

**ANALISIS SNORT IDS DAN HONEYPOT UNTUK MEREDUKSI
SERANGAN DISTRIBUTED DENIAL-OF-SERVICES (DDOS)
PADA LINUX VIRTUAL SERVER**

SKRIPSI



disusun oleh

Fajar Ramadhan Ilhamullah

17.11.1046

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

**ANALISIS SNORT IDS DAN HONEYBOT UNTUK MEREDUKSI
SERANGAN DISTRIBUTED DENIAL-OF-SERVICES (DDOS)
PADA LINUX VIRTUAL SERVER**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Fajar Ramadhan Ilhamullah

17.11.1046

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021**

PERSETUJUAN

SKRIPSI

**ANALISIS SNORT IDS DAN HONEYPOT UNTUK MEREDUKSI
SERANGAN DISTRIBUTED DENIAL-OF-SERVICES (DDOS)
PADA LINUX VIRTUAL SERVER**

yang dipersiapkan dan disusun oleh

Fajar Ramadhan Ilhamullah

17.11.1046

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Januari 2021

Dosen Pembimbing,

Andika Agus Slameto, M.Kom

NIK. 190302109

PENGESAHAN

SKRIPSI

**ANALISIS SNORT IDS DAN HONEYPOT UNTUK MEREDUKSI
SERANGAN DISTRIBUTED DENIAL-OF-SERVICES (DDOS)
PADA LINUX VIRTUAL SERVER**

yang dipersiapkan dan disusun oleh

Fajar Ramadhan Ilhamullah

17.11.1046

telah dipertahankan di depan Dewan Penguji

pada tanggal 19 Juli 2021

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Andika Agus Slameto, M.Kom.
NIK. 190302109

Donni Prabowo, M.Kom.
NIK. 190302253

Arif Dwi Laksito, M.Kom.
NIK. 190302240

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 15 Agustus 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom.

PERNYATAAN

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 31 Juli 2021



Fajar Ramadhan Ilhamullah
NIM 17.11.1046

MOTTO

“Be better than you were yesterday”



PERSEMBAHAN

Saya mempersembahkan skripsi ini kepada semua pihak yang terlibat secara langsung maupun tidak langsung dalam proses pembuatan skripsi.

1. Tuhan Yang Maha Esa yang sudah menguatkan saya dalam menghadapi segala hal.
2. Saya dedikasikan untuk ibu tercinta Sarinah dan ayah Ahmad Joko Purwoto, semoga sehat selalu dan di berikan kemudahan dalam segala hal.
3. Saudara laki-laki Reza Rizki Reynaldo yang selalu memberikan motivasi dan semangat kepada penulis.
4. Bapak Andika Agus Slameto, M.Kom yang sudah membimbing saya dalam pembuatan skripsi dari awal hingga selesai.
5. Dosen-dosen Universitas AMIKOM Yogyakarta yang telah berbagi ilmu dan pengalaman selama masa perkuliahan.
6. Deninta Raefanty Nadya yang selalu setia menemani dan memberikan semangat selama proses pembuatan skripsi ini.
7. Zulfan Ramadhan, Bambang wijayanto, Rochim, M Zaqi Raichan dan teman-teman Informatika-02 2017 teman berproses bersama selama kuliah, semoga kita sama-sama menjadi manusia yang bermanfaat.
8. Terakhir, untuk mereka yang tidak bisa disebutkan satu persatu, terimakasih teruntuk siapapun yang tidak pernah mementingkan dirinya sendiri.

KATA PENGANTAR

Puji dan syukur saya panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan kekuatan kepada saya sehingga dapat menyelesaikan skripsi yang berjudul Analisis dan Perancangan Media Pembelajaran Hewan Prasejarah yang Terdapat di Indonesia Berbasis Multimedia.

Skripsi ini saya buat guna menyelesaikan studi jenjang Strata Satu (S1) pada program studi Informatika Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang strata satu dan untuk memperoleh gelar Sarjana Komputer. Dengan selesainya skripsi ini maka pada kesempatan ini saya mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas AMIKOM Yogyakarta
2. Bapak Hanif Al Fatta, S.Kom., M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Andika Agus Slameto, M.Kom. selaku dosen pembimbing yang selalu bijaksana memberikan bimbingan dan arahan selama proses pembuatan skripsi ini.
4. Dosen Penguji (Donni Prabowo, M.Kom., Arif Dwi Laksito, M.Kom.) dan segenap dosen dan karyawan Universitas AMIKOM Yogyakarta yang telah berbagi ilmu dan pengalaman.
5. Kedua orang tua dan keluarga saya untuk doa dan ridho nya.
6. Semua pihak yang sudah memberikan semangat dan membantu dalam proses pembuatan secara langsung maupun tidak langsung.

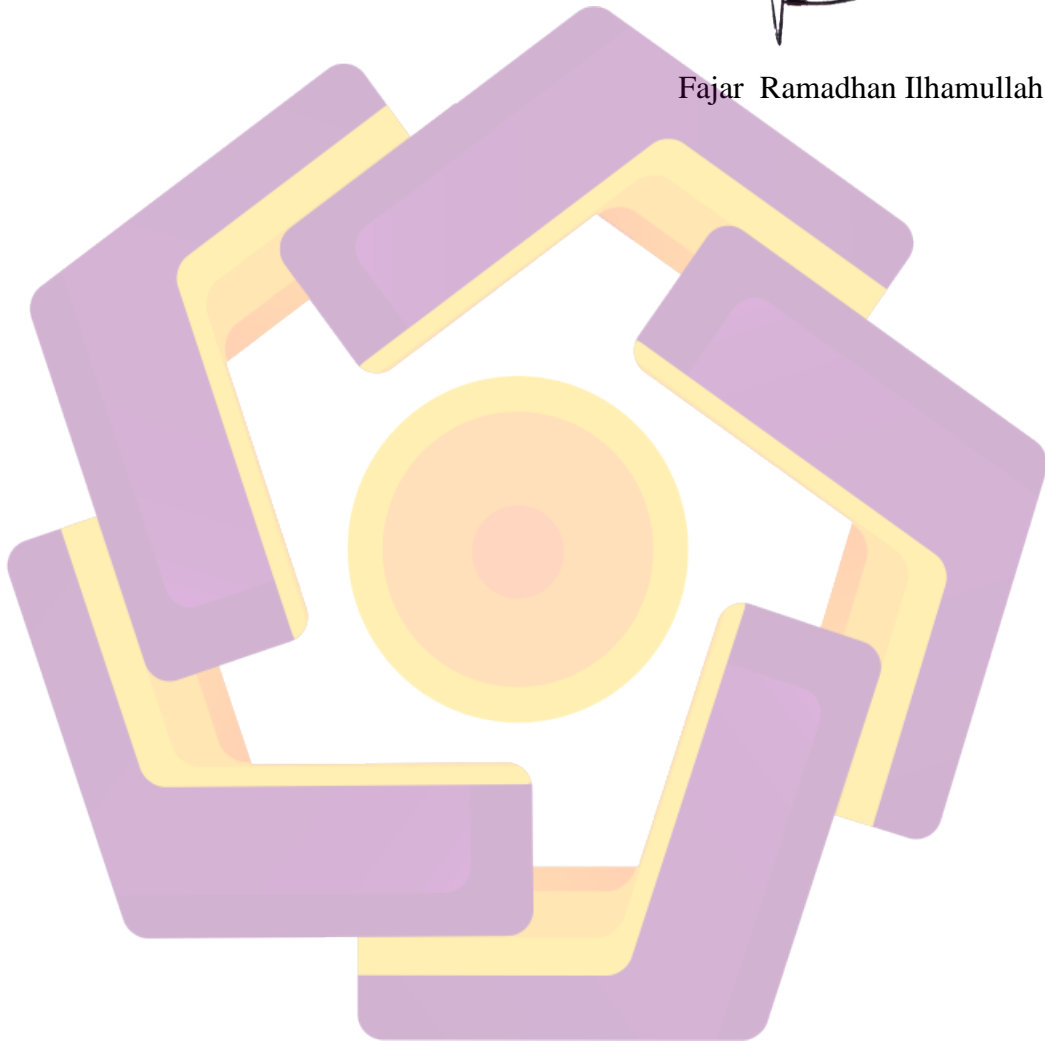
Semoga Tuhan memberikan kebaikan untuk semua yang telah ikut membantu saya hingga skripsi ini dapat selesai. Demi perbaikan selanjutnya, kritik dan saran yang membangun diterima dengan senang

hati. Semoga skripsi ini dapat bermanfaat untuk saya dan kita semua.

Yogyakarta, 31 Juli 2021



Fajar Ramadhan Ilhamullah



DAFTAR ISI

PERSETUJUAN	i
PENGESAHAN	ii
PERNYATAAN	iii
MOTTO	iv
PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
ABSTRACT	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	4
1.4 Maksud dan Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
1.6 Metode Penelitian	5
1.7 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	8
2.1 Kajian Pustaka	8
2.2 Landasan Teori	21
2.2.1 Jaringan Komputer	21
2.2.2 Terminologi Jaringan Komputer	21
2.2.3 Keamanan Jaringan	26
2.2.4 Honeypot	27
2.2.5 Honeyd	32
2.2.6 Snort IDS	35
2.2.7 Scanning	37
2.2.8 Serangan Ddos.....	39
2.2.9 Linux Virtual Server (LVS)	41

2.2.10 Security Policy Development Life Cycle	42
2.2.11 Iptraf	44
BAB III ANALISIS PERANCANGAN SISTEM	46
3.1 Analisis Masalah.....	46
3.2 Identifikasi Masalah.....	52
3.3 Solusi Permasalahan	53
3.4 Analisis Kebutuhan Perangkat	54
3.5 Rancangan Sistem	57
3.5.1 Topologi Sistem	57
3.5.2 Skema Simulasi Jaringan.....	60
3.5.3 Rancangan Pengujian	62
3.5.4 Skenario Pengujian.....	63
BAB IV IMPLEMENTASI DAN PEMBAHASAN	64
4.1 IMPLEMENTASI.....	64
4.1.1 Instalasi Sistem Operasi Pada Virtual Machine	64
4.1.2 Konfigurasi Linux 18.04.5 sebagai router.....	77
4.1.3 Konfigurasi Server Web Apache 2 Untuk Server 1,Server 2 Dan Honeypot.....	85
4.1.4 Konfigurasi LVS (Linux Virtual Server)	89
4.1.5 Instalasi Dan Konfigurasi Snort Pada Virtual Machine LVS.....	95
4.1.6 Instalasi Nmap Pada Attacker	97
4.1.7 Instalasi Ddos tools pada attacker	99
4.2 PENGUJIAN.....	101
4.2.1 Pengujian Fungsional Snort IDS	101
4.2.2 Pengujian terhadap port scanning.....	103
4.2.3 Pengujian Metode Pengalihan Honeypot	104
4.2.4 Pengujian terhadap kinerja CPU dalam menghadapi serangan ddos setelah di lakukan pengalihan serangan.....	107
4.2.5 Pengujian pencatatan Log Serangan.....	110
4.3 HASIL PENGUJIAN DAN PEMBAHASAN.....	111
4.3.1 Hasil Pengujian Pada Sistem.....	111
4.3.2 Hasil Pengujian Pada Serangan.....	112
BAB V PENUTUP.....	115

5.1 Kesimpulan	115
5.2 Saran.....	116



DAFTAR TABEL

Tabel 2. 1 Kajian Pustaka	11
Tabel 2. 2 Tabel Tingkat Interaksi Honeypot	31
Tabel 2. 3 Perintah Nmap Basic Scans.....	37
Tabel 2. 4 Perintah Nmap Advanced Scans.....	38
Tabel 3. 1 Spesifikasi Virtual Machine Komputer Real Server (Server 1 dan Server 2).....	54
Tabel 3. 2 Spesifikasi Virtual Machine LVS Director	54
Tabel 3. 3 Spesifikasi Virtual Machine Honeypot Server	55
Tabel 3. 4 Spesifikasi Virtual Machine PC Router	55
Tabel 3. 5 Spesifikasi Virtual Machine Attacker	55
Tabel 3. 6 Spesifikasi Virtual Machine Client.....	56
Tabel 3. 7 Kebutuhan Perangkat Lunak	56
Tabel 4. 1 Hasil Pengujian pada Sistem.....	111

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Jaringan LAN	22
Gambar 2. 2 Ilustrasi Jaringan MAN	23
Gambar 2. 3 Ilustrasi Jaringan WAN.....	25
Gambar 2. 4 Iustrasi Jaringan Internet.....	26
Gambar 2. 5 Penempatan Eksternal Honeypot.....	28
Gambar 2. 6 Penempatan Internal Honeypot	29
Gambar 2. 7 Penempatan Honeypot Pada DMZ	30
Gambar 2. 8 Jaringan Dengan Sejumlah Unused IP	33
Gambar 2. 9 Honeyd bisa memonitor unused IP.....	33
Gambar 2. 10 Contoh virtual Honeypot dengan bermacam sistem operasi.....	34
Gambar 2. 11 Ilustrasi serangan ddos	40
Gambar 2. 12 Sumber Arsitektur Linux Virtual Server Zhang[18].....	42
Gambar 2. 13 Struktur SPDLc	43
Gambar 3. 1 Web server normal	47
Gambar 3. 2 Port scanning dengan nmap	48
Gambar 3. 3 LVS menangkap adanya aktivitas port scanning.....	48
Gambar 3. 4 Paket yang dikirim	49
Gambar 3. 5 Menerima Paket Serangan.....	49
Gambar 3. 6 Web server 1 dan 2 down.....	50
Gambar 3. 7 Trafik Jaringan Pada Server 1 dan 2	51
Gambar 3. 8 Kinerja proses komputer host atau server 1 dan 2 sebelum adanya serangan DDoS.....	51
Gambar 3. 9 Kinerja proses komputer host atau server 1 dan 2 setelah adanya serangan DDoS.....	52
Gambar 3. 10 Topologi Sistem.....	57
Gambar 3. 11 Skema Simulasi Jaringan.....	60
Gambar 3. 12 Alur Rancang Pengujian.....	62
Gambar 4. 1 Loading Booting Install Ubuntu 18.04.5 Dekstop.....	65

Gambar 4. 2 Untuk Mulai Install Ubuntu 18.04.5 Dekstop	65
Gambar 4. 3 Keyboard Layout	66
Gambar 4. 4 Updates and Other Software	66
Gambar 4. 5 Installation Type	67
Gambar 4. 6 Setting Lokasi	67
Gambar 4. 7 Setting Username dan Password	68
Gambar 4. 8 Instalasi Berjalan	68
Gambar 4. 9 Instalasi Selesai	69
Gambar 4. 10 Tampilan Instalasi Berhasil	69
Gambar 4. 11 Bahasa Ubuntu 16.04.7 Server	69
Gambar 4. 12 Install Ubuntu	70
Gambar 4. 13 Layout Keyboard	70
Gambar 4. 14 Pilih Lokasi	71
Gambar 4. 15 Setting Hostname	71
Gambar 4. 16 Setting Username	72
Gambar 4. 17 Setting Password	72
Gambar 4. 18 Membuat Partisi	73
Gambar 4. 19 Proses Instalasi Berjalan	73
Gambar 4. 20 No Automatic Update	73
Gambar 4. 21 Proses Instalasi Selesai	74
Gambar 4. 22 Tampilan Linux Ubuntu 16.04.7 Berhasil Di Install	74
Gambar 4. 23 Download Kali Linux 2021 Vbox	75
Gambar 4. 24 Memulai Instalasi Kali Linux	75
Gambar 4. 25 Proses Import SO Kali Linux	76
Gambar 4. 26 Berhasil Import SO Kali Linux	76
Gambar 4. 27 Tampilan Kali Linux Setelah Berhasil Di Install	77
Gambar 4. 28 Tampilan Perintah Ifconfig	78
Gambar 4. 29 Setting Ip Tiap Ethernet	79
Gambar 4. 30 Tampilan Perintah Ifconfig	80
Gambar 4. 31 Tampilan Router Table	81
Gambar 4. 32 Setting Ip Server 1 Dan 2	82

Gambar 4. 33 Setting Ip Address LVS dan Honeypot.....	83
Gambar 4. 34 Setting Ip Address Attacker dan Client	84
Gambar 4. 35 Test Ping Antar PC.....	85
Gambar 4. 36 Test Ping Google.Com	85
Gambar 4. 37 Profil Aplkasi UFW	86
Gambar 4. 38 UFW Status	87
Gambar 4. 39 Server Web Pada Server 1	88
Gambar 4. 40 Server Web Pada Server 2	88
Gambar 4. 41 Server Web Pada Honeypot.....	89
Gambar 4. 42 Forward IP	91
Gambar 4. 43 Setting Ipvadm Berhasil	93
Gambar 4. 44 Rules Kernel ip_vs_rr ke Honeypot.....	94
Gambar 4. 45 Versi Snort.....	96
Gambar 4. 46 Option Rules Snort	97
Gambar 4. 47 Instalasi Nmap Berhasil	98
Gambar 4. 48 apt-get install hping3	99
Gambar 4. 49 Versi Hping3.....	100
Gambar 4. 50 Perintah-Perintah Pada Hping3.....	100
Gambar 4. 51 Versi Snort.....	101
Gambar 4. 52 Status snort.conf	102
Gambar 4. 53 Nmap Port Scanning.....	103
Gambar 4. 54 Snort IDS alert port scanning.....	104
Gambar 4. 55 Reply Request dibawah 4000.....	105
Gambar 4. 56 Reply Request diatas 4000	106
Gambar 4. 57 Cpu Usage Server 1	107
Gambar 4. 58 Cpu Usage Server 2	108
Gambar 4. 59 Cpu usage honeypot server	109
Gambar 4. 60 Log blacklist	110
Gambar 4. 61 Presentase CPU Usage pada LVS standar	113
Gambar 4. 62 Persentase CPU Usage LVS Honeypot	114

INTISARI

Perkembangan dunia internet membuat penyedia layanan harus mempertimbangkan banyaknya pengguna yang terus bertambah.. Sebuah server pasti memiliki keterbatasan dalam kemampuan menangani pengguna. Salah satu cara untuk mengatasi hal tersebut adalah dengan penambahan jumlah server. Dengan penambahan server, layanan yang sudah ada tetap berjalan ketika proses konfigurasi sedang dilakukan. Sehingga tidak akan sampai mematikan layanan. Meskipun demikian, penambahan server saja akan cukup merepotkan apabila tidak diatur dengan baik. Penambahan server tentu harus dilakukan dalam waktu yang cepat dan sebisa mungkin tidak diketahui oleh user.

Untuk mengatasi hal-hal tersebut, bisa digunakan Linux Virtual Server (LVS). LVS sebagai salah satu bentuk kumpulan server dapat juga terkena serangan Distributed Denial of Services (DDOS), sebuah serangan yang bertujuan untuk membuat suatu layanan tidak dapat diakses oleh pengguna yang sah. Karena itu, untuk meminimalisir efek dari serangan ini difungsikan Snort IDS dan Honeypot. Tujuannya agar penyerang mengira serangannya berhasil, padahal yang terjadi adalah Snort IDS dan honeypot berhasil menjebak ke server palsu dan mendeteksi IP serta menghasilkan filelog penyerang.

Dari hasil ujicoba, setelah sistem ini diterapkan dengan mengukur kinerja CPU usage yang di serang sebanyak 4x diatas 4000 request/detik menunjukkan real server tetap berjalan normal dengan CPU Usage rata-rata di bawah 50% sedangkan pada honeypot server sebagai server palsu, CPU usage rata-rata sebesar di atas 80%

Kata kunci : Snort IDS, Honeypot, File Log, Ddos, LVS

ABSTRACT

The development of the internet world makes service providers have to consider the increasing number of users. A server must have limitations in the ability to handle users. One way to overcome this is to increase the number of servers. With the addition of a server, existing services will continue to run while the configuration process is being carried out. So it will not turn off the service. However, just adding a server will be quite a hassle if it is not managed properly. The addition of a server must of course be done in a fast time and as much as possible not known by the user.

To overcome these things, Linux Virtual Server (LVS) can be used. LVS as a form of server pool can also be exposed to Distributed Denial of Services (DDOS) attacks, an attack that aims to make a service inaccessible to authorized users. Therefore, to minimize the effects of this attack, Snort IDS and Honeypot are enabled. The goal is for the attacker to think the attack was successful, even though what happened was that Snort IDS and the honeypot managed to trap the fake server and detect the IP and generate the attacker's filelog.

From the test results, after this system was implemented by measuring the performance of the CPU usage that was attacked as much as 4x above 4000 requests/second, it showed that the real server was still running normally with an average CPU Usage below 50% while on the honeypot server as a fake server, the CPU usage was average. average of above 80%

Keywords : *Snort IDS, Honeypot, Filelog, Ddos, LVS*