SKRIPSI

IMPROVING INTRUSION DETECTION SYSTEM TERHADAP SERANGAN *PROBE* MENGGUNAKAN *HONEYPOT* DI *SMALL BOARD COMPUTER*

OLEH :

ARDIN FEBRIANDA
09011181621008

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

IMPROVING INTRUSION DETECTION SYSTEM TERHADAP SERANGAN *PROBE* MENGGUNAKAN *HONEYPOT* DI *SMALL BOARD COMPUTER*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

ARDIN FEBRIANDA
09011181621008

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

HALAMAN PENGESAHAN

IMPROVING INTRUSION DETECTION SYSTEM TERHADAP SERANGAN *PROBE* MENGGUNAKAN *HONEYPOT* DI *SMALL BOARD COMPUTER*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

ARDIN FEBRIANDA
09011181621008

Inderalaya, 30 Desember 2020

Mengetahui,

Pembimbing I	Pembimbing II
Deris Stiawan, Ph. D	**Ahmad Heryanto, S.Kom., M.T**
NIP. 197806172006041002	**NIP. 198701222015041002**

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Rabu

Tanggal : 30 Desember 2020

Tim Penguji :

1. Ketua : Ahmad Fali Oklilas, S.T.,M.T.

2. Sekretaris : Aditya Putra Perdana P, M.T.

2. Anggota : Huda Ubaya, M.T.

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Ardin Febrianda

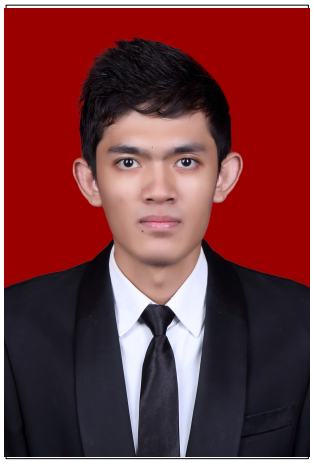
NIM : 09011181621008

Judul : *Improving Intrusion Detection System* Terhadap Serangan *Probe* Menggunakan *Honeypot* di *Small Board Computer*

Hasil Pengecekan *Software iThenticate/Turnitin* : 9 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / *plagiat*, Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



Inderalaya, 08 Januari 2021

Ardin Febrianda

NIM. 09011181621008

HALAMAN PERSEMBAHAN

Katakanlah, "Wahai hamba-hamba-Ku yang melampaui batas terhadap diri mereka sendiri! Janganlah kamu berputus asa dari rahmat Allah. Sesungguhnya Allah mengampuni dosa-dosa semuanya. Sungguh, Dialah Yang Maha Pengampun, Maha Penyayang. (Q.s. Az – Zumar : 53)

Tugas Akhir ini kupersembahkan untuk :

- ***Ayahandaku (Sunardi) dan Ibundaku (Heny Nuraini) yang tercinta, serta saudara - saudariku yang telah memberikan semangat kepada saya dan telah membantu saya baik itu dalam bentuk materi maupun batin serta doa yang hingga akhirnya dapat menyelesaikan studi saya.***
- ***Teman – teman kelas SKA 2016 dari semua yang saya kenal sejak semester 1 sampai dengan akhir ini, semoga kita semua sukses dan berhasil dalam kehidupan dunia maupun akhirat yang kelak akan dilalui.***
- ***Teman seperjuangan dalam suka serta duka, Sistem Komputer 2016***
- ***Seluruh Staff maupun administrasi yang telah membantu***
- ***Seluruh Dosen yang telah mengajarkan saya dari awal sampai akhir***
- ***Pembimbing I Bapak Deris Stiawan, Ph.D dan pembimbing II Bapak Ahmad Heryanto, S.Kom., M.T***
- ***Pembimbing Akademik Bapak Dr. Ir. Sukemi, M.T***
- ***Jurusan Sistem Komputer***
- ***Almamater Universitas Sriwijaya***

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulilahirabbil'alamin. Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan proposal tugas akhir ini dengan judul "*Improving Intrusion Detection System* Terhadap Serangan *Probe* menggunakan *Honeypot* di *Small Board Computer*".

Dalam laporan ini penulis menjelaskan mengenai teknik *Improving Intrusion Detection System* Terhadap Serangan *Probe* menggunakan *Honeypot* di *Small Board Computer*. Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti di keamanan jaringan komputer.

Pada penyusunan laporan ini, penulis banyak mendapatkan ide dan saran serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allat SWT dan terimakasih kepada yang terhormat :

1. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi dan semangat.
2. Bapak Jaidan Jauhari, S.Pd. M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
3. Bapak Dr. Ir. Sukemi M.T selaku Ketua Jurusan Sistem Kompuer Fakutas Ilmu Komputer Universitas Sriwijaya serta Pembimbing Akademik Jurusan Sistem Komputer.
4. Bapak Deris Stiawan, Ph. D selaku Pembimbing Tugas Akhir Penulis.
5. Bapak Ahmad Heryanto, S.kom.,M.T selaku Pembimbing Tugas Akhir Penulis.
6. Seluruh teman-teman Jurusan Sistem Komputer khusunya kelas A angkatan 2016 yang tidak dapat saya sebutkan satu persatu.
7. Dan semua pihak yang telah membantu

Penulis menyadari bahwa Laporan ini masih jauh dari kesempurnaan, oleh karena itu penulis sangat mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dikemudian hari.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Inderalaya, 30 Desember 2020

Ardin Febrianda

IMPROVING INTRUSION DETECTION SYSTEM AGAINST PROBE ATTACKS USING A HONEYPOOT ON THE SMALL BOARD COMPUTER

Ardin Febrianda (09011181621008)
Department of Computer Engineering, Faculty of Computer Science
Sriwijaya University
Email : ardin.febrianda99@gmail.com

Abstract

The focus of the study is to perform a collaboration of IDS system with honeypot and snort. It aims to improve the intrusion detection against probe attack where a probe is an attack that aims to collect information about targets such as host, port, and others. The pattern of the attack is obtained based on traffic analysis that will be tested using tools nessus and zenmap. The purpose of the result of the analysis is to find new rules that are needed to update the rules snort. The system will be installed in Banana Pi R1 as the router. In this study, scenario testing will produce 6 different datasets, consisting of normal datasets, attack datasets, and combined datasets. The test is carried out in two stages: (i) testing before updating the snort rules, and (ii) testing after updating the snort rules. The evaluation of detection results was carried out using the confusion matrix detection rate method, the first dataset before updating snort rules have an accuracy value of 61.90%, TPR 1.49%, and FPR 0.00%, while the first dataset after updating snort rules had a significant increase, it reaches 100% accuracy, TPR 100% and FPR 0.00%, the second dataset before updating the snort rules has an accuracy value of 59.98%, TPR 1.52%, and FPR 0.00%, while for the second dataset after updating the snort rules has the same value as the previous first dataset. It has 100% accuracy, TPR 100%, and FPR 0.00%.

Keywords : *Probe attack, IDS Snort, Honeypot, Banana Pi R1.*

IMPROVING INTRUSION DETECTION SYSTEM TERHADAP SERANGAN *PROBE* MENGGUNAKAN *HONEYPOT* DI *SMALL BOARD COMPUTER*

Ardin Febrianda (09011181621008)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
Email : ardin.febrianda99@gmail.com

Abstrak

Fokus penelitian ini adalah melakukan kolaborasi sistem IDS antara *honeypot* dan *snort*. Bertujuan untuk meningkatkan deteksi intrusi terhadap serangan *probe*, dimana *probe* merupakan suatu serangan yang bertujuan untuk mengumpulkan informasi target seperti *host*, *port*, dll, Pola serangan didapatkan berdasarkan analisa *traffic* yang akan diuji menggunakan *tools nessus* & *zenmap*. Hasil analisa tersebut bertujuan untuk menentukan *rules* baru yang diperlukan untuk *update* pada *rules snort*. Sistem tersebut akan tertanam pada *Banana Pi R1* yang sudah diatur menjadi *router*. Pada penelitian ini pengujian skenario akan menghasilkan 6 *dataset* berbeda, yang terdiri dari *dataset* normal, *dataset* serangan dan *dataset* gabungan. Pengujian dilakukan dengan dua tahapan : (i) pengujian sebelum dilakukan *update rules snort*, dan (ii) pengujian setelah dilakukan *update rules snort*. Evaluasi hasil deteksi dilakukan menggunakan metode *confusion matrix detection rate*, *dataset* pertama sebelum *update rules snort* mendapatkan nilai akurasi 61,90%, TPR 1,49% dan FPR 0,00%, sedangkan untuk *dataset* pertama setelah *update rules snort* mendapatkan peningkatan secara signifikan yaitu mencapai akurasi 100%, TPR 100% dan FPR 0,00%, *dataset* kedua sebelum *update rules snort* mendapatkan nilai akurasi 59,98%, TPR 1,52% dan FPR 0,00%, sedangkan untuk *dataset* kedua setelah *update rules snort* mendapatkan nilai yang sama dengan *dataset* pertama sebelumnya yaitu mencapai akurasi 100%, TPR 100% dan FPR 0,00%.

Kata Kunci : Serangan *Probe*, *IDS Snort*, *Honeypot*, *Banana Pi R1*.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Sistem deteksi intrusi merupakan suatu sistem *software* yang berfungsi untuk mendeteksi suatu hal yang tidak wajar dan tidak dikenali sebelumnya, dimana hal tersebut dilakukan untuk antisipasi akan terjadinya hal yang tidak diinginkan. IDS mampu menghasilkan *alert* dari akitivitas *malicious event* berdasarkan *ruleset* yang telah tertanam di dalam sistem IDS tersebut [1].

IDS telah menjadi bagian yang sangat diperlukan dari keamanan sistem untuk mengidentifikasi beberapa serangan. Oleh karena itu, menemukan intrusi secara akurat menjadi fungsionalitas utama dari kebanyakan Sistem Deteksi Intrusi. Meskipun ada banyak jenis IDS tetapi kesulitan utamanya terletak pada tingkat deteksi yang buruk dan *false alarm* yang besar [2].

Salah satu cara yang dapat dilakukan untuk mengatasi kesulitan ini adalah dengan melakukan kolaborasi dengan sistem *honeypot* atau bisa disebut sarang lebah, dalam hal ini *honeypot* berfungsi sebagai sistem palsu ataupun sistem tiruan yang dibuat menyerupai aslinya untuk mengelabui penyerang yang suatu saat pasti akan menyerang [3]. Setelah dilakukan kolaborasi yaitu melakukan penyesuaian, agar *log* dari *honeypot* bisa dipakai kedalam *ruleset snort*. Hal ini menjadi salah satu kekurangan yang membuat sistem deteksi IDS tidak meningkat secara signifikan.

Pada proses analisa, suatu paket yang dihasilkan akan di ekstrak untuk menampilkan informasi dasar berupa atribut - atribut dari *raw data* suatu paket. atribut tersebut antara lain yaitu protokol, *payload*, ttl, ip *length*, ip *header length*, ip *flags*, *checksum*, dll [4].

Probe adalah jenis serangan yang mencoba mengumpulkan *data* dan menemukan kerentanan jaringan. *Data* (alamat IP, nama layanan, aplikasi sistem operasi, nama *host*, dan lain-lain) diperlukan untuk penyerang. Penyerang akan memanfaatkan program pemindaian untuk mengumpulkan *data* tersebut [5].

Dalam penelitian [5], membahas secara keseluruhan beberapa *snort rules* dan bagaimana *rules* tersebut dapat meningkatkan keamanan pada beberapa jenis serangan *probe* seperti *portsweep, ipsweep, satan, ls_domain, ntinfoscan*, dan *queso* dengan membuat *rules* berdasarkan *signature analysis* pada *dataset* MIT-DARPA 1999.

Di sisi lain [6], membahas tentang menerapkan IDS dengan menggunakan *honeypot* sebagai *network security*, sistem tersebut diterapkan pada *Raspberry Pi*. Namun, hal ini juga memiliki kekurangan dimana pada penelitian ini tidak melakukan perhitungan tingkat akurasi dan deteksi dari sistem yang digunakan.

Penelitian lainnya [7], membahas tentang bagaimana implementasi salah satu *tools* dari *honeypot* yaitu *honeyd* yang mampu melakukan penurunan rasio *false positive* dan *false alarm* terhadap deteksi *traffic data* serangan pada beberapa simulasi yang dilakukan.

Berdasarkan pada beberapa ulasan diatas, untuk meningkatkan pendeteksian serangan diperlukan teknik yang tidak hanya bertumpu pada satu jenis IDS saja. Oleh karena itu, penelitian ini berfokus pada penerapan IDS dalam hal ini menggunakan *snort* berkolaborasi dengan *honeypot*, serta melakukan penyesuaian hasil *log honeypot* untuk membuat *ruleset* yang nantinya akan dipakai pada sistem *snort* berdasarkan atribut yang dihasilkan dari *data extraction* dengan tujuan agar *signature* bisa langsung digunakan oleh *snort*.

1.2. Tujuan

Berikut ini merupakan tujuan dari penelitian:

1. Melakukan pengujian *probe* ke *snort* bersamaan dengan *honeypot.*
2. Melakukan analisa perbandingan antara *log snort* dan *log honeypot*.
3. Melakukan *Improving snort* berdasarkan hasil analisa dengan *update ruleset* kedalam *ruleset snort.*
4. Mengukur akurasi, sebelum dan setelah *update ruleset* pada *snort*.

1.3. Manfaat

Adapun manfaat dari penelitian tugas akhir yang dilakukan ialah :

1. Dapat membuat sistem deteksi intrusi dengan honeypot atau sarang lebah menjadi sangat efisien.
2. Dapat membantu dalam mengatasi serangan *Probe* lebih dini.
3. Menjadi keamanan tambahan dalam sebuah sistem.

1.4. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, permasalahan utama yang dibahas pada penelitian ini yaitu :

1. Bagaimana membuat pendeteksian intrusi menjadi lebih baik dan akurat dengan menggunakan *honeypot*.
2. Bagaimana cara mendapatkan *ruleset* baru dari hasil perbandingan *log* pada *honeypot*.
3. Bagaimana cara membandingkan akurasi deteksi serangan *Probe* yang dihasilkan oleh *snort*, sebelum dan setelah dilakukan *update ruleset*.

1.5. Batasan Masalah

Batasan masalah tugas akhir ini yaitu sebagai berikut :

1. Pengujian skenario dilakukan secara online.
2. Pengamatan akan difokuskan pada serangan *Probe* khususnya protokol TCP.
3. Hanya diujikan pada jaringan lokal.
4. Hanya diujikan pada *traffic* jaringan yang rendah.
5. Tidak membahas bagaimana cara pencegahan serangan tersebut
6. Tidak diujikan pada lalu lintas jaringan yang terenkripsi.
7. Mekanisme mendapatkan *ruleset* baru dengan melakukan analisa antara *log snort* dan *log honeypot*.

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam tugas akhir ini akan melewati beberapa tahapan sebagai berikut:

1. Melakukan Studi Pustaka atapun *Literature*

   Pembelajaran dimulai dari pengertian dan juga fungsi dari semua sistem yang akan dipakai, misalnya *honeypot, snort, dan banana pi r1*.

2. Melakukan perancangan *software* dan *hardware*

   Melakukan perancangan *software* dan *hardware* misalnya melakukan konfigurasi pada *honeyd*, pada *snort* dan konfigurasi *banana pi r1* serta menginstal *software* yang akan dipakai pada penelitian ini.

3. Melakukan pengujian hasil dari perancangan sistem

   Setelah melakukan perancangan sistem, maka sistem tersebut akan diuji berdasarkan skenario yang sudah dibuat sebelumnya, untuk mendapatkan hasil analisa yang baik dan benar.

4. Melakukan analisa dari hasil pengujian

   Melakukan analisa dari hasil pengujian yang telah dilakukan, untuk menemukan pemecahan masalah yang timbul dan untuk mendapatkan kesimpulan dari hasil penelitian ini.

5. Mendapatkan kesimpulan & saran untuk pembaca

   Setelah didapatkan hasil dari analisa, maka didapatkan kesimpulan dan saran yang nantinya akan berguna untuk pembaca dan penulis ini.

1.7. Sistematika Penulisan

Berikut ini merupakan sistematika penulisan untuk lebih jelas dan agar pembaca mengetahui apa saja yang akan dilakukan oleh penulis :

BAB 1 PENDAHULUAN

Pada bab pendahuluan merupakan kumpulan dari latar belakang kenapa penulis mendapatkan ide, lalu ada juga tujuan serta manfaat dari penelitian ini, serta rumusan masalah, yaitu apa saja yang akan dibahas pada penelitian ini.

BAB 2. TINJAUAN PUSTAKA

Pada bab tinjauan pustaka terdapat kumpulan dari pengertian dari apa itu sistem deteksi intrusi, apa itu *snort* dan apa itu *honeypot*, serta mekanisme mengenai *banana pi r1* yang akan dipakai pada penelitian ini.

BAB 3. METODOLOGI PENELITIAN

Pada bab metodologi penelitian merupakan kumpulan secara detail dari konfigurasi *snort* , konfigurasi *honeypot* dan topologi serta apa saja yang akan dipakai pada penelitian ini.

BAB 4. HASIL DAN ANALISA

Pada bab hasil dan analisa ini merupakan hasil yang didapatkan berupa pemecahan masalah hasil dari pengujian yang dilakukan sebelumnya berupa gambar, tabel, dan grafik.

BAB 5. KESIMPULAN

Pada bab kesimpulan, merupakan kumpulan dari kesimpulan yang dapat diambil dari hasil penelitian yang sebelumnya didapatkan dari pengujian dan saran yang akan berguna untuk pembaca.

DAFTAR PUSTAKA

[1] Candra Adi Winanto, "Deteksi Serangan *Denial of Service* Menggunakan *Artificial Immune System*," vol. 2, no. 1, pp. 456–459, 2016.

[2] D. Agrawal, "*A Review on Various Methods of Intrusion Detection System*," vol. 11, no. 1, pp. 7–15, 2020.

[3] S. Lance, *Honeypots: Tracking Hackers By*, vol. 20, no. 4. 2003.

[4] T. I. U. of B. Saad Hafeez B.Eng. and A, "*Deep Packet Inspection using Snort*," *Deep Pack. Insp. using Snort*, p. 24, 2017.

[5] N. Khamphakdee, N. Benjamas, and S. Saiyod, "*Improving intrusion detection system based on Snort rules for network probe attack detection*," *2014 2nd Int. Conf. Inf. Commun. Technol. ICoICT 2014*, pp. 69–74, 2014.

[6] S. Mahajan, A. M. Adagale, and C. Sahare, "*Intrusion Detection System Using Raspberry PI Honeypot in Network Security*," *Int. J. Sci. Eng. Res. IJESC*, vol. 6, no. 3, pp. 2792–2795, 2016.

[7] B. Khosravifar and J. Bentahar, "*An experience improving intrusion detection systems false alarm ratio by using honeypot*," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 997–1004, 2008.

[8] E. A. Winanto, A. Heryanto, and D. Stiawan, "Visualisasi Serangan *Remote to Local* (R2L) Dengan *Clustering K-Means*," *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[9] A. Jamdagni, "*Payload-based Anomaly Detection in HTTP Traffic*," no. November, p. 190, 2012.

[10] N. I. Prasetya, S. Djanali, and M. Husni, "Verifikasi *Signature* Pada Kolaborasi Sistem Deteksi Intrusi Jaringan Tersebar Dengan *Honeypot*," *JUTI J. Ilm. Teknol. Inf.*, vol. 12, no. 2, p. 70, 2014.

[11] B. A. Pratomo, S. Djanali, W. Suadi, J. T. Informatika, and F. T. Informasi, "Pengalihan Paket Ke *Honeypot* Pada *Linux Virtual Server* Untuk Mengatasi Serangan Ddos," pp. 53–61, 2011.

[12] S. K. Patel and A. Sonker, "*Rule-Based Network Intrusion Detection System for Port Scanning with Efficient Port Scan Detection Rules Using Snort*," *Int. J. Futur. Gener. Commun. Netw.*, vol. 9, no. 6, pp. 339–350, 2016.

[13] G. Hill. *The Cable and Telecommunications Professionals' Reference*. 3rd ed. Oxford: Elsevier's *Science & Technology*. 2007.

[14] Z. Dewa and L. A., "*Data Mining and Intrusion Detection Systems*," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 62–71, 2016.

[15] Pangeran, A. Abbas, "Menjadi Admin Jaringan Nirkabel", 2008.