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

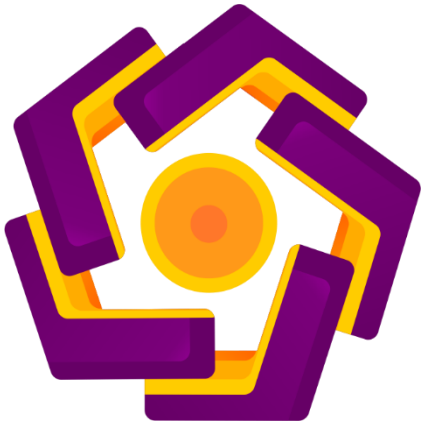
PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2021

ANALISIS SNORT IDS DAN HONEYPOT 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.

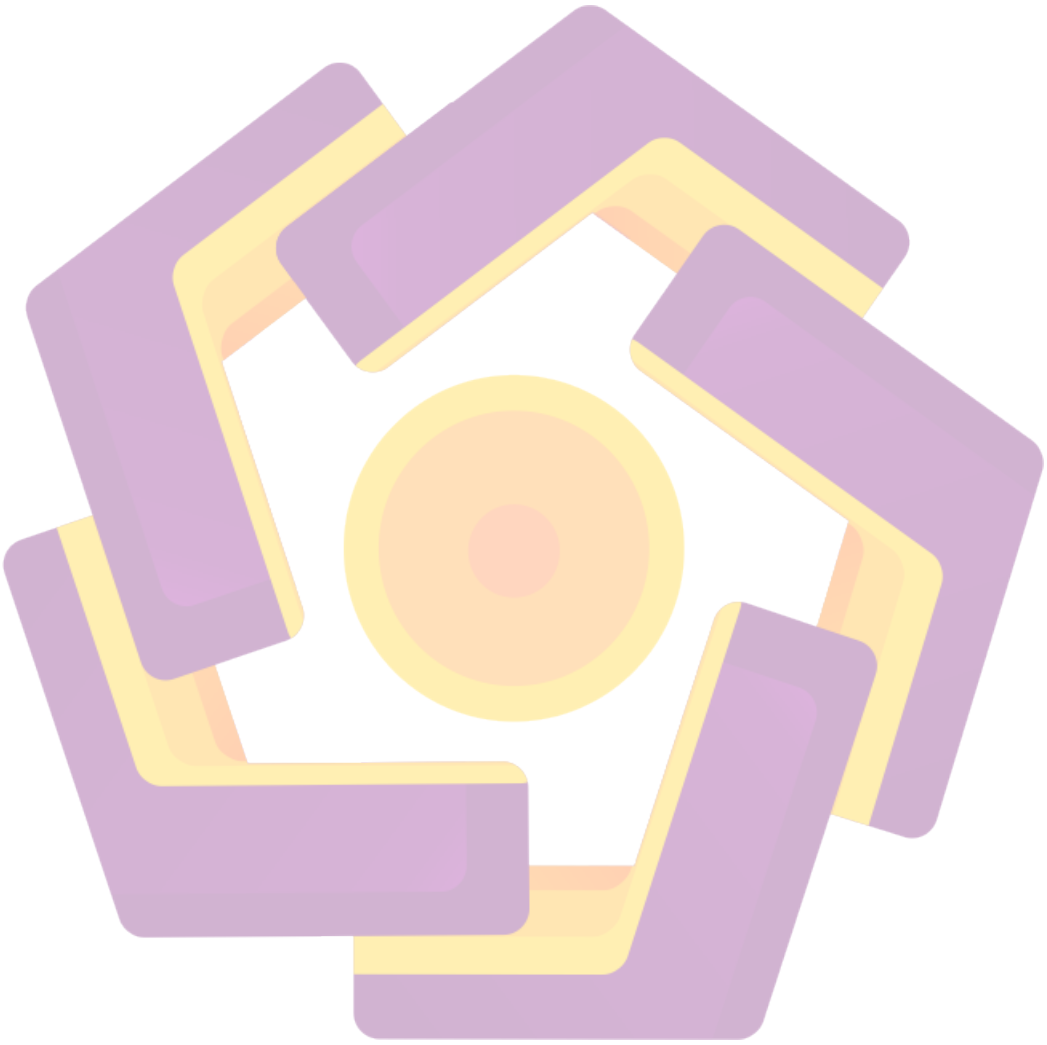
Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

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 menyesaikan 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

DAFTAR TABEL

DAFTAR GAMBAR

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 berhasill 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 menunjukan 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*