PENDETEKSIAN SERANGAN SYN FLOOD PADA JARINGAN KOMPUTER LOKAL MENGGUNAKAN ALGORITMA NAÏVE BAYES

SKRIPSI

OLEH :
DANU BUDI WISUDANA PRABA
(0510963014-96)

PROGRAM STUDI ILMU KOMPUTER
JURUSAN MATEMATIKA FAKULTAS MIPA
UNIVERSITAS BRAWIJAYA
2012


UNIVERSITAS BRAWIJAYA

LEMBAR PENGESAHAN SKRIPSI

PENDETEKSIAN SERANGAN SYN FLOOD PADA JARINGAN KOMPUTER LOKAL MENGGUNAKAN ALGORITMA NAÏVE BAYES

oleh:
Danu Budi Wisudana Praba
0510963014-96

Setelah dipertahankan di depan Majelis Penguji pada tanggal 14 Juni 2012 dan dinyatakan memenuhi syarat untuk memperoleh gelar Sarjana Komputer dalam bidang Ilmu Komputer

Pembimbing I,	Pembimbing II,
Lailil Muflikhah, S.Kom, MSc	Dany Primanita Kartikasari, ST
NIP. 197411132005012001	NIP. 197711162005012003

Mengetahui,
Ketua Jurusan Matematika
Fakultas MIPA Universitas Brawijaya

Dr. Abdul Rouf Alghofari, M.Sc.
NIP. 196709071992031001

UNIVERSITAS BRAWIJAYA

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	**:**	Danu Budi Wisudana Praba
NIM	**:**	0510963014-96
Jurusan	**:**	Matematika
Program Studi	**:**	Ilmu Komputer
Penulis tugas akhir berjudul	**:**	Pendeteksian serangan Syn Flood pada Jaringan Komputer Lokal Menggunakan Algoritma *Naïve Bayes*

Dengan ini menyatakan bahwa :

1. **Isi dari Skripsi yang saya buat adalah benar-benar karya sendiri dan tidak menjiplak karya orang lain, selain nama-nama yang termaktub di isi dan tertulis di daftar pustaka dalam Skripsi ini.**
2. **Apabila dikemudian hari ternyata Skripsi yang saya tulis terbukti hasil jiplakan, maka saya akan bersedia menanggung segala resiko yang akan saya terima.**

Demikian pernyataan ini dibuat dengan segala kesadaran.

Malang, 13 Juni 2012
Yang menyatakan,

Danu Budi Wisudana Praba
NIM. 0510963014

PENDETEKSIAN SERANGAN SYN FLOOD PADA JARINGAN KOMPUTER LOKAL MENGGUNAKAN ALGORITMA NAÏVE BAYES

ABSTRAK

Syn flood adalah salah satu jenis serangan *Denial of Service* (*DoS)* yang memanfaatkan mekanisme *TCP three way handshake* sehingga menyulitkan untuk membedakan dengan koneksi *TCP* legal karena memiliki karakteristik yang sama dengan koneksi *TCP* legal. *Syn flood* memalsukan alamat pengirim paket sehingga membuat target berada dalam *half opening state* karena menunggu respon dari pengirim paket. Hal ini membuat target membuang *resource* percuma dan bisa menyebabkan target dalam kondisi *denied service* jika diserang terus menerus.

Naïve Bayes yang dikenal luas sebagai salah satu algoritma yang banyak melakukan pengklasifikasian spam email diimplementasikan untuk melakukan pendeteksian serangan *syn flood* pada jaringan komputer lokal. Dataset yang digunakan dibangkitkan di lab dengan dua jenis dataset yaitu satu dataset latih dan tiga dataset uji. Dataset uji memiliki *pattern* berbeda dengan dataset latih dan dataset uji lainnya. Setiap dataset uji dideteksi satu per satu untuk mengetahui tingkat akurasi dari algoritma n*aïve bayes. ROC Curve* digunakan untuk melakukan analisa akurasi pendeteksian serangan syn flood oleh algoritma n*aïve bayes.*

Pengujian menunjukkan bahwa Dataset uji satu menghasilkan *false alarm rate* 0.025, Dataset uji dua menghasilkan *false alarm rate* 0.2, dan Dataset uji tiga menghasilkan *false alarm* rate 0.0588. *False Positive* terjadi pada ketiga dataset uji, hal ini bisa dipahami dengan melihat ROC Curve dimana kondisi positif diklasidikasikan lebih baik oleh n*aïve bayes* daripada kondisi negatif, hal ini membuat *naïve bayes* memiliki kecenderungan kesalahan dalam menentukan kondisi negatif yang diklasifikasikan sebagai positif.

SYN FLOOD ATTACK DETECTION IN LOCAL AREA NETWORK USING NAÏVE BAYES CLASSIFIER

Abstract

Syn flood is one of the Denial of Service network attack which uses TCP three way handshake mechanism making so that it is hard to distinguish with legal TCP connection because syn flood has same characteristic with legal TCP connection. Syn flood forges the address of package sender so it makes the target be in half open state because the target waiting the response from the forged address sender.

Naive bayes which widely known as one of the spam classifier, implemented to classify syn flood attack in local area network. The dataset generated in network laboratory. It contains two type of data: training data and test data. Test data has different pattern of connection compared with the training data.Each test data is tested one by one to determine the accuracy level of naïve bayes algorithm. ROC Curve is used to analyze the accuracy of the detection of syn flood attack by naïve bayes algorithm.

The Testing showed that the first test data produced false alarm rate 0.025, the second test data produced false alarm rate 0.2, and the third test data produced false alarm rate 0.0588. False positive occurred in all three test data. This condition could be understood by looking at the ROC Curve which the positive condition classified better by naïve bayes than the negative one. This condition could made naïve bayes error in determining the negative conditions that are classified as positive.

KATA PENGANTAR

Alhamdulillahi rabbil 'alamin. Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas segala rahmat dan limpahan hidayahNya, penulis masih dapat belajar dan mengerjakan skripsi yang berjudul "*Pendeteksian serangan Syn Flood pada jaringan komputer menggunakan algoritma Naïve Bayes*".

Skripsi ini disusun dan diajukan sebagai syarat untuk memperoleh gelar sarjana pada program studi Ilmu Komputer, jurusan Matematika, fakultas MIPA, Universitas Brawijaya.

Dalam penyelesaian tugas akhir ini, penulis telah mendapat begitu banyak bantuan baik moral maupun materiil dari banyak pihak. Atas bantuan yang telah diberikan, penulis ingin menyampaikan penghargaan dan ucapan terima kasih kepada :

1. Ayahanda Bambang Budiono, S.Pd dan Ibunda Supraptiningsih, S.Pd, MMPd. yang telah memberikan cinta, kasih sayang, dukungan, semangat, dan doa yang tiada henti.
2. Lailil Muflikhah, S.Kom, MSc selaku pembimbing I dan Dany Primanita K, ST selaku pembimbing II. Terima kasih atas semua waktu dan bimbingan yang diberikan.
3. Segenap bapak dan ibu dosen yang telah mendidik dan mengamalkan ilmunya kepada penulis.
4. Segenap staf dan karyawan di Jurusan Matematika Fakultas MIPA Universitas Brawijaya.
5. Sigit Adinugroho, Mahendra Data, Iwan, Rio Rosdianto, Rakhmadany, Bu Novi, Pak Raden Arief, Pak Harry Soekotjo, dan teman-teman TIK UB yang telah memberikan dukungan, semangat, bantuan, dan doa yang luar biasa kepada penulis.
6. Sahabat-sahabat ilkomers angkatan 2005 dan seluruh warga Program Studi Ilmu Komputer Universitas Brawijaya.
7. Pihak lain yang telah membantu terselesaikannya skripsi ini yang tidak bisa penulis sebutkan satu-persatu. .

Penulis sadari bahwa masih banyak kekurangan dalam laporan ini disebabkan oleh keterbatasan kemampuan dan pengalaman. Oleh karena itu Penulis sangat menghargai saran dan kritik yang sifatnya membangun demi perbaikan penulisan dan mutu isi skripsi ini untuk kelanjutan penelitian serupa di masa mendatang.

Penulis berharap semoga skripsi ini dapat memberikan manfaat

kepada pembaca dan bisa diambil manfaatnya, baik oleh Penulis selaku mahasiswa maupun pihak-pihak lain yang tertarik untuk menekuni pengembangan Keamanan Jaringan Komputer.

Malang, Juni 2012

Penulis.

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR KODE PROGRAM

Halaman