

**PERANCANGAN DAN IMPLEMENTASI HONEYPOT SEBAGAI
PENUNJANG KEAMANAN HALAMAN WEB LOGIN TERHADAP
SERANGAN BRUTE-FORCE**

**SKRIPSI
KONSENTRASI KOMPUTASI BERBASIS JARINGAN**

Diajukan untuk memenuhi persyaratan mencapai gelar Sarjana Komputer



Disusun Oleh:
JOHAN ISWARA

NIM. 0810680006

**KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS BRAWIJAYA
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER**

MALANG

2013

LEMBAR PERSETUJUAN

**PERANCANGAN DAN IMPLEMENTASI *HONEYPOT* SEBAGAI
PENUNJANG KEAMANAN HALAMAN *WEB LOGIN* TERHADAP
SERANGAN *BRUTE-FORCE* SKRIPSI**

KONSENTRASI KOMPUTASI BERBASIS JARINGAN

Untuk memenuhi sebagian persyaratan untuk mencapai gelar Sarjana Komputer



Disusun Oleh:

JOHAN ISWARA

NIM. 0810680006

Telah diperiksa dan disetujui oleh :

Dosen Pembimbing I

Dosen Pembimbing II

Kasyful Amron, ST., M.Sc
NIP. 19750803 200312 1 003

Eko Sakti P., S.Kom., M.Kom.
NIP. 860805 06 1 1 0252

LEMBAR PENGESAHAN

**PERANCANGAN DAN IMPLEMENTASI *HONEYPOT* SEBAGAI
PENUNJANG KEAMANAN HALAMAN *WEB LOGIN* TERHADAP
SERANGAN *BRUTE-FORCE***

SKRIPSI

Diajukan untuk memenuhi persyaratan mencapai gelar Sarjana Komputer

Disusun Oleh :

Johan Iswara

NIM. 0810680006

Skripsi ini telah diuji dan dinyatakan lulus pada
tanggal 5 Desember 2013

Penguji I

Penguji II

Ir. Heru Nurwasito, M.Kom.
NIP. 196504021990021001

Sabriansyah Rizqika A., ST., M.Eng
NIP. 82080906110084

Penguji III

Adharul Muttaqin, ST., MT.
NIP. 19760121 200501 1 001

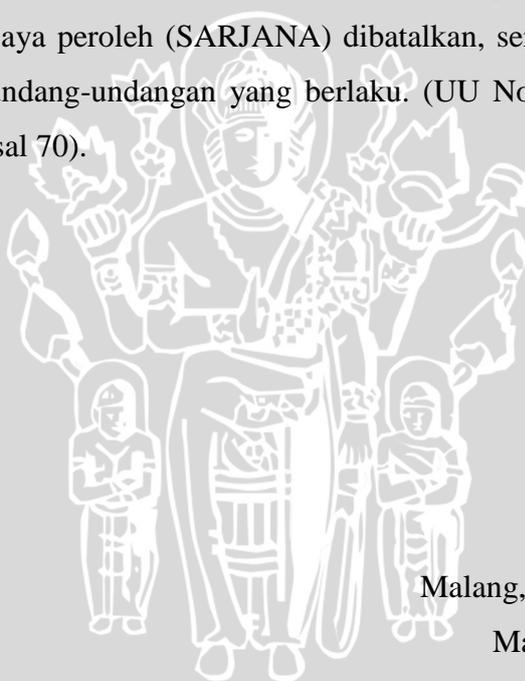
Mengetahui
Ketua Program Studi Teknik Informatika

Drs. Marji, MT
NIP. 19670801 199203 1 001

**PERNYATAAN
ORISINALITAS SKRIPSI**

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah SKRIPSI ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam naskah SKRIPSI ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia SKRIPSI ini digugurkan dan gelar akademik yang telah saya peroleh (SARJANA) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku. (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).



Malang, 8 Desember 2013
Mahasiswa,

Johan Iswara
NIM.0810680006

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan skripsi yang berjudul “Implementasi Dan Perancangan Honeypot Sebagai Penunjang Keamanan Halaman Web Login Terhadap Serangan Brute-Force“ dengan baik.

Penulisan laporan skripsi ini diajukan untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Komputer dan merupakan salah satu syarat yang harus ditempuh oleh setiap mahasiswa Teknik Informatika Universitas Brawijaya Malang.

Penyusunan laporan skripsi ini dapat terlaksana dengan baik karena adanya bantuan secara langsung maupun tidak langsung dari pihak tertentu, diantaranya :

1. Bapak Kasyful Amron., S.T., M.Sc. dan Eko Sakti Pramukantoro., S.Kom., M.Kom. selaku pembimbing dalam menyelesaikan laporan skripsi ini.
2. Orang tua yang telah memberikan dukungan moral dan material.
3. Teman teman yang telah membantu memberi saran dan kritik atas laporan ini.

Penulis menyadari bahwa laporan skripsi ini masih banyak kekurangan dan jauh dari sempurna karena keterbatasan materi dan pengetahuan yang dimiliki penulis. Akhirnya semoga laporan skripsi ini dapat bermanfaat dan berguna bagi pembaca terutama mahasiswa Teknik Informatika Universitas Brawijaya.

Malang, 4 November 2013

Penulis

ABSTRAK

Johan Iswara. 2013. Perancangan dan Implementasi Honeypot Sebagai Penunjang Keamanan Halaman Web Login Terhadap Serangan Brute-Force. Skripsi Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya. Pembimbing: Kasyful Amron., S.T., M.Sc. dan Eko Sakti Pramukantoro., S.Kom., M.Kom.

Pemanfaatan jaringan internet untuk memudahkan komunikasi antar manusia di dunia sudah sangat meluas. Diperlukan suatu usaha untuk menjamin keamanan informasi yang ada agar informasi tersebut tidak “jatuh” pada pihak yang salah. Salah satu cara untuk menanggulangi ancaman yang ada yaitu telah dikembangkan suatu *honeypot* jenis *kippo* yang mampu memberikan emulasi sistem palsu. Berdasarkan penelitian yang ada, diketahui bahwa kemampuan emulasi oleh *kippo* hanya mampu diterapkan pada port SSH saja. Kemudian pada penelitian ini dikembangkan pada port HTTP untuk memberikan emulasi web server terhadap pelaku serangan *Brute-force*. Serangan *Brute-force* bekerja bertujuan untuk mendapatkan *username* dan *password* yang digunakan dalam proses login. Sistem bekerja dengan melakukan pengecekan terhadap paket yang diterima pada port HTTP, yang kemudian dilakukan analisa terhadap kriteria dari serangan brute force. Jika koneksi yang terjadi tergolong dalam serangan brute force, maka sistem akan merespon dengan halaman emulasi, jika tidak maka sistem akan merespon dengan halaman asli. Skenario pengujian yang dilakukan adalah melakukan proses serangan *brute-force* dengan jumlah yang berbeda-beda pada setiap skenario. Selain itu juga memberikan nilai yang berbeda pada pengaturan sistem. Skenario tersebut digunakan untuk mendapatkan akurasi sistem dalam mengenali serangan *brute-force* maupun *non-brute-force* pada port HTTP. Dari skenario tersebut diperoleh hasil akurasi pengujian sebesar 97,22% dalam mengenali paket *non-brute-force* dan akurasi pengujian sebesar 100% dalam mengenali paket *brute-force*.

Kata Kunci: *Honeypot, Port HTTP, Brute-force*

ABSTRACT

Johan Iswara. 2013. Perancangan dan Implementasi Honeypot Sebagai Penunjang Keamanan Halaman Web Login Terhadap Serangan Brute-Force. Skripsi Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya. Pembimbing: Kasyful Amron., S.T., M.Sc. dan Eko Sakti Pramukantoro., S.Kom., M.Kom.

In nowadays, utilization of the Internet to facilitate communication between people in the world have been very widespread. Required an effort to ensure the safety of existing information so that the information does not "fall" to intruder. One solution to deal with the threat is develop a Kippo honeypot that can give fake emulation system to the intruder. Based on existing research, known that the ability of emulation by Kippo only able to be applied to the SSH port. Then in this research was developed a honeypot tha have work system just like kippo honeypot but will be applied on the HTTP port for web servers to provide emulation Brute-force attack perpetrators. Brute-force attacks work aims to obtain a username and password that is used in the login process. System in this research worked by checking the packet received on the HTTP port, which is then analyzed against the criteria of a brute force attack. If the connection is happening belonging in a brute force attack, then the system will respond with fake web data, but if not then the system will respond with the true web data. Scenario testing is to do the brute-force attack with a different number on each scenario. It also gives a different value to the system settings. The scenarios are used to get the system accuracy in recognizing brute-force attacks and non-brute-force the HTTP port. From the scenarios that have been done, obtained 97.22% accuracy for the system to recognize the non-brute-force packet and obtained 100% accuracy for the system to recognize the brute-force packet.

Keyword: Honeypot, Port HTTP, Brute-force