

TUGAS AKHIR

**ANALISIS DAN IMPLEMENTASI HONEY POT MENGGUNAKAN
KIPPO SEBAGAI PENUNJANG KEAMANAN JARINGAN**



TRI HANDOYO SAPUTRO
1010651077

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2015**

PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : TRI HANDOYO SAPUTRO
NIM : 10 1065 1077
Institusi : S1 Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Jember.

Menyatakan bahwa Tugas Akhir yang berjudul **“ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN KIPPO SEBAGAI PENUNJANG KEAMANAN JARINGAN”** adalah benar-benar hasil karya sendiri, bukan merupakan Tugas Akhir orang lain baik sebagian maupun keseluruhan kecuali dalam bentuk kutipan yang telah disebutkan sumbernya. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenar-benarnya, tanpa ada tekanan dan paksaan dari pihak manapun. Saya bersedia mendapat sanksi akademik di kemudian hari jika pernyataan ini tidak benar.

Jember, 28 Juli 2015
Yang menyatakan,

Tri Handoyo Saputro
NIM. 10 1065 1077

HALAMAN PENGESAHAN

**ANALISIS DAN IMPLEMENTASI HONEYPOT MENGGUNAKAN
KIPPO SEBAGAI PENUNJANG KEAMANAN JARINGAN**

Oleh :

**TRI HANDOYO SAPUTRO
1010651077**

Proyek Akhir Ini Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar
Sarjana Komputer (S.Kom)
di
Universitas Muhammadiyah Jember

Disahkan oleh :

Dosen Penguji I

Dosen Pembimbing I

Lutfi Ali Muharom, S.Si M.Si
NPK : 12 03 375

Triawan Adi Cahyanto, S.Kom, M.Kom
NPK : 12 03 719

Dosen Penguji II

Dosen Pembimbing II

Henny Wahyu S, S.Kom
NPK : 08 11 500

Hardian Oktavianto, S.Si
NPK : 12 03 715

Jember, 28 Juli 2015
Mengetahui,

Dekan Fakultas Teknik

Ketua Program Studi Teknik Informatika

Ir. Rusgianto, M.M
NPK : 131 863 867

Agung Nilogiri, ST, M.Kom
NIP : 19770330 200501 1 002



“Jangan pernah berfikir apa yang kamu dapat dari Negaramu, tapi berfirlah apa yang akan kau berikan terhadap Negaramu”

(Penulis)

“Setinggi – tinggi ilmu, semurni – murni tauhid dan
sepintar – pintar siasat ”

(Haji Oemar Said Cokroaminoto)

“COGITO ERGO SUM”

Aku berfikir Maka Aku Ada

(Rene Descartes)

HALAMAN PERSEMBAHAN

Rasa syukur yang tak terhingga penulis panjatkan kepada Allah SWT, sholawat serta salam tercurah limpahkan kepada Nabi Besar Muhammad SAW, dengan terselesaikannya skripsi

Skripsi ini penulis persembahkan untuk :

1. Keluarga penulis Ayah, Ibu serta kakak - kakak yang selalu memberikan doa dan mendukung saya selama ini.
2. Fatimatul Hasanah orang yang selalu setia menemani dan membantu disaat penulis mengalami kesulitan.
3. Rekan-rekan Angkatan 2010 yang selalu memberikan motivasi kepada penulis. Khususnya (M. Fakhur A, Abdul Ajis, Agil Wahyu Royan, Muhammad Gunarso, Emil Salim, Hafid Hadistira, Herman Evfendi, Vidiyanto) semua kenangan dan kebersamaannya akan selalu penulis ingat.
4. Teman-teman “Semeru Coffe” khususnya Fuad, Ulum, Hadi, Noval, Jhony, Dadang, Rudiansyah, Jono, Udin, Ufi, Nyak, Rico, Agung, Agung Purnomo, Ghofur, Yossi, Riki ndo.
5. Bapak Ir. Rusgianto, M.M selaku Dekan Fakultas Teknik Universitas Muhammadiyah Jember. Bapak Agung Nilogiri, S.T, M.Kom selaku Kepala Program Studi Teknik Informatika.
6. Bapak Hardian Oktavianto, S.Si dan Bapak Triawan Adi Cahyanto S.Kom, M.Kom yang meluangkan waktunya untuk membimbing Bapak Lutfi Ali Muharrom, S.Si, M.Si dan Henny Wahyu S.Kom yang telah menguji.
7. Bapak dan Ibu Dosen Fakultas Teknik Universitas Muhammadiyah Jember.
8. Sahabat – sahabat Pergerakan Mahasiswa Islam Indonesia (PMII) khususnya Komisariat Universitas Muhammadiyah Jember yang selalu memberikan spirit pergerakannya untuk penulis.
9. Almamater yang penulis banggakan.

KATA PENGANTAR



Puji syukur kita panjatkan kehadirat Allah SWT atas rahmat dan karuniaNya yang telah dilimpahkan sehingga kami bisa menyelesaikan Laporan Tugas Akhir yang berjudul **“Analisis dan Implementasi Honeypot Menggunakan Kippo Sebagai Penunjang Keamanan Jaringan”**. Penyusunan Laporan Tugas Akhir Disusun Untuk Melengkapi dan Memenuhi Syarat Kelulusan Program Strata 1 Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember dan juga sebagai syarat untuk memperoleh Gelar Sarjana Komputer (S.Kom).

Ungkapan terimakasih ditujukan kepada dosen pembimbing yang telah bersedia membimbing dan memberikan pengarahan dalam penyusunan skripsi ini sehingga skripsi ini terselesaikan dengan baik. Dalam menyelesaikan skripsi ini, peneliti telah berusaha semaksimal mungkin, supaya mendapat hasil yang baik sesuai dengan arti penulisan ilmiah. Peneliti menyadari bahwa penulisan skripsi ini belum sempurna dan baru merupakan suatu karya tulis dengan kemampuan yang terbatas. Semoga bermanfaat bagi para pembaca.

Terselesaikannya penyusunan skripsi ini, maka penulis mengucapkan terima kasih kepada semua pihak atas bantuannya. Semoga segala bantuan dan bimbingan yang telah diberikan kepada penulis mendapat imbalan yang sesuai dari Allah SWT.

Jember, 28 Juli 2015
Hormat Kami,

Tri Handoyo Saputro
NIM : 1010651077

DAFTAR ISI

HALAMAN SAMPUL

HALAMAN PERNYATAAN.....	i
HALAMAN PENGESAHAN.....	ii
ABSTRAK	iii
ABSTRACT	iv
MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xii

BAB I PENDAHULUAN

1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan	3
1.5 Manfaat	3

BAB II TINJAUAN PUSTAKA

2.1 Jaringan Komputer	4
2.2 Pengertian Honeypot.....	5
2.2.1 Low Interaction Honeypot	5
2.2.2 High Interaction Honeypot	6
2.3 Pengertian Kippo.....	8

2.4 Pengertian Server	8
2.4.1 Web Server.....	9
2.4.2 Ftp Server.....	10
2.4.3 Telnet Server.....	12
2.4.4 SSH Server.....	13
2.5 Pengertian nmap.....	13
2.6 Pengertian BruteForce.....	15
2.7 Pengertian Medusa.....	16
2.8 Penelitian Terdahulu	17
2.8.1 Perancangan dan Implementasi Honeypot sebagai penunjang Keamanan Jaringan Terhadap Serangan BruteForce	17
2.8.2 Analisa dan Implementasi Honeypot Menggunakan Honeyd Sebagai Penunjang Keamanan Jaringan.....	17

BAB III METODE PENELITIAN

3.1 Studi Literatur	19
3.2 Analisis dan Perancangan Honeypot.....	19
3.2.1 Analisis	19
3.2.2 Perancangan Honeypot	20
3.2.3 Topologi Jaringan	21
3.3 Implementasi Sistem	22
3.4 Pengujian dan Pengambilan data	22

BAB IV HASIL DAN PEMBAHASAN

4.1 Instalasi Sistem	23
4.1.1 Konfigurasi Kippo	23
4.1.2 Menjalankan Kippo.....	25
4.1.3 Instalasi Aplikasi Pendukung.....	25

4.2 Pengujian Serangan.....	27
4.2.1 Pengujian Scanning Host dan Port.....	27
4.2.2 Pengujian Serangan Bruteforce.....	29
4.3 Analisis Aktifitas Serangan Dengan Kippo-Graph.....	31
4.4 Analisis Kinerja Honeypot.....	36
BAB V KESIMPULAN DAN SARAN	
5.1 Kesimpulan	37
5.1 Saran.....	37
DAFTAR PUSTAKA	38
BIODATA PENULIS.....	39

DAFTAR GAMBAR

Gambar 2.1 Metode Brute Force.....	16
Gambar 3.1 Kerangka Konsep Penelitian	18
Gambar 3.2 Perancangan Honeypot.....	20
Gambar 3.3 Topologi Jaringan.....	21
Gambar 4.1 Konfigurasi Kippo.....	24
Gambar 4.2 Tampilan kippo saat dijalankan.....	25
Gambar 4.3 Instalasi Nmap.....	26
Gambar 4.4 Instalasi Medusa.....	26
Gambar 4.5 Scanning Host dengan Nmap	27
Gambar 4.6 Proses nmap pada 192.168.1.101	28
Gambar 4.7 Bruteforce ssh oleh attacker pertama	29
Gambar 4.8 Bruteforce ssh oleh attacker kedua.....	30
Gambar 4.9 Tampilan awal Kippo-Graph.....	31
Gambar 4.10 Tampilan Kippo-Graph tidak ada aktivitas	31
Gambar 4.11 Tampilan Kippo-Graph ada aktivitas	32
Gambar 4.12 Tampilan Kippo-Ip sebelum serangan	32
Gambar 4.13 Tampilan Kippo-Ip setelah serangan.....	33
Gambar 4.14 Tampilan log web interfaces Graph-Gellery sebelum serangan	33
Gambar 4.15 Tampilan log web interfaces Graph-Gellery setelah serangan.....	34
Gambar 4.16 Top 10 Password	34
Gambar 4.17 Top 10 Username	35
Gambar 4.18 Grafik IP Address Attacker	35
Gambar 4.19 Success ratio attacker	36

DAFTAR TABEL

Tabel 2.1 Perbandingan Honeypot Low Interartion dengan High Interaction	7
Tabel 4.1 Fungsi Perintah yang ada dimedusa.....	30

DAFTAR PUSTAKA

- Eka Pramudita, Krisnaldi (2010) “Brute Force Attack dan penerapannya pada password cracking” Institut Teknologi Bandung. Indonesia
- Hadistira, Hafid (2015) “Analisa dan Implementasi Honeypot Menggunakan Honeyd Sebagai Penunjang Keamanan Jaringan” Universitas Muhammadiyah Jember.
- Muh Masruri Mustofa, (2013) “*Penerapan Sistem Keamanan Honeypot Dan Ids Pada Jaringan Nirkabel (Hotspot)*”, Program Studi Teknik Informatika Universitas Ahmad Dahlan, Yogyakarta
- Nurhasanah Umayah, “*Perancangan dan Implementasi Honeypot pada Virtual Private Server sebagai Penunjang Keamanan Jaringan*” Politeknik Telkom.
- Sugeng, W. (2010). Jaringan Komputer dengan TCP/IP. Bandung: Modula
- Syafrizal, Melwin (2005) “Pengantar Jaringan Komputer” . Yogyakarta: Penerbit Andi
- Utdirartatmo, F. (2005). Menjebak Hacker dengan Honeypot. Yogyakarta: Andi.
- foofus, “Medusa Parallel Network Login Auditor” Diakses tanggal 07 Mei 2015.
<http://foofus.net/goons/jmk/medusa/medusa.html>
- Virtual Private Server, Diakses Januari 22, 2015 dari <http://www.indonic.net/vps-hosting/>
- Wikipedia, “Nmap(Nmap Security Scanner)” Diakses tanggal 07 Mei 2015.
<http://en.m.wikipedia.org/wiki/Nmap>

BIODATA PENULIS



Data Pribadi

Nama : Tri Handoyo Saputro
NIM : 10 1065 1077
Tempat/Tanggal Lahir : Jember, 27 Juni 1992
Jurusan : Teknik Informatika
Alamat Asal : Jl. Hasanudin No.06 RT:01 RW:11 Balung
Kulon, Balung - Jember
Alamat di Jember : Jl. Semeru Raya Jember
No. Telp/HP : 085 749 777 468
E-mail : akun.lawas@gmail.com

Pendidikan

1998 - 2004 : SD Negeri 04 Balung Kulon
2004 - 2007 : SMP Baitul Arqom Balung
2007 - 2010 : SMA Baitul Arqom Balung
2010 - 2015 : Universitas Muhammadiyah Jember