

**ANALISIS PERBANDINGAN EFEKTIVITAS IDS
(INTRUSION DETECTION SYSTEM) SNORT DAN
SURICATA TERHADAP SERANGAN DENGAN METODE
SIMULASI DI PUSTIKOM UNJ**

Skripsi



Skripsi ini ditulis untuk memenuhi sebagian persyaratan dalam memperoleh gelar
Sarjana Pendidikan

**PROGRAM STUDI PENDIDIKAN INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS NEGERI JAKARTA
2020**

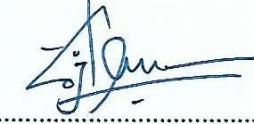
**ANALISIS PERBANDINGAN EFEKTIVITAS INTRUSTION
DETECTION SYSTEM SNORT DAN SURICATA TERHADAP
SERANGAN DENGAN METODE SIMULASI DI PUSTIKOM UNJ**

Nugroho Dedi Riyanto, NIM 5235154798

HALAMAN PENGESAHAN

NAMA DOSEN	TANDA TANGAN	TANGGAL
M.Ficky Duskarnaen, ST.,M.Sc (Dosen Pembimbing I)		14 - 2 - 2020
Hamidillah Ajie,S.Si.,M.T. (Dosen Pembimbing II)		12 - 2 - 2020

PENGESAHAN PANITIA UJIAN SKRIPSI

NAMA DOSEN	TANDA TANGAN	TANGGAL
Prasetyo Wibowo Yunanto, M.Eng NIP. 19790612005011002 (Ketua Penguji)		12 - 2 - 2020
Dr. Yuliatri Sastrawijaya, M.Pd NIP. 195807061983032002 (Dosen Penguji I)		10 - 2 - 2020
Irma Permata Sari, M.Eng NIP. 1989052620193032022 (Dosen Penguji II)		10 - 2 - 2020

Tanggal Lulus : 12 - 2 - 2020

HALAMAN PERNYATAAN

Dengan ini Saya menyatakan bahwa :

1. Karya tulis skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik sarjana, baik di Universitas Negeri Jakarta maupun di perguruan tinggi lain.
2. Karya tulis ini murni gagasan, rumusan, dan penelitian Saya sendiri dengan arahan dosen pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini Saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di Universitas Negeri Jakarta.

Jakarta, 24 Januari 2020

Yang Membuat Pernyataan,



Nugroho Dedi Riyanto

5235154798

NASKAH PUBLIKASI JURNAL

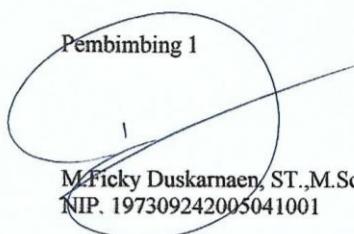
**ANALISIS PERBANDINGAN EFEKTIVITAS IDS
(INTRUSION DETECTION SYSTEM) SNORT DAN
SURICATA TERHADAP SERANGAN DENGAN
METODE SIMULASI DI PUSTIKOM UNJ**

yang diajukan oleh :

Nugroho Dedi Riyanto

5235154798

Telah disetujui oleh :

Pembimbing 1

M. Ficky Duskarnaen, ST.,M.Sc
NIP. 197309242005041001

Tanggal 14-2-2020

Pembimbing 2



Hamidillah Ajie,S.Si.,M.T.
NIP. 197408242005011001

Tanggal 14-2-2020



KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS NEGERI JAKARTA
UPT PERPUSTAKAAN

Jalan Rawamangun Muka Jakarta 13220
Telepon/Faksimili: 021-4894221
Laman: lib.unj.ac.id

**LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademika Universitas Negeri Jakarta, yang bertanda tangan di bawah ini, saya:

Nama : Nugroho Dedi Riyanto
NIM : 5235154798
Fakultas/Prodi : Pendidikan Teknik Informatika dan Komputer
Alamat email : nugroho.dedi.r@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Negeri Jakarta, Hak Bebas Royalti Non-Ekslusif atas karya ilmiah:

Skripsi Tesis Disertasi Lain-lain (.....)

yang berjudul :

Analisis Perbandingan Efektivitas IDS (Intrusion Detection System) Snort dan Suricata Terhadap serangan dengan Metode Simulasi di Pustikom UNJ.

Dengan Hak Bebas Royalti Non-Ekslusif ini UPT Perpustakaan Universitas Negeri Jakarta berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain secara *fulltext* untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan Universitas Negeri Jakarta, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 21 Februari 2020

Penulis

(Nugroho Dedi Riyanto)

ANALISIS PERBANDINGAN EFEKTIVITAS INTRUSION DETECTION SYSTEM SNORT DAN SURICATA TERHADAP SERANGAN DENGAN METODE SIMULASI DI PUSTIKOM UNJ

ABSTRAK

Di lingkungan Pustikom UNJ kampus A Universitas Negeri Jakarta keamanan yang efektif pada jaringan sangat dibutuhkan untuk menjaga kerahasiaan data pada server, memangkas aktifitas oknum yang tidak bertanggung jawab serta aktifitas dari luar kampus. Pustikom UNJ menyediakan fasilitas internet yang bias diakses mahasiswa, dosen dan karyawan melalui internet yang disebarluaskan melalui server pustikom UNJ. *User* dapat mengakses segala jenis aktifitas pada jaringan yang bersifat rahasia sekalipun tanpa khawatir diretas oleh oknum tidak bertanggung jawab yang dapat memantau kapan saja. Oleh sebab itu, dibutuhkan keamanan efektif dalam mendeteksi adanya aktifitas yang tidak wajar. Analisa dan perbandingan IDS Snort dan Suricata untuk mengukur tingkat akurasi kecepatan deteksi dengan serangan simulasi. Proses untuk mencari perbandingan yang efektif dari segi kecepatan pendektsian dimulai dari menginstal sistem operasi ubuntu dan windows yang berfungsi untuk menjalankan perangkat lunak serta aplikasi yang digunakan, menginstal perangkat lunak snort, suricata, cacti dan aplikasi *hacking* untuk simulasi serangannya, dan simulasi yang dilakukan menggunakan jaringan lokal khusus tanpa mengganggu jaringan yang ada. Proses pengujian proses pengukuran dilakukan di dalam mesin virtual simulasi dengan serangan *denial of service*, *port scanning* dan *remote access terminal* dari sisi perangkat lunak dan kecepatan pendektsian dari masing-masing perangkat lunak. Hasil penelitian Snort lebih unggul dalam hal mendeteksi serangan akan tetapi Suricata lebih unggul dalam hasil penggunaan sumber daya pada hasil pengukuran.

Kata kunci : IDS snort dan suricata, jaringan lokal, kecepatan pendektsian, serangan simulasi

COMPARISON ANALYSIS OF SNORT AND SURICATA INTRUSION DETECTION SYSTEM AGAINST ATTACKS USING SIMULATION METHOD AT PUSTIKOM UNJ

ABSTRACT

In the environment of Pustikom UNJ campus A State University of Jakarta, an effective security for networking is needed to keep the privacy of data on servers, cutting the activity of irresponsible people and activity from outside of campus. Pustikom UNJ provides internet facility that can be accessed by students, lecturers, and employees through internet that is spread by Pustikom UNJ's server. Users can access any kind of activity on the network, even those that are private, without worrying being hacked by irresponsible people that can be watching anytime. Therefore, effective security is needed to detect these kinds of irresponsible activities. Analysis and comparison of IDS Snort and Suricata to measure the level of accuracy. The process to find an effective comparison of the detection speed started from installing operating systems Ubuntu and Windows that function to run the software and application used, installing Snort, Suricata, Cacti software and hacking software to simulate the attack, and simulation that was done using a special local network that did not affect the other networks. Measurements carried out in a virtual machine, simulating denial of service, port scanning and remote access terminal from the standpoint of software and detection speed of each software. Snort is superior research results in terms of detection accuracy will attack, however the speed and the use resources on the measurements results.

Keywords: IDS Snort and Suricata, local network, detection speed, attack simulation

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah Subhanahu Wa Ta'ala yang telah melimpahkan rahmat dan karunia-Nya sehingga akhirnya penulis dapat menyelesaikan skripsi ini tepat pada waktunya.

Skripsi yang berjudul ‘Perbandingan Efektivitas Intrusion Detection System IDS Snort dan Suricata terhadap serangan dengan metode simulasi di Pustikom UNJ’ ini ditulis untuk memenuhi salah satu syarat guna memperoleh gelar Sarjana Pendidikan Teknik Informatika dan Komputer pada Fakultas Teknik, Universitas Negeri Jakarta.

Pada kesempatan yang baik ini, izinkanlah penulis mengucapkan rasa hormat dan ucapan terima kasih kepada semua pihak yang dengan tulus dan ikhlas telah memberikan bantuan dan semangat dalam menyelesaikan skripsi ini, terutama kepada:

1. Allah Subhanahu Wa Ta'ala dan Nabi Muhammad SAW
2. Bapak Iriyanto Hakam .S dan Ibu Dede Kurningsih selaku kedua orang tua penulis. Terima kasih telah membesarkan, mendidik, merawat dan mendoakan serta selalu mengingatkan untuk menyelesaikan tugas akhirnya sehingga penulis dapat menyelesaikan skripsi ini.
3. Hanna Nur Oktaviyani, dan Dimas selaku adik yang selalu mengingatkan, mendoakan dan memberi motivasi untuk menyelesaikan skripsi ini.
4. Bapak Lipur Sugiyanta Phd. selaku Ketua Program Studi Pendidikan Teknik Informatika dan Komputer.
5. Bapak M. Ficky Duskarnaen, M.Sc. selaku Dosen Pembimbing I yang penuh kesabaran membimbing hingga malam hari dan tak hentinya memberikan semangat kepada Penulis hingga selesaiannya skripsi ini.
6. Bapak Hamidiilah Ajie, S.Si., M.T. selaku Dosen Pembimbing II yang telah memberikan bimbingan dan arahan sehingga penulis dapat menyelesaikan skripsi ini.
7. Staff Tata Usaha dan Administrasi Program Studi Pendidikan Teknik Informatika dan Komputer, Pak Yanto dan Mba Nafisa yang selalu memberikan informasi dan kemudahan kepada penulis dalam memproses administrasi selama penyusunan skripsi.
8. Teman-teman Haris, Fiky, Aldo, Alam, Rekza, Affan, Dimas Omen, Fadila, Putri, Dewi, Bang Reivaldi, Atikah dan Gadanta dkk, yang sama-sama masih cari masa depannya
9. Teman-teman seperjuangan Progam Studi Pendidikan Teknik Informatika dan Komputer 2015, Teruntuk jurusan TKJ PTIK 2015.

10. Untuk teman dekatku yang dari awal Skripsi sampai saat ini menemaniku, Neng Ayu Herawati. Semangat Kuliah nya biar cepat Skipsian!!
11. Seluruh pihak yang telah mendukung dan tidak bisa disebutkan satu persatu demi terselesaikannya skripsi ini dengan baik dan lancar. Jazakumullah Khairan (Semoga Allah membala kalian dengan kebaikan). Aamiin

Segala kesempurnaan hanya milik Allah, penulis menyadari bahwa skripsi ini sangatlah jauh dari kata sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun agar skripsi ini lebih baik di kemudian hari. Akhir kata, semoga skripsi ini dapat bermanfaat bagi pembaca dan dapat ikut serta dalam mendukung kemajuan ilmu pengetahuan baik dari segi pendidikan maupun teknologi.



DAFTAR ISI

HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN.....	iii
ABSTRAK.....	iv
ABSTRACT	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
DAFTAR LAMPIRAN.....	xii
BAB I.....	1
PENDAHULUAN	1
1.1 Latar belakang	1
1.2 Identifikasi masalah	4
1.3 Batasan masalah.....	4
1.4 Rumusan masalah	4
1.5 Manfaat Penelitian	5
1.6 Tujuan Penelitian	5
BAB II	6
TINJAUAN PUSTAKA	6
2.1 Teori dan Konsep	6
2.1.1 Universitas Negeri Jakarta	6
2.1.1.1 Layanan Internet Universitas Negeri Jakarta.....	6
2.1.1.2 UPT TIK.....	7
2.1.2 Ancaman Keamanan Jaringan Komputer.....	8
2.1.2.1 DOS Attack.....	9
2.1.3 Fitur-Fitur Keamanan Jaringan	10
2.1.3.1 IDS (Intrusion Detection System).....	10
2.1.3.2 Snort.....	14
2.1.3.3 Suricata.....	18
2.1.4 Network Analyzer.....	20
2.1.5 Sistem Operasi	21
2.2 Penelitian Relevan	22
2.3 Kerangka Berpikir.....	25
BAB III.....	27
METODOLOGI PENILITIAN.....	27
3.1 Tempat dan Waktu Penlitian	27
3.2 Alat dan Bahan Penelitian	27
3.2.1 Perangkat Keras.....	27
3.2.2 Perangkat Lunak.....	28
3.2.3 Skema topologi Pengujian UPT TIK.....	28
3.2.4 Metode Pengujian.....	29

3.3	Diagram Alir Penelitian	30
3.4	Teknik dan Prosedur Pengumpulan Data.....	32
3.5	Teknik Analisis Data.....	33
3.6	Perancangan Server IDS.....	33
BAB IV	35
HASIL PENELITIAN	35
4.1	Deskripsi Hasil Penelitian	35
4.1.1	Analisis Kebutuhan	35
4.2	Analisis dan Penelitian	35
4.3	Perancangan Sistem	37
4.3.1	Perancangan Jaringan Komputer.....	37
4.3.2	Snort.....	38
4.3.3	Suricata.....	38
4.3.4	Cacti.....	39
4.3.5	LOIC.....	40
4.3.6	Advance Port Scanner.....	41
4.3.7	njRAT.....	42
BAB V	44
KESIMPULAN DAN SARAN	44
5.1	Kesimpulan.....	44
5.2	Saran.....	45
DAFTAR PUSTAKA	46
LAMPIRAN	48

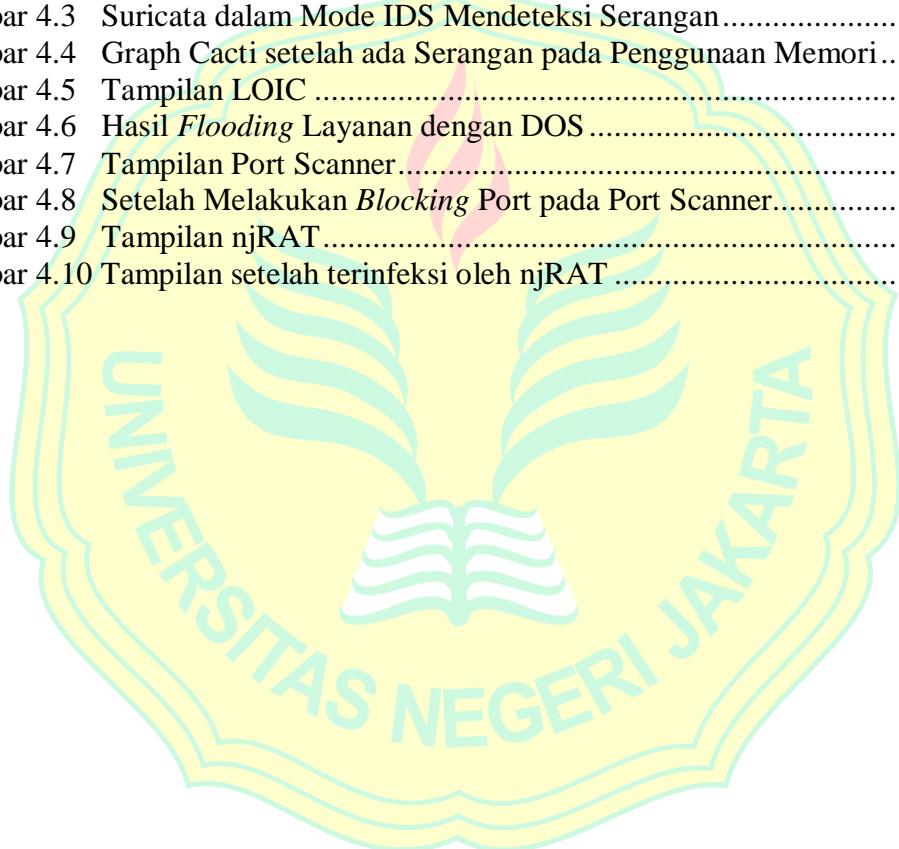
DAFTAR TABEL

Tabel 2.1	Perbedaan HIDS dan NIDS	14
Tabel 2.2	Penelitian Relevan	23
Tabel 3.1	Perangkat Keras.....	27
Tabel 3.2	Perangkat Lunak	28
Tabel 3.3	Pengujian Kecepatan Pendekripsi	29
Tabel 3.4	Pengujian pada attacker	29
Tabel 4.1	Pengukuran Kecepatan Pendekripsi	35
Tabel 4.2	Pengujian attacker.....	36
Tabel 4.3	Hasil Eksperimen Perbandingan.....	36



DAFTAR GAMBAR

Gambar 2.1	Topologi Jaringan UPT TIK	7
Gambar 2.2	Skema DOS	10
Gambar 2.3	HIDS dan NIDS.....	13
Gambar 2.4	Komponen Snort.....	17
Gambar 2.5	Cacti Traffic Network Software	20
Gambar 2.6	Kerangka Berpikir	26
Gambar 3.1	Skema Pengujian pada jaringan lokal UPT TIK	28
Gambar 3.2	Diagram Alir Penelitian	30
Gambar 4.1	Topologi Pengujian.....	37
Gambar 4.2	Snort dalam Mode IDS Mendeteksi Serangan	38
Gambar 4.3	Suricata dalam Mode IDS Mendeteksi Serangan.....	39
Gambar 4.4	Graph Cacti setelah ada Serangan pada Penggunaan Memori.....	39
Gambar 4.5	Tampilan LOIC	40
Gambar 4.6	Hasil Flooding Layanan dengan DOS	41
Gambar 4.7	Tampilan Port Scanner.....	41
Gambar 4.8	Setelah Melakukan <i>Blocking</i> Port pada Port Scanner.....	42
Gambar 4.9	Tampilan njRAT	43
Gambar 4.10	Tampilan setelah terinfeksi oleh njRAT	43



DAFTAR LAMPIRAN

Lampiran 1	Instalasi Snort.....	48
Lampiran 2	Instalasi Suricata.....	48
Lampiran 3	Dashboard Cacti	49
Lampiran 4	Konfig awal IDS	49
Lampiran 5	IDS setelah diinstall	50
Lampiran 6	Hasil Instalasi rrd tool.....	50
Lampiran 7	Hasil Instalasi Lamp	51
Lampiran 8	Hasil Instalasi SNMP.....	51
Lampiran 9	Hasil Instalasi Cacti.....	52
Lampiran 10	Suricata tidak mendeteksi serangan dengan mode IDS	52
Lampiran 11	Buat password pada web cacti	53
Lampiran 12	Simulasi serangan dengan LOIC	53
Lampiran 13	Simulasi serangan dengan Port Scanner	54
Lampiran 14	Simulasi serangan dengan nJRAT	54
Lampiran 15	Graph Cacti sebelum ada aktifitas pada penggunaan memori	55
Lampiran 16	Graph Cacti setelah aktifitas pada penggunaan memori.....	55
Lampiran 17	Graph Cacti setelah aktifitas penggunaan memori.....	56
Lampiran 18	Timer untuk mengukur kecepatan akurasi	56
Lampiran 19	Eksperimen Kedelapan	57
Lampiran 20	Eksperimen Ketujuh	57
Lampiran 21	Eksperimen Keenam	58
Lampiran 22	Eksperimen Kelima	58
Lampiran 23	Eksperimen Keempat	59
Lampiran 24	Eksperimen Ketiga	59
Lampiran 25	Eksperimen Kedua.....	60
Lampiran 26	Eksperimen Pertama	60