ANALISA SERANGAN DDOS

(DISTRIBUTED DENIAL OF SERVICE)

TCP FLOOD DAN UDP FLOOD PADA HONEYD

SKRIPSI

Oleh :

GENTA PAMBUDI PUTRA WIDYASTORO
1034010011

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAWA TIMUR
2013

ANALISA SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE) TCP FLOOD DAN UDP FLOOD PADA HONEYD

SKRIPSI

Diajukan Untuk Memenuhi Sebagai Persyaratan

Dalam Memperoleh Gelar Sarjana Komputer

Program Studi Teknik Informatika

Oleh :

GENTA PAMBUDI PUTRA WIDYASTORO
NPM : 1034010011

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL
“VETERAN” JAWA TIMUR
2013

SKRIPSI

ANALISA SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE) TCP FLOOD DAN UDP FLOOD PADA HONEYD

Disusun Oleh :

GENTA PAMBUDI PUTRA WIDYASTORO
NPM : 1034010011

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal 20 Desember 2013

Pembimbing :
1.

I Made Suartana, S.Kom, M.Kom.
NPT.

2.

Achmad Junaidi, S.Kom.
NPT. 3 7811 040 199 1

Tim Penguji :
1.

Achmad Junaidi, S.Kom.
NPT. 3 7811 040 199 1

2.

Chrystia Aji Putra, S.Kom.
NPT. 3 8610 100 296 1

3.

Intan Yuniar Purbasari, S.Kom, M.Sc.
NPT. 3 8006 040 198 1

Mengetahui,
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur

Ir. Sutiyono, MT
NIP. 19600713 198703 1 001

LEMBAR PENGESAHAN

ANALISA SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE) TCP FLOOD DAN UDP FLOOD PADA HONEYD

Disusun oleh :

GENTA PAMBUDI PUTRA WIDYASTORO
NPM : 1034010011

Telah disetujui mengikuti Ujian Negara Lisan

Periode V Tahun Akademik 2013

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
I Made Suartana, S.Kom, M.Kom.	Achmad Junaidi, S.Kom.
NPT.	NPT. 3 7811 040 1991

Mengetahui,
Ketua Program Studi Teknik Informatika
Fakultas Teknologi Industri
Universitas Pembangunan Nasional ”Veteran” Jawa Timur

Dr. Ir. Ni Ketut Sari, M.T
NIP. 19650731 199203 2 001

YAYASAN KESEJAHTERAAN PENDIDIKAN DAN PERUMAHAN
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS TEKNOLOGI INDUSTRI

KETERANGAN REVISI

Kami yang bertanda tangan di bawah ini menyatakan bahwa mahasiswa berikut :

Nama : GENTA PAMBUDI PUTRA WIDYASTORO
NPM : 1034010011
Jurusan : Teknik Informatika

Telah mengerjakan REVISI SKRIPSI Ujian Lisan Gelombang V , TA 2012/2013 dengan judul:

ANALISA SERANGAN DDOS
(DISTRIBUTED DENIAL OF SERVICE)
TCP FLOOD DAN UDP FLOOD PADA HONEYD

Surabaya, 20 Desember 2013
Dosen Penguji yang memeriksa revisi

1) Achmad Junaidi, S.Kom. { }
NPT. 3 7811 040 199 1

2) Chrystia Aji Putra, S.Kom. { }
NPT. 3 8610 100 296 1

3) Intan Yuniar Purbasari, S.Kom, M.Sc. { }
NPT. 3 8006 040 198 1

Mengetahui,

Pembimbing Utama	Pembimbing Pendamping
I Made Suartana, S.Kom, M.Kom.	Achmad Junaidi, S.Kom
NPT :	NPT : 3 7811 040 199 1

KATA PEGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan segala nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi tepat pada waktunya. Serta atas limpahan rahmat yang tak terhingga penulisan laporan skripsi yang berjudul "Analisa Serangan DDoS (Distributed Denial of Service) TCP flood dan UDP flood Pada Honeyd" dapat terselesaikan.

Skripsi ini dibuat sebagai salah satu syarat memperoleh gelar sarjana komputer di jurusan teknik informatika UPN "Veteran" Jatim. Selesainya skripsi ini juga berkat dukungan semua pihak. Oleh karena itu, penulis inign mengucapkan terimakasih kepada :

1. Bapak dan Ibuku yang paling tersayang, terima kasih atas semua doa, dukungan, serta banyak hal lain yang tidak bisa di ucap satu per satu, tanpa dukungan dari kalian penulis tidak yakin bisa menyelesaikan skripsi ini tepat waktu. Terima kasih sebanyak-banyaknya atas semuanya. Dan penulis memohon doa agar setelah lulus dari perguruan tinggi dan menyandang gelar sarjana komputer, penulis mampu menjadi lebih bermanfaat bagi orang lain dan dapat membahagiakan keluarga terutama orangtua.
2. Adik-adik ku yang tersayang, terima kasih karena selama proses pengerjaan skripsi dapat berusaha mengerti keadaan, sehingga penulis mampu mengerjakan skripsi dengan tenang saat di rumah.

3. Bapak Prof. Dr. Ir. Teguh Soedarto, MP., selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Bapak Ir. Muttasim Billah, MS., selaku Wakil Dekan Fakultas Teknologi Industri UPN “Veteran ” Jawa Timur.
5. Ibu Dr. Ir. Ni Ketut Sari, MT., selaku Ketua Jurusan Teknik Informatika UPN “Veteran” Jawa Timur.
6. Bapak I Made Suartana, S.Kom, M.Kom., Selaku dosen pembimbing satu. Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
7. Bapak Achmad Junaedy, S.Kom., Selaku dosen pembimbing dua, Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
8. Sayangku Bella Chintya Dewi, terima kasih banyak telah memberiku banyak motivasi dan dukungan dari awal pengajuan skripsi hingga skripsi ini selesai, serta menjadi penghibur hati saat sedang kacau mengerjakan skripsi ini.
9. Teman-teman seperjuanganku Davi, Indra Paijo, Zen, Irsyad, Reza, Angga, Indra Primz, Handung, Abah Pringga, Mifta, Hamid, serta teman-teman seangkatan 2010 semuanya. Terima kasih karena semuanya selalu memberi motivasi dan memberi dorongan untuk penulis, tanpa kalian kuliah selama 7 semester ini tidak akan berkesan, TF angkatan 2010 Thanks for everything guys.

Penulis menyadari skripsi ini masih jauh dari kata sempurna, sehingga saran dan kritik yang membangun sangat berguna bagi penulis. Semoga laporan skripsi ini bermanfaat bagi pembaca dan semua orang yang membutuhkan referensi.

Akhirnya, penulis berharap agar penyusuan laporan ini mampu memberikan sumbangsih bagi perkembangan dan kemajuan teknik informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Surabaya, Desember 2013

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Judul	:	ANALISA SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE) TCP FLOOD DAN UDP FLOOD PADA HONEYD
Pembimbing I	:	I Made Suartana, S.Kom, M.Kom.
Pembimging II	:	Achmad Junaidi, S.Kom.
Penyusun	:	Genta Pambudi Putra Widyastoro

ABSTRAK

Kebutuhan akan teknologi informasi di era modern ini sangat besar serta dapat diaplikasikan dalam berbagai bidang. Banyak perusahaan, sekolah, dan universitas yang sudah memiliki sistem informasi berbasis online yang menggunakan layanan web dan internet dengan tujuan untuk mengembangkan lembaganya sendiri-sendiri. Namun ada juga hacker yang bertujuan untuk merusak sistem web tersebut hingga mengalami down atau tidak dapat diakses. Teknik andalan hacker untuk menyerang web korban hingga menjadi down adalah dengan menggunakan teknik DDoS (Distributed Denial of Service) TCP flood dan UDP flood. Untuk itu perlu suatu sistem yang dapat mendeteksi serangan-serangan tersebut secara tepat, cepat dan dapat mendokumentasikan serangan-serangan tersebut sehingga dapat dipelajari karakteristik serangannya.

Pada tugas akhir ini penulis menggunakan sistem honeypot untuk mendeteksi serangan DDoS TCP flood dan UDP flood. Honeypot yang digunakan adalah Honeyd. Karena informasi yang dicatat pada log Honeyd cukup lengkap maka analisa dapat dilakukan mengguanakan log tersebut. Untuk implementasi deteksi dilakukan menurut skenario yang sudah dirancang. Dan hasil dari implementasi deteksi adalah Honeyd mampu mendeteksi serangan DDoS TCP flood dan UDP flood dan dapat mendokumentasikan serangan dengan membuat file log. Dan Analisa yang dilakukan adalah membandingkan traffic normal pada protokol TCP dan UDP dengan traffic serangan DDoS TCP flood dan UDP flood sesuai skenario yang sudah dirancang serta menyamakan dengan karakteristik DDoS itu sendiri. Hasil dari analisa menunjukan bahwa terdapat perbedaan yang sangat significant dari traffic biasa dan traffic serangan. Dan setelah disamakan dengan karakteristik DDoS mulai jelas menunjukan alamat IP yang benar-benar melakukan serangan.

Kesimpulan yang diperoleh dalam tugas akhir ini adalah, bahwa Honeyd merupakan aplikasi yang efektif untuk melakukan deteksi secara realtime dan juga untuk proses analisa serangan. Selain itu Honeyd juga dapat digunakan sebagai media belajar untuk memahami karakteristik serangan.

Kata kunci: Botnet, DDoS (Distributed Denial of Service), Honeypot, Honeyd, TCP flood, UDP flood.

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Kebutuhan akan teknologi informasi di era modern ini sangat besar serta dapat diaplikasikan dalam berbagai bidang, sebab itu juga banyak pihak-pihak yang saat ini jadi bergantung pada sistem komputer sehingga sistem komputer dituntut untuk berjalan sepanjang waktu pada jaringan internet, tidak dipungkiri juga bahwa banyak virus ataupun serangan yang terjadi dari internet itu sendiri sehingga perusahaan yang menjadi korban serangan mengalami kerugian yang besar untuk membenahi jaringan yang down akibat serangan orang-orang yang tidak berjanggung jawab atau biasa disebut cracker.

DoS merupakan kependekan dari Denial of Service yang diartikan dalam bahasa Indonesia menjadi penolakan layanan, dan kepanjangan dari DDoS adalah Distibuted Denial of Service yang artinya penolakan layanan secara terdistibusi. Serangan DDoS merupakan tahap tingkat lanjut dari DoS, jika DoS hanya menyerang dengan man to man lain halnya dengan DDoS yang melakukan serangan secara bersama-sama. Cara melaksanakan serangan ini juga tidak terlalu sulit karena sudah banyak tools yang beredar di internet dan juga dengan script php dan perl.

Karena begitu merugikannya serangan DDoS terhadap suatu server maka diperlukan sebuah solusi untuk menyelesaikan permasalahan tersebut. honeypot menjadi salah satu solusi untuk deteksi serangan DDoS. Honeypot adalah suatu sistem yang di desain untuk diserang atau disusupi oleh cracker, oleh karena itu

semua trafik dari atau menuju honeypot patut di curigai sebagai aktivitas penyusupan. honeypot dapat digunakan untuk membantu administrator jaringan untuk mendeteksi trafik berbahaya ini.

Dalam tugas akhir ini, akan menganalisa tentang pendeteksian serangan dengan Honeyd sebagai aplikasi honeypot yang digunakan dalam melakukan pendeteksian serangan, dengan dilakukannya beberapa skenario yang nantinya dapat menjadi bahan analisa untuk menguji apakah serangan dapat dideteksi oleh Honeyd. untuk Serangan yang akan dilancarkan dalam tugas akhir ini adalah tipe DDoS yaitu TCP flood dan UDP flood.

1.2. RUMUSAN MASALAH

Adapun rumusan masalah yang akan di bahas dalam tugas akhir ini :

a. Bagaimana cara mengimplementasikan virtual honeypot dengan Honeyd sebagai aplikasi yang digunakan sebagai pendeteksi serangan ?
b. Bagaimana cara agar sistem keamanan virtual Honeyd agar dapat mendeteksi serangan DDOS TCP flood dan UDP flood ?
c. Bagaimana cara membuat sistem yang dapat mendokumentasikan serangan-serangan dari cracker ?
d. Bagaimana cara menganalisa serangan DDoS TCP flood dan UDP flood pada Honeyd ?

1.3. BATASAN MASALAH

Batasan masalah pengimplementasian dan analisa pada tugas akhir ini sebagai berikut :

a. Menggunakan 4 zombie komputer untuk melakukan serangan ke target yang dilakukan secara offline atau LAN (Local Area Network).
b. Serangan yang digunakan adalah DDOS TCP flood dan UDP flood.
c. Diasumsikan paket serangan telah dialihkan ke Honeyd.
d. Menggunakan Honeypot low interaction.
e. Sistem diuji secara virtual.

1.4. TUJUAN TUGAS AKHIR

Adapun tujuan dari tugas akhir ini adalah :

a. Dapat mengimplementasikan virtual honeypot dengan Honeyd pada sistem yang diinginkan.
b. Membuat sistem keamanan virtual Honeyd agar dapat mendeteksi serangan DDOS TCP flood dan UDP flood.
c. Dapat mendokumentasikan serangan-serangan yang di lakukan oleh cracker.
d. Melakukan analisa terhadap serangan DDoS TCP flood dan UDP flood menggunakan Honeyd.

1.5. MANFAAT TUGAS AKHIR

Manfaat yang di peroleh dari pengimplementasian dan analisa honeypot antara lain :

a. Bagi penulis, bermanfaat untuk menerapkan pengetahuan yang diperoleh selama menempuh ilmu di bangku perkuliahan.

b. Bagi mahasiswa, bermanfaat untuk mengenal lebih jauh tentang ilmu keamanan jaringan terutama honeypot.
c. Bagi pembaca, bermanfaat menambah informasi tentang honeypot, juga sebagai bahan referensi dan pengembangan lebih lanjut.

1.6. SISTEMATIKA PENULISAN

Sistematika penulisan tugas akhir ini akan membantu memberikan informasi tentang tugas akhir yang dijalankan dan agar penulisan laporan ini tidak menyimpang dari batasan masalah yanga ada, sehingga susunan laporan ini sesuai dengan apa yang diharapkan. Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi mengenai gambaran umum penelitain tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka berisi tentang berbagai konsep dasar penyerangan, honeypot, serta analisa yang digunakan dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal-hal yang berguna dalam proses analisis permasalahan.

BAB III METODE PENELITIAN

Metode tugas akhir ini berisi tentang rancangan jaringan, rancangan serangan-serangan, rancangan pendeteksian terhadap serangan-serangan yang dilakukan, dan konfigurasi-konfigurasi yang digunakan dalam mendeteksi, serta metode-metode lain yang digunakan untuk menyelesaikan tugas akhir ini.

BAB IV HASIL DAN PEMBAHASAN

Dalam implementasi sistem ini berisi tentang hasil dan pembahasan tentang beberapa konfigurasi yang dilakukan pada bab sebelumnya untuk mendeteksi serangan-serangan, serta di lakukannya analisa dengan menggunakan beberapa skenario yang di lakukan pada metode pendeteksian terhadap serangan-serangan yang di lancarkan.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran dari penulis yang sudah diperoleh dari hasil penulisan tugas akhir.