Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik

TESIS

Oleh

Dedi Haris Widyatmoko

NIM :5541810009

PROGRAM MAGISTER TEKNIK ELEKTRO

PROGRAM PASCA SARJANA

UNIVERSITAS MERCU BUANA

2021

https://lib.mercubuana.ac.id

Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik

TESIS

Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan Program Pascasarjana Program Magister Teknik Elektro

Oleh

Dedi Haris Widyatmoko

NIM :5541810009

UNIVERSITAS MERCU BUANA

PROGRAM PASCA SARJANA

https://lib.mercubuana.ac.id

ABSTRAK

Mendeteksi intrusi jaringan dan mencegah ancaman aktor dunia maya dari melaksanakan tujuan mereka adalah langkah-langkah penting untuk menjaga keamanan siber. Kesadaran dan kewaspadaan terhadap keamanan siber setiap organisasi dan bahkan individu diperlukan untuk menghadapi ancaman ini. Dan tidak semua orang atau organisasi mempunyai dana yang cukup memanfaatkan intelijen ancaman untuk mendeteksi gangguan jaringan. Sehingga diperlukan system keamanan jaringan yang berbasis *opensource.*

Security Onion adalah *open source* platform *Network Security Manager (NSM)* yang menyediakan beberapa *Intrusion Detection Systems (IDS)* yaitu *Host Intrusion Detection System (HIDS)* dan Network *Intrusion Detection System (NIDS).* Pada penelitian yang akan penulis teliti adalah bagaimana menganalisa performa fungsi *network security* dan *network forensic* pada *Security Onion* dengan tipe penerapan terdistribusi / *"Distributed"* .. Pada performa *network security* bagian *IDS Engine* pada *NIDS* (*Network Intrusion Detection System*) akan dioptimalkan performanya dengan mengevaluasi beberapa pilihan *IDS Ruleset* non komersial pada opsi *IDS Engine Snort* dan *Suricata*. Yaitu *Emerging Threads Open , Snort Talos NoGPL* dengan *oinkcode* dan *Snort Talos subscriber policy* (*connectivity , balance* dan *security*). Untuk serangan siber yang akan disimulasikan menggunakan serangan siber nomor 2 dan 3 dari top 5 klasifikasi yaitu *"information gathering"* dan *"exploit.kit"*.Sedangkan untuk performa network forensic penulis akan mengevaluasi *NFAT (Network Forensic Analysis Tools)* pada *Security Onion.*

Berdasarkan hasil pengujian *antara IDS Suricata* dengan *IDS Snort* diperoleh *IDS Suricata* dengan *"IDS ruleset Emerging Threats Open"* memperoleh jumlah alert deteksi paling tinggi yaitu sebanyak 629 dibandingkan dengan IDS Snort sebanyak 541 .Sedangkan besarnya jumlah total ruleset yang aktif pada *IDS Engine Suricata* tidak berpengaruh dengan hasil jumlah alert deteksi sguil events. Hasil pengetesan *Sguil* dan *Squert* ekstrak dari *IDS Engine Suricata* memberikan kebutuhan informasi untuk *network forensic*.

***Keywords**: NIDS, Security Onion, Forward Nodes, Network Forensic, IDS Ruleset*

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa atas berkat yang dilimpahkan sehingga Penulis dapat menyelesaikan laporan penelitian tesis yang berjudul "*Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik*"

Penulisan laporan penelitian ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Teknik Elektro pada Fakultas Teknik Elektro – Universitas Mercubuana.

Evaluasi efektivitas IDS Engine dan *NFAT* pada *NSM Security Onion* dengan tipe penerapan terdistribusi / *"Distributed"* . Dengan menggunakan arsitektur *master server* dan *slave / forward nodes* yg akan meneruskan alert dan packet_logs tersentralisasi. Beberapa bahasan menunjukkan cara konfigurasi system dengan tipe penerapan *"Distributed"*. Diharapkan dengan penelitian ini dapat diterapkan "*Cyber Security"/ keamanan siber* secara komprehensif pada suatu organisasi yang membutuhkan keamanan jaringan siber .

Penulis mengucapkan terima kasih yang sebesar-besarnya atas bimbingan dalam proses penyusunan laporan tesis ini kepada

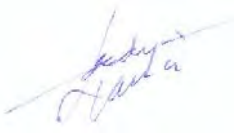
1. Dr.Marza Ihsan Marzuki, S.T., M.T., selaku dosen pembimbing yang telah menyediakan waktu ,tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini.
2. Dr Umaisaroh, selaku Ketua Program Pascasarjana Fakultas Teknik Elektro Universitas Mercubuana.
3. Kepada (Alm) Papa & Mama saya, terima kasih atas semua yang telah mereka berikan kepada Penulis.
4. Istri dan anak-anak tercinta, yang selalu memberikan motivasi , semangat dan dukungan kepada penulis dalam penyelesaian tesis ini.
5. Seluruh rekan-rekan Angkatan 23 Magister Teknik Elektro yang telah memberikan dorongan dan memberikan masukan dan saran kepada penulis.
6. Semua pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu dan mendukung penyelesaian tesis ini.

Akhir kata , saya berharap Tuhan Yang maha Esa berkenan membalas kebaikan semua pihak yang telah membantu. Semoga karya akhir ini membawa manfaat bagi pengembangan ilmu.

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

Jakarta, 20 Agustus 2021



Penulis

UNIVERSITAS
MERCU BUANA

https://lib.mercubuana.ac.id

PENGESAHAN TESIS

Judul	: Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik
Nama	: Dedi Haris Widyatmoko
N I M	: 55418110009
Program	: Pascasarjana Program Magister Teknik Elektro
Konsentrasi	: Keamanan Jaringan ICT
Tanggal	: 20 Agustus 2021

Mengesahkan

Pembimbing I

(Dr Marza Ihsan Marzuki, MT)

UNIVERSITAS MERCU BUANA

Dekan Fakultas Teknik	Ketua Program Studi
(Dr. Ir. Mawardi Amin, M.T.)	(Dr Umaisaroh, S.ST)

https://lib.mercubuana.ac.id

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini :

Judul	: Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik
Nama	: Dedi Haris Widyatmoko
N I M	: 55418110009
Program	: Magister Teknik Elektro
Konsentrasi	: Keamanan Jaringan ICT
Tanggal	: 20 Agustus 2021

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, 20 Agustus 2021

Dedi Haris Widyatmoko

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

PERNYATAAN *SIMILARITY CHECK*

Saya yang bertanda tangan di bawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh

Nama	: Dedi Haris Widyatmoko
NIM	: 55418110009
Program Studi	: Magister Teknik Elektro

dengan judul
"Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensic", telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal 21/06/2021, didapatkan nilai persentase sebesar 21%.

Jakarta, 21 Juni 2021
Administrator Turnitin

Arie Pangudi, A.Md

https://lib.mercubuana.ac.id

DAFTAR ISI

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

DAFTAR GAMBAR

Halaman

UNIVERSITAS MERCU BUANA

https://lib.mercubuana.ac.id

https://lib.mercubuana.ac.id

https://lib.mercubuana.ac.id