



**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**



# **Analisa Performa Intrusion Detection dengan Security Onion menggunakan Metode Forensik**

**TESIS**

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

UNIVERSITAS  
MERCU BUANA

Oleh

**Dedi Haris Widyatmoko**

**NIM :5541810009**

**UNIVERSITAS MERCU BUANA  
PROGRAM PASCA SARJANA**

## 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 Threats 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*

## 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.

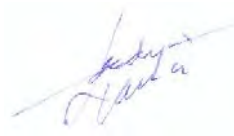
Evaluasi efektivitas IDS Engine dan *NFAT* pada *NSM Security Onion* dengan tipe penerapan terdistribusi / “*Distributed*” . Dengan menggunakan arsitektur *master server* dan *slave / forward nodes* yg akan meneruskan alert dan *packet\_logs* tersentralisasi. Beberapa bahasan menunjukkan cara konfigurasi 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 Umairroh, 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.

Jakarta, 20 Agustus 2021



Penulis



UNIVERSITAS  
MERCU BUANA

## 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

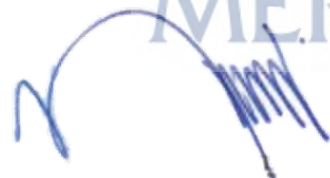
Pembimbing I

(Dr Marza Ihsan Marzuki, MT)

UNIVERSITAS

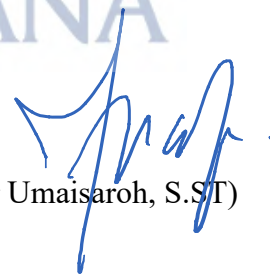
MERCU BUANA

Dekan Fakultas Teknik



(Dr. Ir. Mawardi Amin, M.T.)

Ketua Program Studi



(Dr Umairah, S.ST)

## 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

## 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

UNIVERSITAS  
MERCU BUANA

Arie Pangudi, A.Md



# DAFTAR ISI

	Halaman
<b>PENGESAHAN TESIS</b> .....	I
<b>LEMBAR PENGESAHAN</b> .....	II
<b>LEMBAR PERNYATAAN</b> .....	III
<b>KATA PENGANTAR</b> .....	IV
<b>DAFTAR ISI</b> .....	V
<b>DAFTAR GAMBAR</b> .....	VI
<b>DAFTAR TABEL</b> .....	VII
<b>DAFTAR SINGKATAN</b> .....	VIII
<b>BAB I      PENDAHULUAN</b>	
1.1    Latar Belakang.....	1
1.2    Perumusan Masalah.....	4
1.3    Tujuan Penelitian.....	4
1.4    Manfaat Penelitian.....	4
1.5    Batasan Masalah.....	4
<b>BAB II     KAJIAN PUSTAKA</b>	
2.1    Teori Dasar .....	6
2.2.   Perbedaan Antara <i>Network Forensic</i> dan <i>Netwok Security</i> .....	8
2.3.   Pengenalan Security Onion .....	11
2.4.   Penelitian Sebelumnya .....	13
<b>BAB III    METODOLOGI PENELITIAN</b>	
3.1    Metode Penelitian .....	19
3.2    Alur Penelitian .....	15
3.3    Parameter Penelitian.....	16
3.4    Rancangan Penelitian .....	18
3.4.1 <i>Oracle Virtualbox</i> .....	27
3.4.2 <i>Metasploitable 2</i> .....	28

3.4.3	<i>Kalilinux</i> .....	29
3.4.4	<i>Security Onion</i> .....	30
<b>BAB IV</b>	<b>HASIL PENELITIAN DAN ANALISA</b>	
4.1	Pengujian <i>IDS Engine</i> .....	48
4.1.1	...Hasil pengujian <i>IDS Engine</i> dengan <i>IDS Ruleset</i> .....	50
4.1.2	...Perhitungan Nilai Efisiensi .....	53
4.2	Pengujian NFAT .....	53
4.2.1	NMAP .....	53
4.2.2	<i>Apache CGI Argument Injection</i> .....	54
4.2.3	<i>Unreal IRCD 3281 backdoor</i> .....	55
4.2.4	Deteksi Alert Sguil .....	55
4.2.5	Deteksi Alert Squert .....	57
4.2.6	Analisa NFAT .....	60
4.2.7	Ekstrak <i>Sguil Transcript</i> .....	60
4.2.8	Ekstrak <i>Wireshark</i> .....	63
4.2.9	Ekstrak <i>Network Miner</i> .....	64
4.2.10	Reporting Data .....	64
<b>BAB V</b>	<b>KESIMPULAN DAN SARAN</b>	
5.1	Kesimpulan .....	66
5.2	Saran .....	67
<b>DAFTAR PUSTAKA</b> .....		68

## DAFTAR GAMBAR

	Halaman
Gambar 1.1 Serangan Siber Januari-April 2020 .....	1
Gambar 1.2 Top 5 Klasifikasi Serangan .....	2
Gambar 2.1.1 Diagram Network Forensic Process.....	8
Gambar 2.2.1 Diagram Network Security dan Network Forensic.....	9
Gambar 3.1 Diagram Alur Penelitian .....	21
Gambar 3.3.1 Arsitektur IDS Engine dan IDS Ruleset pada Security Onion .....	22
Gambar 3.3.2 Alur Evaluasi IDS Engine dengan IDS Ruleset.....	23
Gambar 3.3.3 Snort Talos ruleset & Snort Subscriber policy connectivity, balance dan security.....	24
Gambar 3.3.4 Alur evaluasi IDS Engine Snort dengan IDS ruleset Snort Talos ruleset & Snort Subscriber policy .....	25
Gambar 3.3.5 Alur Evaluasi Network Forensic Analysis Tool .....	26
Gambar 3.4 Perencanaan Topologi penerapan Virtual Machine .....	27
Gambar 3.4.1 Tampilan Utama Oracle Virtualbox.....	28
Gambar 3.4.2 Tampilan Utama Metasploitable2.....	29
Gambar 3.4.3.1 Tampilan Utama Kalilinux.....	29
Gambar 3.4.3.2 Tampilan Armitage yang jalan di Kalilinux .....	30
Gambar 3.4.4.1 Tampilan Utama Security Onion .....	30
Gambar 3.4.4.2 Arsitektur Security Onion .....	31
Gambar 3.4.4.3 Diagram Penerapan Tipe Distributed.....	32
Gambar 3.5.1 IP address pada antarmuka Network Bridge.....	33
Gambar 3.5.2 ifconfig pada host target Metasploitable 2 .....	34
Gambar 3.5.3 ifconfig pada host attacker Kalilinux .....	34
Gambar 3.5.4 ifconfig host Security Onion Master Server .....	35
Gambar 3.5.5 ifconfig pada host Security Onion Slave Sensor.....	35
Gambar 3.7.1 Security Onion Setup .....	36
Gambar 3.7.2 Security Onion Setup pilihan Evaluation dan Production Mode .....	36
Gambar 3.7.3 Penerapan New atau Existing Security Onion .....	37
Gambar 3.7.4 Isikan username untuk account Kibana , Squert dan Sguil.....	37
Gambar 3.7.5 Isikan Password untuk akses Sguil client.....	37

Gambar 3.7.6 Konfirmasi Password.....	37
Gambar 3.7.7 Best Practice.....	38
Gambar 3.7.8 Opsi IDS Ruleset yang akan digunakan dalam IDS Engine ...	38
Gambar 3.7.9 Pilihan IDS Engine.....	39
Gambar 3.7.10 Network Sensor Services .....	39
Gambar 3.7.11 Store logs locally.....	39
Gambar 3.7.12 LOG_SIZE_LIMIT .....	39
Gambar 3.7.13 Proceed with the changes .....	39
Gambar 3.7.14 Setup is now completed! .....	40
Gambar 3.7.15 Sguil username password.....	40
Gambar 3.7.16 Pilih interface yang akan dimonitor .....	40
Gambar 3.7.17 Tampilan dashboard pada aplikasi Sguil .....	41
Gambar 3.8.1 Slave Sensor Setup.....	41
Gambar 3.8.2 Konfigurasi Jaringan .....	42
Gambar 3.8.3 Production Mode.....	42
Gambar 3.8.4 Existing Security Onion Deployment .....	42
Gambar 3.8.5 Master Server IP address.....	43
Gambar 3.8.6 SSH Master Server Username.....	43
Gambar 3.8.7 Forward Nodes .....	43
Gambar 3.8.8 Best Practice.....	43
Gambar 3.8.9 PF_RING .....	44
Gambar 3.8.10 Antarmuka jaringan mana yang akan dimonitor.....	44
Gambar 3.8.11 HOME_NET .....	44
Gambar 3.8.12 Proceed with the changes .....	45
Gambar 3.8.13 Terminal SSH Master Server password .....	45
Gambar 3.8.14 Setup Completed .....	45
Gambar 4.1.1 Ping host target dari host attacker .....	48
Gambar 4.1.2 Port scan dalam aplikasi Armitage.....	48
Gambar 4.1.3 Serangan exploit dengan “Hail Mary” .....	49
Gambar 4.1.4 Command sudo sostat .....	49
Gambar 4.1.5 Total rules yang aktif .....	49
Gambar 4.1.1.1 Hasil pengujian dengan perbandingan jumlah total IDS Ruleset & Sguil Events.....	50

Gambar 4.1.1.2 Chart Perbandingan IDS Ruleset Aktiv .....	50
Gambar 4.1.1.3 Chart Perbandingan Total Sguil Event yang terdeteksi oleh IDS.....	51
Gambar 4.1.1.4 Total Sguil Event yang terdeteksi oleh IDS rulset Snort Talos berdasarkan Subs Policy.....	52
Gambar 4.2.1 Tampilan hasil port scan dengan NMAP .....	54
Gambar 4.2.2 php_cgi_arg injections .....	55
Gambar 4.2.3 Unreal IRCD 3281 backdoor .....	55
Gambar 4.2.4.1 Alert NMAP pada Sguil console.....	56
Gambar 4.2.4.2 Alert Apache CGI Argument Injection.....	57
Gambar 4.2.4.3 Unreal IRCD 3281 backdoor exploit .....	57
Gambar 4.2.5.1 Pilihan view Squert :Events, Summary (1) dan Views (2.....	58
Gambar 4.2.5.2 Tampilan Summary.....	58
Gambar 4.2.5.3 Tampilan Views .....	59
Gambar 4.2.5.4 Squert Nmap .....	59
Gambar 4.2.5.5 Apache CGI Argument Injection .....	60
Gambar 4.2.5.6 Unreal IRCD 3281 backdoor .....	60
Gambar 4.2.7.1 Pilihan ekstrak Sguil Console Alert ID.....	61
Gambar 4.2.7.2 Ekstrak serangan port scan nmap.....	61
Gambar 4.2.7.3 Ekstrak serangan apache cgi arg injection dengan Transcript .....	62
Gambar 4.2.7.4 Ekstrak serangan unreal ircd exploit dengan Transcript.....	62
Gambar 4.2.8.1 Ekstrak alert Nmap menggunakan Wireshark .....	63
Gambar 4.2.8.2 Ekstrak alert apache cgi arg injection menggunakan Wireshark .....	63
Gambar 4.2.8.3 Ekstrak alert unreal ircd exploit dengan Wireshark.....	64
Gambar 4.2.9 Ekstrak port scan Nmap dengan NetworkMiner.....	64