ISSN 1411-0865

INFOMATEK

Volume 15 Nomor : 1 Juni 2013

JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

Jurnal INFOMATEK	Vol. 15	No. 1	Hal. 1 – 58	Bandung Juni 2013	ISSN 1411-0865

FAKULTAS TEKNIK UNIVERSITAS PASUNDAN BANDUNG

TELAH TERAKREDITASI BERDASARKAN SURAT KEPUTUSAN
DIRJEN DIKTI DEPDIKNAS RI NO. 34/DIKTI/Kep/2003

ISSN 1411-0865

INFOMATEK

Volume 15 Nomor 1 Juni 2013 JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

Penerbit : Jurnal INFOMATEK - Informatika, Manajemen dan Teknologi - diterbitkan oleh Fakultas Teknik Universitas Pasundan Bandung

Penerbitan : Frekuensi terbit INFOMATEK dalam satu volume sebanyak 2 nomor per tahun pada setiap bulan : Juni dan Desember. Penerbitan perdana Volume 1 nomor 1 dimulai pada bulan Juni 1999.

Alamat Penyunting dan Tata Usaha : Fakultas Teknik Universitas Pasundan Jl. Dr. Setiabudhi No. 193 Bandung 40153, Tel. (022) 2019435,HUNTING 2019433, 2019407 Fax. (022) 2019329, *E-mail* : infomatek_ft@yahoo.com

ISSN 1411-0865

KEBIJAKAN REDAKSI

1. UMUM

Kontribusi artikel dapat diterima dari berbagai institusi pendidikan maupun penelitian atau sejenis dalam bidang informatika, manajemen dan teknologi. Manuskrip dapat dialamatkan kepada redaksi :

Dr. Bonita Anjarsari, Ir., M.Sc
Jurusan Teknologi Pangan
Fakultas Teknik – Universitas Pasundan
Jl. Dr. Setiabudhi No. 193
Bandung 40153

Manuskrip harus dimasukkan dalam sebuah amplop ukuran A4 dan dilengkapi dengan judul artikel, alamat korepondensi penulis beserta nomor telepon/fax, dan jika ada alamat e-mail. Bahasa yang digunakan dalam artikel lebih diutamakan bahasa Indonesia. Bahasa Inggris, khusus untuk bahasa asing, akan dipertimbangkan oleh redaksi.

2. ELEKTRONIK MANUSKRIP

Penulis harus mengirimkan manuskrip akhir dan salinannya dalam disket (3,5" HD) kepada alamat di atas, dengan mengikuti kondisi sebagai berikut :

a. Hanya mengirimkan manuskrip dalam bentuk 'hard copy' saja pada pengiriman pertama,
b. Jika manuskrip terkirim telah diperiksa oleh tim redaksi, dan 'Redaktur Ahli' untuk kemudian telah diperbaiki oleh penulis, kirimkan sebuah disket (3,5" HD) yang berisi salinan manuskrip akhir beserta 'hard copy'nya. Antara salinan manuskrip dalam disket dan hard copy nya harus sama,
c. Gunakan word for windows '98, IBM compatible PC sebagai media penulisan,
d. Manuskrip harus mengikuti aturan penulisan jurnal yang ditetapkan seperti di bawah ini,
e. Persiapkan 'back-up' salinan di dalam disket sebagai pengamanan.

3. PENGETIKAN MANUSKRIP

a. Pada halaman pertama dari manuskrip harus berisi informasi sebagai berikut : (I) judul, (ii) nama dan institusi penulis, (iii) abstrak yang tidak boleh lebih dari 75 kata, diikuti oleh kata kunci yang berisi maksimum 8 kata, (iv) sebuah catatan kaki dengan simbol bintang (*) pada halaman pertama ini berisi nomor telepon, fax maupun e-mail penulis sebagai alamat yang dapat dihubungi oleh pembaca.
b. Setiap paragrap baru harus dimulai pada sisi paling kiri dengan jarak satu setengah spasi. Semua bagian dalam manuskrip (antara abstrak, teks, gambar, tabel dan daftar rujukan) berjarak dua spasi. Gunakan garis bawah untuk definisi Catatan kaki (footnotes) harus dibatasi dalam jumlah dan ukuran, serta tidak harus berisi ekpresi formula matematik.
c. Abstrak harus menjelaskan secara langsung dengan bahasa yang jelas isi daripada manuskrip, tetapi bukan motivasinya. Ia harus menerangkan secara singkat dan jelas prosedur dan hasil, dan juga tidak berisi abreviasi ataupun akronim. Abstrak diketik dalam satu kolom dengan jarak satu spasi.
d. Teks atau isi manuskrip diketik dalam dua kolom dengan jarak antar kolom 0,7 cm dengan ukuran kertas lebar 19,3 cm dan panjang 26,3 cm. Sisi atas dan bawah 3 cm, sisi samping kiri dan kanan 1,7 cm.
e. Setiap sub judul atau bagian diberi nomor urut romawi (seperti I, II, …, dst), diikuti sub-sub judulnya, mulai dari PENDAHULUAN sampai dengan DAFTAR RUJUKAN. Gunakan hurup kapital untuk penulisan sub-judul.
f. Gambar harus ditempatkan pada halaman yang sama dengan teks dan dengan kualitas yang baik serta diberi nama gambar dan nomor urut. Sama halnya untuk tabel.
g. Persamaan harus diketik dengan jelas terutama untuk simbol-simbol yang jarang ditemui. Nomor persamaan harus ditempatkan di sisi sebelah kanan persamaan secara berurutan, seperti (1), (2).
h. Sebutkan hanya referensi yang sesuai dan susun referensi tersebut dalam daftar rujukan yang hanya dan telah disebut dalam teks. Referensi dalam teks harus diindikasikan melalui nomor dalam kurung seperti [2]. Referensi yang disebut pertama kali diberi nama belakang penulisnya diikuti nomor urut referensi, contoh **:** Prihartono [3], untuk kemudian bila disebut kembali, hanya dituliskan nomor urutnya saja [3].
i. Penulisan rujukan dalam daftar rujukan disusun secara lengkap sebagai berikut :

   Sumber dari jurnal ditulis :

   [1] Knowles, J. C., and Reissner, E., (1958), Note on the stress strain relations for thin elastic shells. *Journal of Mathematics and Physic,* **37**, 269-282.

   Sumber dari buku ditulis :

   [2] Carslaw, H. S., and Jaeger, J. C., (1953), *Operational Methods in Applied Mathematics, 2nd edn*. Oxford University Press, London.

j. Urutan penomoran rujukan dalam daftar rujukan disusun berurutan berdasarkan nama pengarang yang terlebih dahulu di sebut dalam manuskrip.
k. Judul manuskrip diketik dengan hurup "Arial" dengan tinggi 12, 9 untuk abstrak, dan 10 untuk isi manuskrip.

ISSN 1411-0865

INFOMATEK

Volume 15 Nomor 1 Juni 2013 JURNAL INFORMATIKA, MANAJEMEN DAN TEKNOLOGI

DAFTAR ISI

INFOMATEK
Volume 15 Nomor 1 Juni 2013

PEMANFAATAN TEKNOLOGI HONEYPOT DALAM MENINGKATKAN AVAILABILITY PADA SISTEM JARINGAN

Doddy Ferdiansyah[*)]

Program Studi Teknik Informatika
Fakultas Teknik – Universitas Pasundan

Abstrak: Tingkat ketersediaan data (Availability) merupakan hal yg mutlak yang harus disediakan oleh pihak penyedia data/informasi. Apa yang dibutuhkan oleh pengguna layanan IT harus dapat dipenuhi. Sehingga tingkat ketersediaan (availability) ini merupakan salah satu faktor yang harus diperhatikan dalam mencapai tingkat dari keamanan informasi. Honeypot merupakan sebuah teknologi yang bertindak sebagai umpan sehingga penyerang terjebak dalam melakukan serangannya. Hal ini dapat di ilustrasikan bahwa honeypot akan membuat server-server bayangan/palsu (fake) sebagai umpan. Setiap pergerakan dari jenis-jenis serangan tersebut dapat dipantau dan dianalisis hasilnya. Hasil akhir dari penelitian ini merupakan sebuah requirement (kebutuhan) teknologi honeypot yang sesuai dengan kondisi di Jurusan Teknik Informatika UNPAS.

Kata kunci: Honeypot, Availability, Server

I. PENDAHULUAN

1.1 Latar Belakang

Keamanan informasi sangat penting di era teknologi sekarang ini. Penyimpanan dan penyebaran informasi saat ini tidak lagi menggunakan media kertas, tetapi sudah banyak menggunakan teknologi komputer dan internet. Untuk menjaga keamanan informasi tersebut harus mengutamakan 3 faktor yaitu *Confidentiality, Integrity, dan Availability*.

Berbicara mengenai keamanan informasi, terutama aspek Availability, harus mendapat perhatian yang lebih terutama pada teknik-teknik pengamanannya. Banyak cara untuk dapat mencapai tingkat availability yang baik, mulai dari sistem backup, redundancy, Intrusion Detection System / Intrusion Prevention System, hingga honeypot.

Salah satu cara untuk mencegah terjadinya serangan yang mengakibatkan tingkat availability dari sebuah layanan jaringan menurun adalah dengan menggunakan honeypot.

[1]Staf pengajar Prodi Teknik Informatika UNPAS
e-mail: doddy2112@hotmail.com

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, dapat di identifikasi bahwa permasalahan yang timbul adalah bagaimana membuat rekomendasi honeypot yang sesuai dengan kondisi jaringan Teknik Informatika UNPAS saat ini. Karena banyak parameter-parameter yang harus diperhatikan dalam menggunakan honeypot di lingkukan jaringan TIF UNPAS.

1.3 Tujuan

Penilaian ini mempunyai tujuan untuk menghasilkan rekomendasi sistem honeypot yang sesuai dengan kondisi jaringan TIF UNPAS saat ini.

II. METODE PENELITIAN

Metode yang dilakukan dalam studi dan eksplorasi ini adalah sebagai berikut :

1. Studi Literatur

Mencari dan mempelajari referensi mengenai :

   a. Konsep *Honeypot*
   b. Konsep keamanan informasi
   c. Konsep Serangan (hacking)

2. Analisis

Melakukan penyelidikan atau pembelajaran lebih lanjut terhadap *honeypot*, kondisi jaringan TIF saat ini, dan tools yang cocok digunakan untuk *honeypot.*

3. Perancangan

Membuat sebuah rekomendasi rancangan yang sesuai dengan studi kasus berdasarkan dari hasil analisis.

3.1 Pemahaman Umum

Menurut buku berjudul Fundamentals of Network Security karangan John E. Canavan [1] keamanan jaringan komputer mempunyai tiga basis yang harus terpenuhi yang disebut dengan The Security Trinity yang digambarkan pada Gambar 1.

Gambar 1

The Security Trinity

1. Prevention

Prevention adalah pencegahan yang menjadi pondasi dari The Security Trinity. Pencegahan untuk menyediakan beberapa tingkat keamanan dan skema keamanan jaringan itu sendiri. Pencegahan dan skema keamanan tersebut harus memenuhi beberapa kriteria, yaitu sistem keamanan yang harus lebih mudah untuk

digunakan, lebih efisien dan biaya yang jauh lebih efektik, bukan sebaliknya.

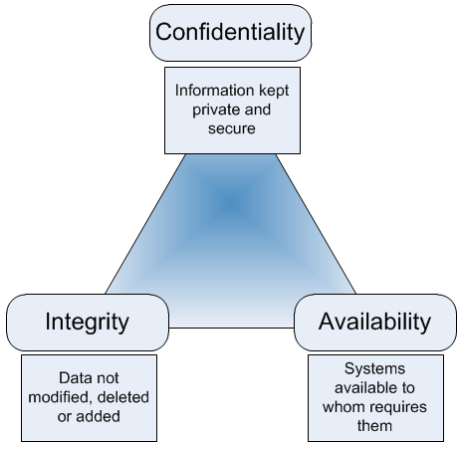
2. Detection

Setelah tahap pencegahan sudah terpenuhi, maka pencegahan tersebut harus di implementasi untuk mendeteksi masalah yang berada di jaringan. Semakin cepat bahaya tersebut terdeteksi, semakin mudah untuk melakukan perbaikan.

3. Response

Langkah terakhir adalah membuat rencana tindakan yang tepat apabila ada bahaya di jaringan. Rencana tersebut harus tertulis dan harus mengidentifikasi siapa yang bertanggung jawab atas rencana tersebut akan dilakukan.

Sedangkan menurut Chad Perrin yang dituliskan pada Techrepublic.com, CIA (confidentiality, Integrity, Availability) merupakan jantung dari keamanan informasi.



Gambar 2

CIA Triad

Pada Gambar 2 dijelaskan bahwa masing-masing dari tujuan keamanan informasi berbeda-beda.

1. Confidentiality

Merupakan bagaimana kita menjaga kerahasiaan data (privacy) dari orang-orang yang tidak mempunyai hak/wewenang terhadap data tersebut.

2. Integirity

Merupakan bagaimana kita menjamin dan memastikan keakurasian sebuah data memulai siklus hidupnya sampai dengan berakhir ketujuannya.

3. Availability

Merupakan bagaimana kita menjamin kebutuhan pengguna terhadap data tersebut dimanapun dan kapanpun, selama dibutuhkan pengguna.

3.2 Honeypot

Menurut buku berjudul Honeypots a New Paradigm to Information Security karangan R.C. Joshi & Anjali Sardana [2], Honeypot adalah sebuah teknologi yang bekerja untuk mengumpulkan pengetahuan apriori seperti tentang serangan dengan cara memikat para hacker untuk menyerang. Honeypot bertindak sebagai umpan yang memikat pengguna yang diduga akan mencoba melakukan suatu tindakan jahat dan mengantisipasinya. Setiap

pergerakan yang diduga penyerang akan dipantau dan dianalisis.

Sebuah Honeypot diatur pada jaringan untuk menjadi sasaran tunggal untuk diserang. Hal ini dirancang dengan kelemahan yang disengaja, yang terpapar pada jaringan publik. Tidak ada nilai produksi yang ditugaskan untuk honeypot, sehingga Honeypot tidak selamanya harus menerima lalu lintas yang sah. Oleh karena itu, semua lalu lintas ditujukan untuk honeypot bertujuan untuk menganalisa kemungkinan serangan yang sedang berlangsung dan dapat mengungkapkan kelemahan yang ditargetkan oleh penyerang.

Menurut tujuan keamanan, Honeypot dapat dibagi menjadi empat kategori besar, yaitu pencegahan, deteksi, reaksi atau respon dan dalam penelitian.

1. Pencegahan Honeypot mempunyai peran menghentikan penyerang dengan mengorbankan sistem produksi yang tidak langsung. Dengan begitu hacker hanya membuang-buang waktu dan sumber daya dikarenakan hacker menyerang Honeypot bukan sistem produksi yang asli.
2. Deteksi Honeypot memberikan peringatan saat serangan terjadi. Mendeteksi interaksi dengan menganalisis kegiatan sistem dan efektif dalam mendeteksi serangan baru atau tidak dikenal. Ini mengurangi resiko baik tingkat positif palsu dan tingkat negatif palsu.
3. Reaksi Honeypot memberikan lingkungan yang mirip dengan sistem produksi yang asli untuk mengambil langkah-langkah untuk menemukan penyebab dan menambal kelemahan setelah sistem produksi yang palsu yang diserang dan terganggu. Mengambil sistem produksi yang off-line untuk analisis penuh tidak selalu layak dan mungkin mendapatkan kerugian setelah intrusi terjadi. Reaksi Honeypot menghilangkan kesulitan.

Tujuan dari penelitian Honeypot adalah penelitian keamanan. Para peneliti menganalisis alat penyerang baru serta worm yang diambil dari rekaman informasi. Remedies atau solusi dapat diterapkan untuk meningkatkan keamanan sistem normal.

3.3 Denial of Service

Menurut Analisis Kelakuan Denial-of-Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas, karangan Nurwenda S, Irawan B, Irzaman [3] Denial of Service (DoS) attack merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan layanannya (denial of service) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapatbermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi “bengong”

(hang, crash), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).

Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial.

Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut.
Tujuan serangan seperti ini berakibat server korban jadi kewalahan melayani request yang terkirim dan berakhir dengan menghentikan aktivitas atau berhenti dengan sendirinya karena tak mampu melayani request. Kadang serangan yang dilakukan dengan cara ini dapat merusak atau mematikan sistem secara keseluruhan. Sistem yang diserang dapat menjadi “bengong” (hang, crash), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).
Beberapa tipe serangan Denial of Service Attack antara lain : Ping of Death, SYN Attack, Land Attack, Smurf Attack, dan UDP Flood.

1. Ping of Death

Pada kondisi normal program utility ping digunakan untuk men-cek beberapa waktu yang dibutuhkan untuk mengirimkan sejumlah data dari suatu komputer ke komputer lain, dimana panjang maksimum paket data yang dapat dikirimkan menurut spesifikasi protokol IP adalah 65.536 byte. Pada Ping of Death data yang dikirim melebihi maksimum paket yang di ijinkan menurut spesifikasi protokol IP. Ping of Death mengeksploitasi kelemahan didalam reassembly kembali fragmen paket IP. Ketika data dikirimkan ke jaringan, paket IP sering berubah menjadi potongan paket yang lebih kecil. Ping of Death akan memanipulasi offset potongan data sehingga akhirnya terjadi overlapping antara paket yang diterima di bagian penerima setelah potongan-potongan paket ini di reassembly. Konsekuensinya, pada sistem yang tidak siap akan menyebabkan sistem tersebut crash (tewas), hang (bengong) atau reboot (booting ulang) pada saat sistem tersebut menerima paket yang demikian panjang.

2. SYN Attack

Pada kondisi normal, aplikasi klien akan mengirimkan paket TCP SYN untuk mensinkronisasi paket pada aplikasi di server (penerima). Server (penerima) akan mengirimkan respond acknowledgement berupa paket TCP SYN ACK. Setelah paket TCP SYN ACK di terima dengan baik oleh klien (pengirim), maka klien (pengirim) akan mengirimkan paket ACK sebagai tanda transaksi pengiriman / penerimaan data akan di mulai. Proses ini disebut juga dengan three-way handshake
Dalam serangan SYN flood (banjir paket SYN), hacker mengirimkan paket SYN yang source addressnya telah dispoof menjadi suatu address yang tidak ada dan dikirimkan ke Server. Server

membalas dengan mengirimkan SYN/ACK ke alamat palsu (spoof), dan port yang digunakan berada pada kondisi SYN_RECV. Jika seandainya alamat Spoff (palsu) tersebut ada (terdapat system/komputer) maka akan membalas dengan paket RST karena merasa tidak memulai koneksi. Karena alamat palsu tersebut tidak ada maka koneksi yang telah dialokasikan pada port server tersebut akan berada pada keaadaan menunggu (75 detik – 23 menit). Dengan cara ini, server akan tampak seperti bengong dan tidak memproses responds dalam waktu yang lama.

3. Land Attack

Dalam LAND attack, Hacker menyerang server yang dituju dengan mengirimkan paket TCP SYN palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, Source dan Destination address dari paket dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung. Apabila serangan diarahkan kepada sistem Windows, maka sistem yang tidak diproteksi akan menjadi hang (dan bisa keluar layar biru).

4. Smurf Attack

Pada Smurf attack, hacker membanjiri router dengan paket permintaan echo Internet Control Message Protocol (ICMP) yang di kenal sebagai aplikasi ping. Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan, maka router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terjadi trafik ICMP echo respons & permintaan dalam jumlah yang sangat besar. Akibatnya terjadi ICMP trafik yang tidak hanya akan memacetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di spoof

5. UDP Flood

Pada UDP attack dengan cara spoofing, User Datagram Protocol (UDP) flood attack akan menempel pada servis UDP chargen di salah satu mesin, yang akan mengirimkan sekelompok karakter ke mesin lain, yang di program untuk meng-echo setiap kiriman karakter yang di terima melalui servis chargen. UDP Flood ini pada dasarnya mengkaitkan dua sistem tanpa disadarinya. Karena paket UDP tersebut di spoofing antara ke dua mesin tersebut, maka yang terjadi adalah banjir tanpa henti kiriman karakter yang tidak berguna antara ke dua mesin tersebut.

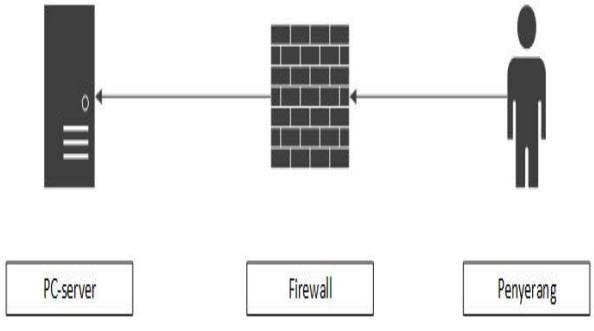
III. ANALISIS KEBUTUHAN

Dalam melakukan pengujian sistem honeypot, diperlukan beberapa perangkat keras dan perangkat lunak. Untuk perangkat keras (server) dalam penelitian ini menggunakan spesifikasi sebagai berikut :

1. Processor: Intel Pentium 4 (atau sejenisnya)
2. RAM: 512 MB

3. Harddisk: Minimun 8GB freespace
4. VGA: 1024x768 resolution

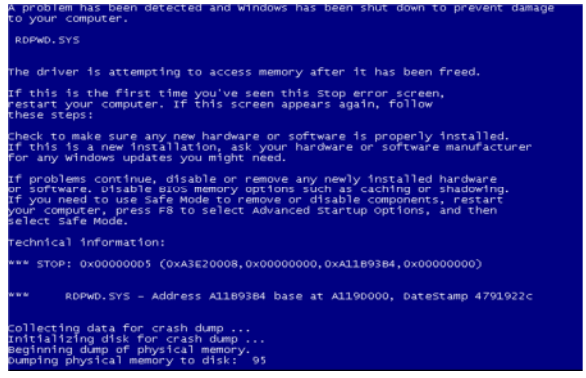
Sedangkan untuk kebutuhan perangkat lunak server honeypotnya, dalam penelitian ini menggunakan KFSensor. KFSensor adalah honeypot berbasis Windows. KFSensor termasuk kedalam low interaction honeypot yang memiliki karakteristik interaksi minimal dengan hacker dan meniru layanan palsu. Honeypots low interaction dapat membantu dalam mengidentifikasi penyerang alamat IP, Tanggal dan waktu serta port yang diserang.
Lingkup pengujian pada penelitian ini adalah mencoba melakukan serangan dengan teknik Denial Of Service (DoS) terhadap sebuah server. Dimana rancangan skenario pengujian dijelaskan pada Gambar 3.



Gambar 3
Skenario pengujian

IV. PENGUJIAN SISTEM HONEYPOT

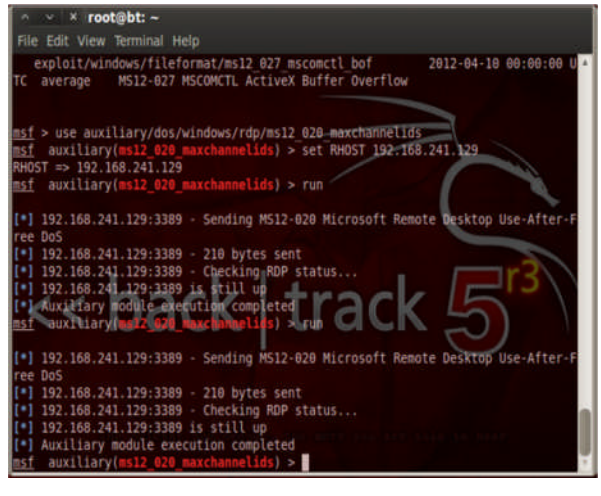
Pengujian pertama adalah kondisi sebuah server layanan tanpa menggunakan sistem honeypot.



Gambar 4
Hasil Pengujian 1

Dari hasil pada Gambar 4, server terjadi bluescreen akibat dari serangan DoS. Sehingga layanan yang diberikan oleh server menjadi terganggu.

Pada pengujian kedua, penelitian ini menggunakan sistem honeypot. Honeypot sudah dikonfigurasi terlebih dahulu dan dipasang di depan server. Hasil dari pengujian 2 dapat dilihat pada Gambar 5.



Gambar 5
Hasil Pengujian 2

Dari hasil pengujian kedua, dapat dilihat bahwa server masih aktif. Hal ini dijelaskan pada keterangan dari IP server : *192.168.241.129 is still up*

V. KESIMPULAN DAN SARAN

Setelah melakukan penelitian tentang sistem honeypot, dapat diambil kesimpulan bahwa sistem honeypot ini dapat di implementasikan pada jaringan TIF UNPAS dengan kondisi perangkat keras yang minimal. Sedangkan perangkat keras yang bisa digunakan dapat menggunakan KFSensor.

Saran yang dapat diberikan yaitu penelitian ini masih dalam tahap analisis dan pengujian dari perangkat keras dan perangkat lunak, dan masih belum selesai. Oleh karena itu, penelitian leih lanjut dapat dilakukan pada implementasi sistem honeypot pada jaringan yang lebih luas, yaitu jaringan Fakultas dan jaringan Universitas.

VI. DAFTAR RUJUKAN

[1] Canavan, John E, 2001. “Fundamentals of Network Security”, Artech House, Boston, London.

[2] Joshi, R.C., Sardana, A, 2011. “Honeypots a New Paradigm to Information Security”. Enfield, New Hampshire:Science Publishers.

[3] Nurwenda S, Irawan B, Irzaman, "Analisis Kelakuan Denial-of-Service attack (DoS attack) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas", Jurnal UNIKOM, Oktober 2004