ANALISIS PERBANDINGAN PERFORMASI UNCOMPLICATED FIREWALL (UFW) DAN CLOUDFLARE DALAM RANGKA MITIGASI SERANGAN DISTRIBUTED DENIAL OF SERVICE(DDOS)

SKRIPSI

disusun oleh:

Melfan Afandi

16.11.0143

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

2022

ANALISIS PERBANDINGAN PERFORMASI UNCOMPLICATED FIREWALL (UFW) DAN CLOUDFLARE DALAM RANGKA MITIGASI SERANGAN DISTRIBUTED DENIAL OF SERVICE(DDOS)

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai gelar Sarjana
Pada program Studi Informatika

disusun oleh:

Melfan Afandi

16.11.0143

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022

PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMANSI UNCOMPLICATED FIREWALL(UFW) DAN CLOUDFLARE DALAM RANGKA MITIGASI SERANGAN DISTRIBUTED DENIAL OF SERVICE(DDOS)

yang dipersiapkan dan disusun oleh

Melfan Afandi

16.11.0143

telah disetujuai oleh Dosen Pembimbing

Skripsi pada tanggal 10 Februari 2022

Dosen Pembimbing,

Nila Feby Puspitasari,S.Kom,M.Cs

NIK. 190302161

PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN PERFORMANSI UNCOMPLICATED FIREWALL(UFW) DAN CLOUDFLARE DALAM RANGKA MITIGASI SERANGAN DISTRIBUTED OF SERVICE (DDOS)

yang dipersiapkan dan disusun oleh

Melfan Afandi

16.11.0143

telah dipertahankan di depan Dewan Penguji pada
tanggal 17 Februari 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Wahyu Sukestyastama Putra, S.T., M.Eng **NIK. 190302328**	
Anggit Ferdita Nugraha, S.T.,M.Eng **NIK. 190302480**	
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer

Tanggal 25 Februari 2022

DEKAN FAKULTAS ILMU KOMPUTER

HANIF AL FATTA, M.KOM
NIK. 190302096

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, 08 Maret 2022

Melfan Afandi
16.11.0143

MOTTO

Never give up and keep pushing through , you’re almost there.

(**Melfan Afandi**)

Tak ada sesuatu apapun yang instan, terlebih sesuatu yang kau impikan

(**Melfan Afandi**)

Tidak usah takut gagal. bekerjalah semaksimal mungkin dan percayalah bahwa semua jerih payah kita akan diperhitungkan oleh tuhan.

(**Merry Riana**)

PERSEMBAHAN

Puji syukur yang tak terhingga Saya ucapkan kepada Allah SWT, Tuhan Maha Esa yang telah meridhoi dan mengabulkan segala do'a sehingga penulis dapat menyelesaikan Skripsi berjudul **"Analisis Perbandingan Performasi Uncomplicated Firewall (UFW) Dan Cloudflare Dalam Rangka Mitigasi Serangan Distributed Denial Of Service (DDOS)"** sesuai dengan yang diharapkan oleh penulis. Alhamdulillah, dengan rasa bangga dan bahagia penulis persembahkan skripsi ini kepada:

1. Allah SWT karena atas izin dan karunia-Nya maka skripsi ini dapat dibuat dan selesai pada waktunya.
2. Kedua orang tua, yaitu Ibu dan Bapak yang banyak memberi dukungan dan do'a.
3. Ibu Nila Feby Puspitasari, S.kom,M.Cs selaku dosen pembimbing, terima kasih sudah membimbing dan membantu saya dalam pengerjaan skripsi. Terima kasih atas segala kesabaran dan ilmu yang diberikan selama ini.
4. Dan yang terakhir saya ucapkan terimakasih kepada teman-teman dan pasangan saya yaitu Mas Ulza , Hari, dan Novia Resta Burhan, Yang telah membantu banyak hal yang berkaitan dengan penelitian ini.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah, dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diharapkan. Tidak lupa sholawat dan salam penulis haturkan pada junjungan umat yaitu Nabi Muhammad SAW yang telah menuntun kita pada jalan kebaikan.

Skripsi ini disusun dalam rangka memenuhi salah satu persyaratan kelulusan jenjang Program Sarjana Strata 1 pada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta. Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada:

1. Ibu dan Bapak saya, yang selalu menyelipkan doa di setiap sujudnya.
2. Bapak Prof. Dr. M. Suyanto, M.M. , selaku Rektor Universitas AMIKOM Yogyakarta.
3. Ibu Nila Feby Puspitasari,S.Kom,M.Cs selaku Dosen Pembimbing yang telah memberikan bimbingan, saran, dan waktunya dengan sepenuh hati.
4. Bapak Sukestyastama Putra,S.T.,M.Eng dan Bapak Anggit Ferdita Nugraha,S.T., M.Eng sebagai dosen penguji serta semua dosen Prodi Informatika Universitas Amikom Yogyakarta, terima kasih atas semua jasa Bapak dan Ibu Dosen.

5. Segenap Dosen dan Civitas Akademika Universitas AMIKOM Yogyakarta yang telah memberikan banyak ilmu dan pengalaman kepada penulis selama menjalani perkuliahan.
6. Seluruh pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu sehingga skripsi ini dapat terselesaikan.

Penulis tentunya menyadari bahwa pembuatan skripsi ini masih banyak kekurangan dan kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 8 Maret 2022

Melfan Afandi

16.11.0143

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Analisa aktivitas jaringan perlu dilakukan untuk mengetahui aktivitas yang mencurigakan guna melakukan pencegahan dari serangan jaringan. *Network forensics* salah satu teknik dalam forensika digital yang digunakkan untuk mencatat, menangkap dan menganalisa aktivitas jaringan untuk menemukan bukti digital dari suatu serangan menggunakan jaringan komputer sehingga pelaku bisa dapat dituntut sesuai hukum yang berlaku contoh serangan menggunakkan jaringan komputer adalah *Denial Of Service (Dos)*, Spoofing, Phishing, Sniffing. Bukti digital pada forensik jaringan dapat diketahui dari pola serangan yang dikenali atau penyimpangan dari kondisi tanpa serangan jaringan. Penelitian ini merupakan analisis dari kondisi tanpa serangan jaringan.

Penelitian ini merupakan analisis dari skenario yang bertujuan untuk menginvestigasi dan menganalisa serangan DoS dengan cara mengumpulkan log data dari wireshark, membuat analisa antar skenario pada Ubuntu Server 21.04. menggunakan protokol HTTP. Terdapat dua perlakuan terhadap server yaitu menggunakan UFW dan menggunakan Cloudflare. Server diserang menggunakan tools seperti Low Orbit Ion Cannon (Loic). Setelah dilakukan pembuatan skenario maka tahap selanjutnya adalah pengujian antara Virtual Private Server dengan Komputer penyerang agar mengetahui apakah jaringan sudah terhubung dan sebagai tahap monitoring jaringan pada kondisi tanpa serangan. Setelah dilakukan pengujian komunikasi, tahap selanjutnya merupakan Penyerangan ddos menggunakan loic terhadap target. Penyerangan ddos ini ditargetkan pada port 80. Tahap selanjutnya adalah analisa bukti digital. Metode yang digunakan adalah anomaly-based detection. Metode ini bertujuan untuk membandingkan kondisi tanpa serangan traffic jaringan yang tanpa serangan dengan traffic jaringan yang telah dilakukan skenario. Tools yang digunakan pada analisa adalah wireshark. Hal yang dilihat adalah log wireshark dari expert information, conversation antar server dan penyerang lalu kinerja server dengan system monitor.

Hasil penelitian yang dilakukan adalah log wireshark dan conversation pada Ubuntu Server 21.04. penggunaan *UFW* dan *Cloudflare* masih sangat dapat diimplementasikan pada sector web ringan dengan load database yang masih sederhana dengan pengeluaran cost yang sangat minim ditambah kemanan yang baik.

.

Kata Kunci: : Network Forensics, Wireshark, DOS, Denial of Service

ABSTRACT

Analysis of network activity needs to be done to find out suspicious activities to prevent network attacks. Network forensics is one of the techniques in digital forensics that is used to record, capture and analyze network activity to find digital evidence of an attack using a computer network so that the perpetrator can be prosecuted according to applicable law. Examples of attacks using computer networks are Denial of Service (Dos), Spoofing, Phishing, Sniffing. Digital evidence in network forensics can be identified from recognized attack patterns or deviations from the no-attack state of the network. This research is an analysis of the conditions without network attacks

This research is an analysis of scenarios that aims to investigate and analyze DoS attacks by collecting log data from Wireshark, analyzing scenarios on Ubuntu Server 21.04. using the HTTP protocol. There are two treatments for the server, namely using UFW and using Cloudflare. Servers are attacked using tools such as Low Orbit Ion Cannon (Loic). After making the scenario, the next stage is testing between the Virtual Private Server and the attacker's computer to find out whether the network is connected and as a stage of network monitoring in conditions without attacks. After testing the communication, the next stage is a ddos attack using loic against the target. This ddos attack is targeted at port 80. The next stage is digital evidence analysis. The method used is anomaly-based detection. This method aims to compare conditions without attack network traffic without attack with network traffic that has been carried out in scenarios. The tools used in the analysis are wireshark. The things seen are wireshark logs from expert information, conversations between servers and attackers and then server performance with system monitoring.

The results of this research are Wireshark logs and conversations on Ubuntu Server 21.04. the use of UFW and Cloudflare can still be implemented in the lightweight web sector by loading a database that is still simple at a very minimal cost plus good security.

Keywords : Network Forensics, Wireshark, DOS, Denial of Service