ANALISIS SISTEM KEAMANAN JARINGAN HOST DAN SERVER MENGGUNAKAN METODE TRAFFIC FLOODING

SKRIPSI

disusun oleh

Muhammad Yusuf Alwi

16.11.0111

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

2021

ANALISIS SISTEM KEAMANAN JARINGAN HOST DAN SERVER MENGGUNAKAN METODE TRAFFIC FLOODING

SKRIPSI

untuk memenuhi sebagian persyaratan

mencapai gelar Sarjana

pada Program Studi Informatika

Muhammad Yusuf Alwi

16.11.0111

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

PERSETUJUAN

SKRIPSI

ANALISIS SISTEM KEAMANAN JARINGAN HOST DAN SERVER MENGGUNAKAN METODE TRAFFIC FLOODING

yang dipersiapkan dan disusun oleh

Muhammad Yusuf Alwi

16.11.0111

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 30 Oktober 2019

Dosen Pembimbing,

Yudi Sutanto, M. Kom
NIK. 190302039

PENGESAHAN

SKRIPSI

ANALISIS SISTEM KEAMANAN JARINGAN HOST DAN SERVER MENGGUNAKAN METODE TRAFFIC FLOODING

yang disusun oleh

Muhammad Yusuf Alwi

16.11.0111

telah dipertahankan di depan Dewan Penguji
pada tanggal 30 Juli 2021

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Donni Prabowo, M.Kom **NIK. 190302253**	_____
Senie Destya, M.Kom **NIK. 190302312**	_____
Yudi Sutanto, M. Kom **NIK. 190302039**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 30 Agustus 2021

Dekan Fakultas Ilmu Komputer

Hanif Al Fatta,S.Kom., M.Kom
NIK. 190302096

PERNYATAAN

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI) dan isi dalam skripsi ini tidak terdapat karya institusi pendidikan 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, 6 Agustus 2021

Muhammad Yusuf Alwi
NIM. 16.11.0111

MOTO

"Allah akan meninggikan orang-orang yang berilmu di antaramu dan orang-orang yang diberi ilmu pengetahuan beberapa derajat. Dan Allah Maha Mengetahui apa yang kamu kerjakan"

(Q.S. Al Mujadilah : 11)

"Apa yang kita hasilkan sekarang hanyalah sedikit bagian dari kehidupan ini, jalani hidup ini dengan penuh semangat dan do'a"

(Muhammad Yusuf Alwi)

PERSEMBAHAN

Dengan mengucap Alhamdulillah sebagai rasa syukur kepada Allah Subhanahu wa Ta'ala atas segala nikmat dan karuniaNya sehingga skripsi ini bisa terselesaikan. Pada kesempatan ini tak lupa penulis ucapkan terimakasih kepada:

1. Allah SWT, karena berkat izin-Nya dan karunia-Nya skripsi ini dapat terselesaikan.
2. Ayah dan Ibu yang telah memberikan doa, motivasi, semangat, kasih, sayang dan pengorbanan yang telah diberikan.
3. Kakak, adikku (Wahyuni Alwi, Muthmainnah Alwi, dan Arif Arif Alwi) yang selalu mendoakan dan memberi semangat.
4. Bapak Yudi Sutanto, M.Kom sebagai dosen pembimbing yang telah mencurahkan waktu untuk membimbing perjalanan penyusunan skripsi ini dari awal hingga akhir.
5. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu yang bermanfaat.
6. Keluarga Besar 16-S1-IF-02 yang telah menemani masa perkuliahan di Universitas Amikom Yogyakarta.
7. Dan teman-teman saya yang tidak bisa saya tulis satu persatu, saya ucapkan banyak terimakasih.

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Allah SWT yang selalu melimpahkan rahmat dan karunia-nya kepada setiap hamba-nya dan tak lupa shalawat serta salam kepada junjungan Nabi besar kita, Nabi Muhammad SAW.

Skripsi ini dibuat sebagai salah satu syarat kelulusan Program Strata-1 Jurusan Informatika Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta dan untuk memeroleh gelar Sarjana Komputer.

Dengan selesainya skripsi yang berjudul " Implementasi Realtime Response ", dengan ini peneliti mengucapkan terimakasih yang sebesar-besarnya kepada :

Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor UNIVERSITAS AMIKOM YOGYAKARTA.

Bapak Hanif Al Fatta,S.Kom., M.Kom, selaku Dekan Fakultas Ilmu Komputer UNIVERSITAS AMIKOM YOGYAKARTA.

Ibu Windha Mega PD, M.Kom., selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Bapak Yudi Sutanto, M.Kom. selaku dosen pembimbing yang telah memberikan bimbingan dan ilmu yang bermanfaat kepada penulis selama melakukan bimbingan skripsi.

Segenap dosen Universitas Amikom Yogyakarta yang telah memberikan pengajaran ilmu-ilmu baru selama masa perkuliahan.

Bapak, Ibu, Kakak, Adik dan semua keluarga tercinta yang telah begitu tulus memberikan semangat, dorongan dan doa yang bermanfaat bagi penulis.

Sahabat-sahabat yang telah membantu dan memberikan dukungan dalam berbagai bentuk.

Keluarga Besar 16-S1IF-02 yang telah bejuang bersama selama masa perkuliahan hingga sampai saat ini.

Semua pihak yang telah membantu dalam penyelesaiaan skripsi ini yang tidak dapat disebutkan satu persatu.

Dalam penulisan skripsi ini penulis menyadari sepenuhnya akan kekurangan karena keterbatasan pengetahuan dan kemampuan penulis. Oleh karena itu saran dan kritik yang membangun senantiasa diharapkan demi menyempurnakan hasil penelitian ini.

Akhir kata semoga skripsi ini dapat memberikan manfaat bagi pembaca umumnya dan khususnya untuk penulis serta untuk pengembangan sistem pendukung keputusan berikutnya.

Yogyakarta, 6 Agustus 2021

Penulis,

Muhammad Yusuf Alwi

DAFTAR ISI

JUDUL ii
PERSETUJUAN iii
PENGESAHAN iv
PERNYATAAN v
MOTO vi
PERSEMBAHAN vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xiii
DAFTAR GAMBAR xiv
Intisari xvi
Abstract xvii
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Maksud dan Tujuan 3
1.5 Manfaat Penelitian 3
1.5.1 Bagi Penulis 3
1.5.2 Bagi Administrator Jaringan 4
1.5.3 Bagi Pembaca 4
1.6 Metode Penelitian 4
1.6.1 Metode Pengumpulan Data 4
1.6.2 Metode Pengembangan 5
1.7 Sistematika Penulisan 6
BAB II 8
LANDASAN TEORI 8
2.1 Tinjauan Pustaka 8

2.2 Dasar Teori 13
2.2.1 Jaringan Komputer 13
2.2.2 Keamanan Jaringan Komputer 14
2.2.3 Aspek-aspek keamanan Komputer 14
2.2.4 Macam-macam kejahatan Komputer 15
2.2.5 Topologi Jaringan 16
2.2.6 IP Address 16
2.2.7 QoS (Quality Of Service) 17
2.2.4.1 Parameter *Quality Of Service (QoS)* 18
2.2.8 Firewall 20
2.2.9 Virtual Private Server 24
2.2.10 Ubuntu Server 26
2.2.11 Protocol HTTP 27
2.2.12 Denial Of Service 28
2.2.13 Traffic Flooding 30
2.3 Metode Pengembangan 32
BAB III 36
METODE PENELITIAN 36
3.1 Metode Pengumpulan Data 36
3.1.1 Studi Literatur 36
3.1.2 Metode Eksperimen 36
3.2 Metode Pengembangan 36
3.2.1 Analisis 36
3.2.2 Desain 45
3.2.3 Implementasi 47
3.2.4 *Enforcement* (Audit) 47
BAB IV 48
IMPLEMENTASI DAN PEMBAHASAN 48
4.1 Implementasi 48
4.2 Pengujian 65
4.2.1 Serangan *Traffic Flooding* 65
4.2.2 Monitoring Jaringan 65

4.3 Hasil Analisis Jaringan 67
4.3.1 Tanpa *Firewall* 67
4.3.2 Menggunakan *Firewall* 71
BAB V 76
PENUTUP 76
5.1 Kesimpulan 76
5.2 Saran 76
DAFTAR PUSTAKA 78

DAFTAR TABEL

Tabel 2.1 Kategori Delay (TIPHON 1999) 18
Tabel 2.2 Kategori Packet Loss (TIPHON 1999) 19
Tabel 2.3 Kategori Throughput (TIPHON 1999) 19
Tabel 2.4 Kategori Jitter (TIPHON 1999) 20
Tabel 3.2 Spesifikasi Laptop 39
Tabel 3.3 Spesifikasi Router Access Point 39
Tabel 3.4 Desain IP Address 46
Tabel 4.2 Hasil Analisis QoS Tanpa Firewall 68
Tabel 4.3 Hasil Analisis QoS Tanpa Firewall Lanjutan 69
Tabel 4.4 Hasil Analisis Server Tanpa Firewall 70
Tabel 4.5 Hasil Analisis Server Tanpa Firewall Lanjutan 71
Tabel 4.6 Hasil Analisis QoS Dengan Firewall 72
Tabel 4.7 Hasil Analisis QoS Dengan Firewall Lanjutan 73
Tabel 4.8 Hasil Analisis Server Dengan Firewall 74
Tabel 4.9 Hasil Analisis Server Dengan Firewall Lanjutan 75

DAFTAR GAMBAR

Gambar 2.1 Tabel Perbandingan Penelitian 9
Gambar 2.2 Tabel Perbandingan Penelitian Lanjutan 10
Gambar 2.3 Tabel Perbandingan Penelitian Lanjutan 11
Gambar 2.4 Tabel Perbandingan Penelitian Lanjutan 12
Gambar 2.10 Firewall Melindungi Jaringan Lokal 21
Gambar 2.11 Firewall Melindungi Jaringan Lokal 21
Gambar 2.12 Virtual Private Servers 26
Gambar 2.13 Ubuntu Server 27
Gambar 2.14 *Traffic Flooding* 31
Gambar 2.15 *SPDLC* 34
Gambar 3.1 IO Graph Non Firewall Non Attack 44
Gambar 3.2 Resource Non Firewall Non Attack 45
Gambar 3.3 Desain Topologi Jaringan 46
Gambar 4.1 Instalasi *Ubuntu Server* 48
Gambar 4.2 Instalasi Ubuntu Server b Lanjutan 49
Gambar 4.3 Instalasi *Ubuntu Server* c Lanjutan 49
Gambar 4.4 Mengakses Ubuntu Server 50
Gambar 4.5 Mengakses Ubuntu Server Lanjutan 50
Gambar 4.6 Instalasi Desktop Environtment 51
Gambar 4.7 Instalasi Desktop Environtment Lanjutan 52
Gambar 4.8 Instalasi Desktop Environtment Lanjutan 52
Gambar 4.9 Instalasi Desktop Environtment Lanjutan 52
Gambar 4.10 Instalasi Nginx 53
Gambar 4.11 Instalasi Mysql Server 54
Gambar 4.12 Instalasi Mysql Server lanjutan 54
Gambar 4.13 Instalasi Mysql Server lanjutan 55
Gambar 4.14 Instalasi Mysql Server lanjutan 55
Gambar 4.15 Instalasi PHP Server 56
Gambar 4.16 Instalasi PHP Server Lanjutan 57
Gambar 4.17 Instalasi Wireshark 57
Gambar 4.18 Instalasi Wireshark 58
Gambar 4.19 Konfigurasi Web Server 59
Gambar 4.20 Konfigurasi Web Server Lanjutan 59
Gambar 4.21 Konfigurasi Web Server Lanjutan 60
Gambar 4.22 Konfigurasi Web Server Lanjutan 60
Gambar 4.23 Konfigurasi Web Server Lanjutan 61
Gambar 4.24 Konfigurasi Web Server Lanjutan 61
Gambar 4.25 Konfigurasi Web Server Lanjutan 62
Gambar 4.26 Konfigurasi Web Server Lanjutan 62
Gambar 4.27 Konfigurasi Web Server Lanjutan 62
Gambar 4.28 Konfigurasi firewall 63

Gambar 4.29 Konfigurasi firewall Lanjutan 64
Gambar 4.30 Konfigurasi firewall Lanjutan 64
Gambar 4.31 Serangan Traffic Flooding 65
Gambar 4.32 Monitoring Jaringan 66
Gambar 4.33 Monitoring Jaringan Lanjutan 66
Gambar 4.34 Monitoring Jaringan Lanjutan 66
Gambar 4.35 Akses Website Tanpa Firewall 67
Gambar 4.36 Akses Website Dengan Firewall 71

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 18.04. menggunakan protokol HTTP. Terdapat dua perlakuan terhadap server yaitu tanpa firewall dan firewall yang telah dikonfigurasi 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 dos 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 task manager. Hasil penelitian yang dilakukan adalah log wireshark dan conversation pada Ubuntu Server 18.04. Jumlah packet dan jumlah bytes pada saat dilakukan eksperimen tidak mengalami perbedaan yang signifikan. Yang membedakan adalah kinerja. Penggunaan Firewall cukup berpengaruh dalam menangani serangan DoS tersebut.

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

Abstract

Analysis of network activity needs to be done to find out suspicious activity in order to prevent network attacks. Network forensics, 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, for example attacks using computer networks are Denial Of Service (Dos), Spoofing, Phishing, Sniffing. Digital evidence in network forensics can be identified from known attack patterns or deviations from the non-attack state of the network.

This study is an analysis of 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, making analysis between scenarios on Ubuntu Server 18.04. using the HTTP protocol. There are two treatments for the server, namely without a firewall and a firewall that has been configured. The server is 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 step is to attack ddos using loic against the target. This 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 the conditions without attack network traffic without attack with network traffic that has been carried out in the scenario. The tools used in the analysis are wireshark. What is seen is the wireshark log of expert information, the conversation between the server and the attacker, and the server's performance with the task manager. The results of the research conducted are wireshark logs and conversations on Ubuntu Server 18.04. The number of packets and the number of bytes at the time of the experiment did not experience a significant difference. The difference is performance. The use of a firewall is quite influential in dealing with these DoS attacks.

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