Honeyd untuk Mendeteksi Serangan Jaringan di Universitas Muhammadiyah Purwokerto

(Honeyd for Detecting Network Atacks in Muhammadiyah University of Purwokerto)

Harjono[1)], Agung Purwo Wicaksono[2)]

[1) 2)]*Teknik Informatika, F. Teknik, Universitas Muhammadiyah Purwokerto*
Jl. Raya Dukuhwaluh PO. Box 202 Purwokerto 53182

[1)]harjono@ump.ac.id

Abstrak - Teknologi jaringan komputer merupakan sebuah kebutuhan yang harus diterapkan oleh setiap organisasi saat ini. Namun dengan terhubungnya komputer satu dengan lainnya tersebut dapat dimanfaatkan pihak tertentu untuk melakukan serangan guna memperoleh keuntungan pribadi. Penelitian ini bertujuan untuk mendeteksi adanya serangan di dalam jaringan Universitas Muhammadiyah Purwokerto menggunakan *Honeyd*. *Honeyd* ditempatkan pada segmen jaringan internal, dengan konfigurasi untuk menirukan empat host dengan sistem operasi dan layanan yang berbeda-beda. Dari penelitian ini didapatkan sejumlah serangan kepada *honeyd* yang berasal dari sejumlah *host* dengan alamat IP *private* dari dalam jaringan internal. Serangan yang terdeteksi dilakukan secara otomatis oleh malware.

Kata kunci: Jaringan komputer, serangan, honeyd, malware.

Abstract - Computer network technology is a necessity that must be applied by any organization at this time. But the connection of computers to each other can be exploited by certain parties to carry out the attack in order to obtain personal gain. This research aimed to detect attacks in the network of Muhammadiyah University of Purwokerto using Honeyd. Honeyd is placed on the internal network segment, with the configuration to mimic the four host operating systems and different services. A number of attacks to Honeyd originated from several host with private IP address of the internal network. Attacks are detected done automatically by malware.

Keywords: Computer network, attack, Honeyd, Malware.

I. PENDAHULUAN

Pada awal perkembangan komputer, teknologi jaringan belum dikenal. Kebanyakan sistem komputer berupa mainframe yang terkendali secara terpusat. Pengguna (*user*) terhubung ke sistem komputer dengan menggunakan *dumb* terminal. Terminal ini mempunyai kemampuan yang sangat terbatas, yaitu sebatas untuk memasukkan serta melihat hasil dari olahan data yang dilakukan oleh sistem komputer mainframe. Terminal tersebut terhubung melalui port tertentu seperti port serial RS-232. Setiap terminal membutuhkan satu port dari komputer mainframe. Hal ini sangat berbeda dengan keadaan sekarang, yaitu sebuah sistem dapat terhubung dengan ratusan bahkan ribuan sistem lainnya hanya dengan sebuah kartu jaringan [1].

Seiring dengan perkembangan komputer pribadi (*personal computer* = PC), perkembangan jaringan, semakin murahnya harga hardware, dan perkembangan aplikasi baru maka jaringan komputer semakin banyak diterapkan. Tidak hanya perusahaan atau organisasi besar yang menggunakan jaringan. Organisasi atau instansi kecilpun semuanya menggunakan teknologi jaringan komputer.

Pada awal dikembangkan, jaringan lokal (*Local Area Network* = LAN) relatif aman karena secara fisik terpisah atau antar jaringan tidak saling terhubung. Namun setelah dihubungkannya satu jaringan dengan jaringan yang lain hingga terbentuk jaringan yang luas (*Wide Area Network* = WAN) maka faktor keamanan menjadi berkurang. Jaringan komputer yang terhubung ke internet akan memudahkan pengaksesan beragam informasi dari seluruh penjuru dunia. Namun dari segi keamanan hal tersebut justru memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. Oleh karena itu sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dirancang dengan baik agar sumber daya yang berada dalam jaringan tersebut dapat terlindungi dengan baik. Keamanan sistem komputer melingkupi enam aspek, yaitu *privacy,*

integrity, authentication, availability, access control, dan *non-repudiation* [2].

Pada dunia keamanan jaringan, banyak profesional yang sangat tertarik pada *Honeypot* karena seorang pengamat serangan akan dapat melihat informasi secara nyata tentang suatu serangan. Salah satu hal yang bisa didapat dengan *Honeypot* adalah informasi bagaimana seorang penyerang dapat menerobos dan apa yang sudah dilakukannya. *Honeyd* merupakan sebuah *low-interaction honeypot* yang dapat membuat banyak *honeypot* pada sebuah jaringan [3]. *Honeyd* mendukung protocol IP dan merespon permintaan jaringan sesuai dengan layanan (*service*) yang dikonfigurasi.

Jaringan komputer Universitas Muhammadiyah Purwokerto sudah pasti memiliki banyak informasi penting yang harus dilindungi dari berbagai gangguan dan serangan. Tujuan dari penelitian ini adalah mendeteksi serangan yang ada di dalam jaringan Universitas Muhammadiyah Purwokerto dengan menggunakan *honeyd.*

II. METODE PENELITIAN

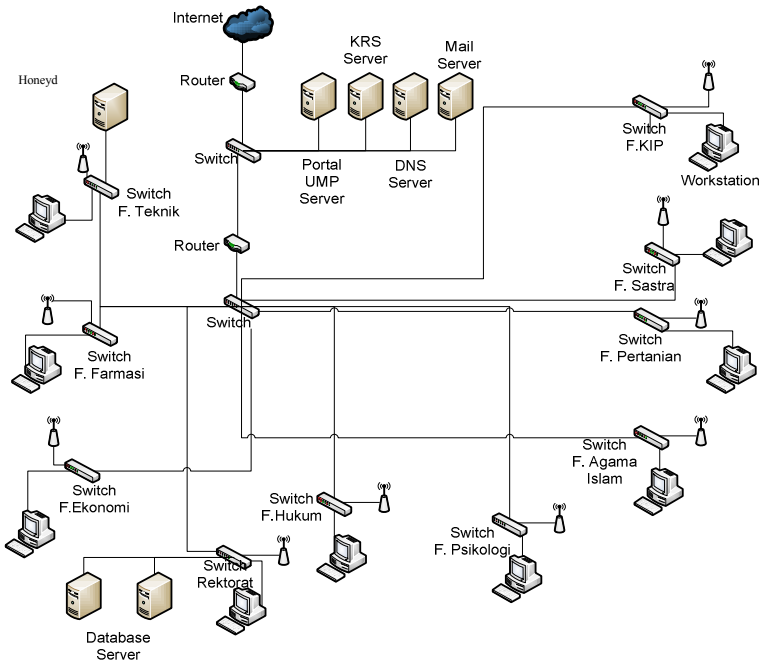
Perangkat lunak yang digunakan dalam penelitian ini adalah *honeyd* yang berjalan di atas sistem operasi *Linux Ubuntu* 10.04. Perangkat lunak pendukung yang digunakan adalah nmap, farpd, gedit, notepad, dan web browser. Sedangkan peralatan yang digunakan berupa sebuah perangkat keras komputer dengan spesifikasi yang cukup untuk menjalankan *honeypot honeyd* diatas Sistem Operasi *Linux Ubuntu* 10.04. Selain itu juga digunakan perangkat jaringan yang sudah terpasang pada jaringan lokal Universitas Muhammadiyah purwokerto.

Data yang dipakai pada penelitian ini adalah data sekunder yang diambil dari penelitian [4] berupa topologi jaringan UMP. Penelitian diawali dengan melakukan evaluasi jaringan kemudian dilakukan perancangan sistem keamanan yang baru. Pada tahap ini ditentukan juga lokasi penempatan *honeyd*. Setelah instalasi *honeyd* kemudian dilakukan pembuatan kode atau script program untuk konfigurasi *honeyd.* Langkah berikutnya adalah pengujian dan simulasi. Setelah pengujian sesuai seperti yang diharapkan, kemudian *honeyd* dioperasikan. *Honeyd* dioperasikan selama dua bulan untuk mendeteksi serangan yang ada di dalam jaringan UMP. Langkah terakhir adalah melakukan analisis terhadap log file yang dihasilkan oleh *honeyd*. Analisis ini dilakukan untuk mengetahui berapa banyaknya serangan, alamat asal serangan, dan tujuan serangan.

III. HASIL DAN PEMBAHASAN

A. Perancangan Sistem

Rancangan sistem seperti pada Gambar 1. *Honeyd* digunakan untuk mendeteksi serangan dalam jaringan komputer di UMP.



Gambar 1. Rancangan Topologi Jaringan

B. Pembuatan Script Konfigurasi Honeyd

Konfigurasi *honeyd* digunakan untuk menentukan sistem operasi serta port yang terbuka atau layanan yang disediakan oleh *honeypot honeyd. Honeyd* dikonfigurasi untuk menirukan empat host dengan alamat IP masing-masing 10.12.6.220, 10.12.6.221, 10.12.6.222, dan 10.12.6.223. Dengan menirukan sistem operasi berturut-turut Microsoft Windows XP SP1, Microsoft Windows 2000 SP3, FreeBSD 2.1.0 – 2.1.5, dan Linux 2.4.20.

Tujuan dari konfigurasi tersebut adalah untuk mengelabui penyerang seolah-olah terdapat empat server dengan berbagai layanan (port yang terbuka). Karena tahapan penyerang dalam melakukan serangan biasanya dengan melakukan *scanning* untuk mencari pintu masuk atau tempat serangan akan dijalankan. Seorang penyerang melalui aktivitas ini berusaha mencari lubang-lubang keamanan tempat serangan masuk. Dari proses ini dapat diketahui sistem operasi dan port-port yang terbuka. Penyerang akan melakukan serangan berdasar pada teknik yang dikuasainya terhadap kerentanan yang ada.

C. Simulasi Honeyd

Setelah proses instalasi serta pembuatan script konfigurasi *honeyd* selesai, tahap berikutnya adalah melakukan simulasi terhadap sistem untuk mengetahui apakah sistem dapat berjalan sesuai dengan yang diharapkan. *Honeyd* berjalan sesuai dengan yang diinginkan jika memenuhi syarat-syarat berikut.

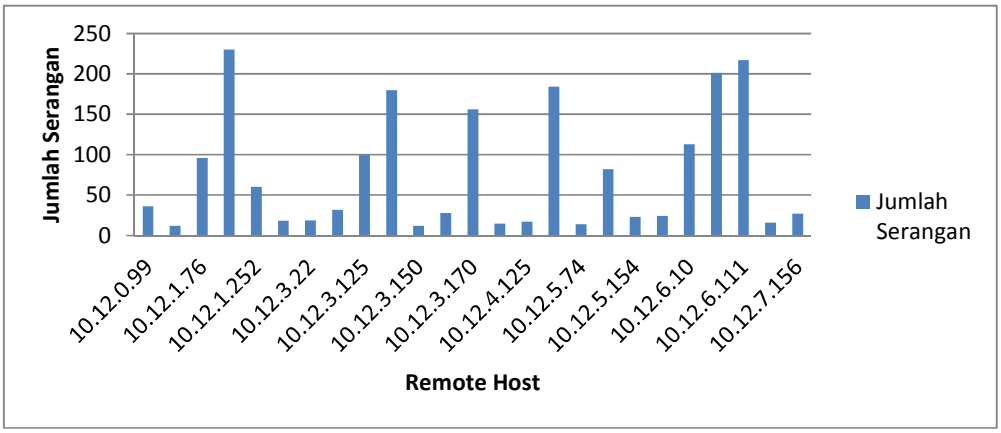
a. Alamat IP dari host yang ditirukan oleh *honeyd* dapat dijangkau atau diakses oleh host lain dalam jaringan.
b. *Scanning* yang dilakukan terhadap host-host yang ditirukan oleh *honeyd* menggunakan *nmap* menghasilkan sistem operasi dan port terbuka sesuai dengan file konfigurasi *honeyd*.
c. Layanan yang ditirukan oleh *honeyd* dapat diakses oleh host lain dalam jaringan.
d. Setiap trafik yang menuju *honeyd* tercatat dalam *log file.*

D. Pengujian Dionaea

Setelah dilakukan simulasi terhadap *Dionaea*, langkah berikutnya adalah penerapan *honeyd* dalam jaringan lokal UMP. Pada tahapan ini *honeyd* dijalankan atau dioperasikan, sehingga dihasilkan data pada file log. Pada penelitian ini *honeyd* dioperasikan pada bulan Juni dan Juli 2013.

E. Analisis Data dari Honeyd

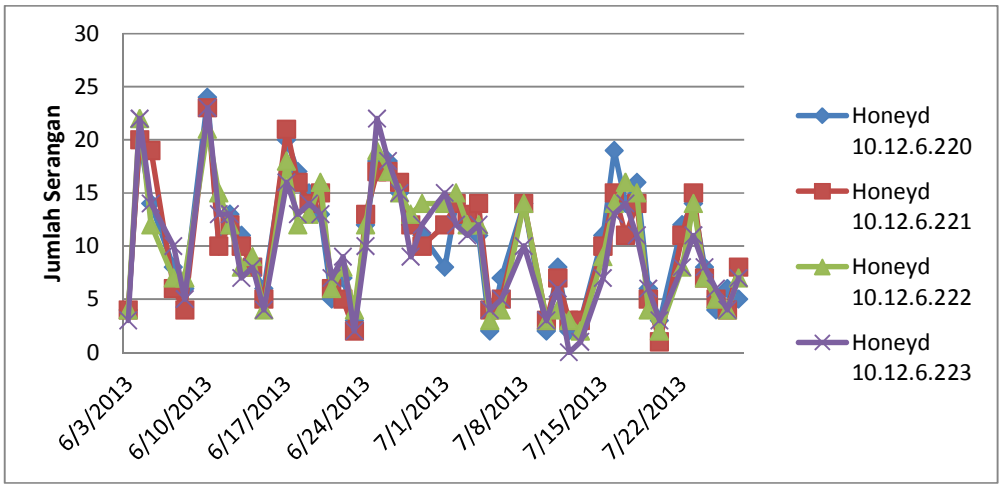
Dari pengamatan selama *honeyd* dijalankan, pada file *log* tercatat sejumlah *host* yang mencoba untuk berinteraksi dengan *honeyd*. Karena *honeyd* tidak menyediakan layanan produksi, seharusnya tidak menerima atau menghasilkan trafik apapun. Sehingga semua trafik yang menuju *honeyd* dapat dianggap sebagai serangan. Dari total serangan yang menuju ke *honeyd*, dapat dikelompokkan berdasar alamat IP *honeyd* yaitu 10.12.6.220, 10.12.6.221, 10.12.6.222, dan 10.12.6.223. Jumlah serangan yang menuju ke *honeyd* tersebut dapat ditunjukkan seperti pada Gambar 2.



Gambar 2. Jumlah Serangan dari Sejumlah *Host*

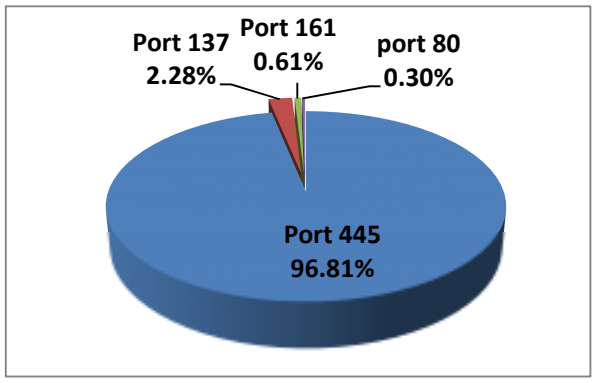
Distribusi serangan yang menuju ke tiap-tiap alamat IP *honeyd* selama dioperasikan dapat ditunjukkan pada Gambar 3. Tampak bahwa jumlah trafik yang menuju tiap-tiap IP *honeyd* relatif sama meskipun konfigurasi sistem operasi dan layanan yang disediakan dari masing-masing IP *honeyd* berbeda. Rata-rata dalam satu

hari jumlah trafik yang menuju *honeyd* sebanyak 10 trafik.



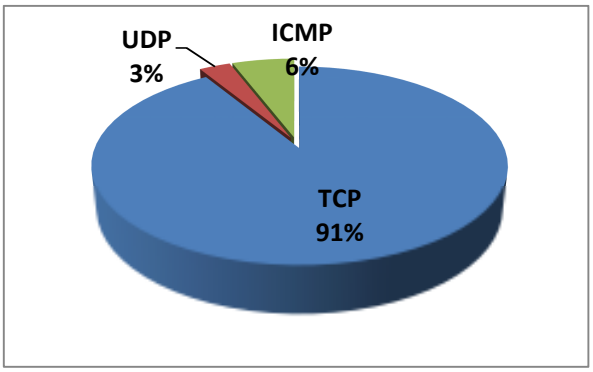
Gambar 3. Distribusi Serangan ke *Honeyd*

Adapun jumlah trafik yang menuju ke *honeyd* jika dikelompokkan berdasarkan protokol yang digunakan seperti ditunjukkan pada Gambar 4. Terlihat bahwa protokol TCP paling banyak dipakai yaitu sebesar 91% dari total trafik. Sementara protokol ICMP dan UDP jauh lebih kecil yaitu masing-masing sebesar 6% dan 3%.



Gambar 4. Persentase Protokol dari Trafik *Honeyd*

Sementara persentase nomor port tujuan trafik *honeyd* seperti ditunjukkan pada Gambar 5. Terlihat bahwa port 445 paling banyak dituju yaitu sebesar 96,81%. Sedangkan tiga port yang lainnya jauh lebih kecil, port 137 sebesar 2,28%, port 161 sebesar 0,61%, dan port 80 hanya 0,30%.



Gambar 5. Persentase Port yang Diserang

Dari data yang didapat, serangan yang menuju *honeyd* tersebut tidak dilakukan secara manual tetapi serangan otomatis yang dilakukan oleh *malware*. Sebagai indikasi serangan dilakukan sangat cepat dalam hitungan milidetik sudah berganti tujuan. Kemudian serangan mencoba melakukan eksploitasi port 445 untuk semua *host* (IP *honeyd*). Port 445 digunakan oleh windows untuk layanan microsoft-ds. Windows menggunakan TCP port 445 untuk menjalankan protokol SMB (*Server Message Block*) *over* TCP/IP. Protokol SMB merupakan protokol yang digunakan untuk keperluan *sharing*. Mereka begitu cepat menyerang *host* tanpa memeriksa apakah *host* tersebut rentan terhadap eksploit yang mereka coba atau tidak. Serangan juga tidak memperdulikan sistem operasi serta layanan yang disediakan oleh *host* sasaran.

IV. PENUTUP

A. Kesimpulan

Dari hasil penelitian, dapat ditarik kesimpulan bahwa serangan yang terdeteksi oleh *honeyd* berasal dari sejumlah host yang mempunyai alamat *IP private* dari dalam jaringan internal UMP. Hal tersebut menunjukkan bahwa penyerang berasal dari dalam jaringan internal. Rata-rata dalam satu hari jumlah serangan yang menuju *honeyd* sebanyak 10 kali serangan. Empat host yang disimulasikan *honeyd* mendapatkan jumlah serangan yang relatif sama besar. Serangan yang terdeteksi oleh *honeyd* adalah serangan dilakukan secara otomatis oleh *malware.*

B. Saran

Informasi serangan yang diperoleh pada penelitian dengan menggunakan *honeyd* ini sangat terbatas. Pada penelitian selanjutnya, untuk mendapatkan informasi yang lebih lengkap tentang serangan yang ada, sebaiknya digunakan *high interaction honeypot*.

DAFTAR PUSTAKA

[1] Canavan, John E. 2001. *Fundamental of Network Security*. Artech House. London.

[2] Rahardjo, B. 2005. *Keamanan Sistem Informasi berbasis Internet*, PT. Insan Indonesia. Bandung.

[3] Provos, N. 2004. *A Virtual Honeypot Framework*. Google Inc.

[4] Harjono dan Pinandita, T. 2012. Deteksi Malware di Jaringan Lokal Universitas Muhammadiyah Purwokerto Menggunakan Dionaea. *Laporan Penelitian*. FT-UMP. Purwokerto.