lokal terdapat pada Universitas Nusantara PGRI Kediri, sehingga dapat diminimalisir dengan cara menambahkan sistem keamanan tambahan pada server.
2. Operasiaonal *tools* pendukung seperti *valhala honeypot, backofficer friendly,* dan *beetrap* yang dapat membantu mengoptimalkan kinerja dari *Honeypot,* sehingga lalu lintas jaringan *hotspot* yang ada di Universitas Nusantara PGRI Kediri menjadi lancar.

IV. DAFTAR PUSTAKA

Borut, R. K. 2011. *Pengamanan Jaringan Komputer Pascasarjana UPN "Veteran" Jatim Menggunakan Metode "IDS (Intruction Detection System) Dari Aktivitas Hacking IRC*. Surabaya : Universitas Pembangunan Nasional “Veteran”.

Husnan, S. 2013. *Implementasi Honeypot Untuk Meningkatkan Sistem Keamanan Server Dari Aktivitas Serangan*. Surakarta : Universitas Muhammadiyah.

Herwindo, Akbar, Ali. 2005. *Mengenal Sistem Komputer Masa Kini*. Bandung : Yrama Widya.

Mustofa, M. M., dan Ariwibowo, E. 2013. *Penerapan Sistem Keamanan Honeypot Dan IDS Pada Jaringan Nirkabel (Hotspot)*. Yogyakarta : Universitas Ahmad Dahlan.

Pranajaya, H. 2011. *Metode Implementasi Honeypot*. Palembang : Universitas Sriwijaya.

Provos,N., dan Holz,T. 2007. *Virtual Honeypots: From Botnet Tracking To Intrusion Detection.* Massachusetts : Addison Wesley.

Singh, R.K., dan Ramanujam, T. 2009. *Intrusion Detection System Using Advanced Honeypot*. International Journal of Computer Science and Information Security.

Sulistiyo. 2012. *Jurnal Komunikasi Data Dan Jaringan*. Jakarta Selatan : Universitas Indraprasta PGRI.

Sumarno, dan Bisosro, S. 2011. *Solusi Network Security Dari Ancaman SQL Injection Dan Denial Of Service (DOS)*. Sidoarjo : Universitas Muhammadiyah.

Tambunan, B., Raharjo, S. W., dan Purwadi, J. 2013. *Desain Dan Implementasi Honeypot Dengan Fwsnort Dan PSAD Sebagai Intrusion Prevention System*. Yogyakarta : Universitas Kristen Duta Wacana.

Utdirartatmo, F. 2005. *Trik Menjebak Hacker Dengan Honeypot.* Yogyakarta: ANDI.