IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI

SKRIPSI

Oleh :

ACHMAD RIZAL BAKRI
NPM. 1334010075

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"

JAWA TIMUR

2020

LEMBAR PENGESAHAN SKRIPSI

Judul : **IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI**

Oleh : **ACHMAD RIZAL BAKRI**

NPM : **13340100775**

Telah Diseminarkan Dalam Ujian Skripsi Pada :

Hari Senin, Tanggal 20 Juli 2020

Mengetahui

Dosen Pembimbing	Dosen Penguji
1.	1.
Henni Endah Wahani, ST., M.Kom	Dr. Basuki Rahmat, S.Si, MT.,
NPT : 3 7809 13 0348 1	NPT : 3 6907 06 0209 1
2.	2.
Firza Prima Aditiawan, S.Kom., M.TI	Wahyu Syaifullah J.S, S.Kom., M.Kom
NPT: 3 8605 13 0344 1	NPT : 3 8608 10 0295 1

Menyetujui

Dekan	Koordinator Program Studi
Fakultas Ilmu Komputer	Informatika
Dr. Ir. Ni Ketut Sari, MT	Budi Nugroho, S.Kom, M.Kom.
NPT : 19650731 199203 2 001	NPT : 3 8009 05 0205 1

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAWA TIMUR
FAKULTAS ILMU KOMPUTER

Skripsi 13340100075

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Informatika UPN "Veteran" Jawa Timur, yang bertanda tangan di bawah ini :

Nama : Achmad Rizal Bakri

NPM : 1334010075

Menyatakan bahwa Judul Skripsi / Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul :

"IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)

MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI "

Bukan merupakan plagiat dari Skripsi / Tugas Akhir / Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi / Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN "Veteran" Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 20 Juli 2020

Hormat Saya,

METERAI TEMPEL 0829DAHF529157620 6000 ENAM RIBU RUPIAH

Achmad Rizal Bakri

SURAT PERNYATAAN ANTI PLAGIAT

Saya, mahasiswa Informatika UPN "Veteran" Jawa Timur, yang bertanda tangan di bawah ini :

Nama : Achmad Rizal Bakri

NPM : 1334010075

Menyatakan bahwa Judul Skripsi / Tugas Akhir yang Saya ajukan dan akan dikerjakan, yang berjudul :

"IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS)

MENGGUNAKAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI "

Bukan merupakan plagiat dari Skripsi / Tugas Akhir / Penelitian orang lain dan juga bukan merupakan produk dan atau *software* yang saya beli dari pihak lain. Saya juga menyatakan bahwa Skripsi / Tugas Akhir ini adalah pekerjaan Saya sendiri, kecuali yang dinyatakan dalam Daftar Pustaka dan tidak pernah diajukan untuk syarat memperoleh gelar di UPN "Veteran" Jawa Timur maupun di institusi pendidikan lain.

Jika ternyata di kemudian hari pernyataan ini terbukti tidak benar, maka Saya siap menerima segala konsekuensinya.

Surabaya, 20 Juli 2020

Hormat Saya,

Achmad Rizal Bakri

ABSTRAK

Keamanan suatu informasi sangatlah penting, terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Keamanan jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun luar maka dari itu diperlukan untuk mengamankan informasi tersebut.Salah satu perangkat lunak yang dapat menangkal serangan dari luar adalah *Intrusion Detection System*(IDS).Implementasi IDS yang dilakukan untuk meminimalkan penyusupan adalah dengan menggunakan Telegram sebagai media notifikasi agar administrator segera tahu jik ada penyusup secara real time.Pesan yang dikirim ke Telegram berupa log serangan yang dilakukan oleh penyusup.Serangan tersebut akan terdeteksi ke dalam IDS Snort lalu akan disimpan ke Database MySql pada saat yang bersamaan lalu akan otomatis trigger akan menjalankan Iptable yang sudah didefinisikan lalu akan mengirim ke Telegram administrator. Pada pengujian dapat diketahui sistem mampu mengolah data output dari IDS snort serta dapat mengenali segala aktifitas yang dilakukan penyusup dalam usaha untuk menyusup ke dalam sistem dengan menggunakan Port Scanning berdasarkan rule yang telah diterapkan. Kemudian dilakukan proses blocking terhadap IP address yang dianggap sebagai intruder setelah itu sistem akan memberikan laporan kepada administrator melalui media jejaring sosial dan web monitoring mengenai adanya serangan yang mencoba masuk ke dalam sistem.

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Shalawat dan salam senantiasa tercurah kepada Rasulullah SAW yang mengantarkan manusia dari zaman kegelapan ke zaman yang terang benderang ini. Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian syarat-syarat guna mencapai gelar Sarjana Komputer di Universitas Pembangunan Nasional "Veteran"Jawa Timur

Penulis menyadari bahwa penulisan ini tidak dapat terselesaikan tanpa dukungan dari berbagai pihak baik moril maupun materil. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dalam penyusunan skripsi ini terutama kepada:

Kedua orang tua, ayahanda tercinta Misli Arifin dan ibunda tersayang Eni Susilowati yang telah memberikan dukungan baik moril maupun materil serta doa yang tiada henti-hentinya kepada penulis.

Kedua Adik,Mila Dia Nor Asiya dan Fadhil Muhammad yang telah memberikan semangat dan dukungan yang tiada henti-hentinya kepada penulis.

1. Ibu Dr,Ir.Ni Ketut Sari,MT selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur
2. Bapak Budi Nugroho,S.Kom,M,Kom.selaku Koordinator Program Studi Teknik Informatika Fakultas Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur

3. Ibu Henni Endah Wahanani, ST., M.Kom, selaku dosen Pembimbing Skripsi I yang telah berkenan memberikan tambahan ilmu dan solusi pada setiap permasalahan atas kesulitan dalam penulisan skripsi ini.
4. Bapak Firza Prima Aditiawan, S.Kom., M.TI,selaku dosen Pembimbing Skripsi II yang telah bersedia membimbing dan mengarahkan penulis selama menyusun skripsi dan memberikan banyak ilmu serta solusi pada setiap permasalahan atas kesulitan dalam penulisan skripsi ini.
5. Bapak Dr. Basuki Rahmat, S.Si, MT,selaku dosen Penguji I atas Bimbingan,koreksi dan Arahan yang diberikan.
6. Bapak Wahyu Syaifullah Jauharis Saputra, S.Kom., M.Kom selaku dosen Penguji II atas Bimbingan,koreksi dan Arahan yang diberikan.
7. Seluruh Bapak/Ibu dosen Fakultas Ilmu Komputer yang telah memberikan pengetahuan yang sangat bermanfaat selama masa perkuliahan.
8. Seluruh teman-teman seangkatan, terutama kelas TF-B Angkatan 2013 dan yang selalu mengisi hari-hari menjadi sangat menyenangkan.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dikarenakan terbatasnya pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak. Semoga skripsi ini dapat bermanfaat bagi para pembaca dan semua pihak khususnya dalam bidang manajemen pemasaran.

Surabaya, Juli 2020

Penulis,

DAFTAR ISI

LEMBAR PENGESAHAN SKRIPSI ii
SURAT PERNYATAAN ANTI PLAGIAT iii
ABSTRAK iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR GAMBAR ix
DAFTAR TABEL x
BAB 1 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan masalah 4
1.4 Tujuan Penelitian 5
1.5 Manfaat 5
1.6 Sistematika penulisan 6
BAB II 7
TINJAUAN PUSTAKA 7
2.1 Penelitian Terdahulu 7
2.2 Landasan Teori 9
2.2.1 Jaringan Komputer 10
2.2.2 Snort 10
2.2.3 LAMP (Linux,Apache,MySQL,PHP) 12
2.2.4 Telegram Bot 12
2.2.5 Ubuntu 13
2.2.6 PHP 15
2.2.7 MySql 15
2.2.8 PhpMyAdmin 15
2.2.9 IDS*(Intrusion Detection System)* 16
2.2.10 BASE *(Basic Analysis and Security Engine)* 16
2.2.11 Port Scanning 17

BAB III 18
METODE PENELITIAN 18
3.1 Tahap Penelitian 18
3.2 Analisis Permasalahan 20
3.3 Rancangan Skenario 21
3.3.1. Skenario Pendeteksian Pola Serangan 22
3.4 SPESIFIKASI KEBUTUHAN SISTEM 23
3.5 PERANCANGAN SISTEM 25
3.5.1 Konfigurasi Sistem 26
3.5.2 Rancangan Simulasi Jaringan 27
3.6 Jadwal Kegiatan 28
BAB IV 30
HASIL DAN PEMBAHASAN 30
4.1 Pembangunan Arsitektur Jaringan 30
4.1.1 Setting IP Server 30
4.1.2 Setting IP Attacker 30
4.2 Implementasi Perangkat Lunak 30
4.2.1 Instalasi Aplikasi Pendukung 31
4.2.2 Instalasi dan Konfigurasi Snort 31
4.2.3 Instalasi dan Konfigurasi Barnyard2 33
4.2.4 Implementasi Database 34
4.2.5 Implementasi *Rule* Snort 35
4.2.6 Implementasi Telegram *Bot* 36
4.2.7 Implementasi *Trigger* 39
4.2.8 Hasil Pengujian Serangan 40
BAB V 42
KESIMPULAN DAN SARAN 42
5.1 Kesimpulan 42
5.2 Saran 42
DAFTAR PUSTAKA 44

DAFTAR GAMBAR

Gambar 3.1 Flowchart Alurt Penelitian 19

Gambar 3.2 Alur Serangan Uji Coba Sistem 22

Gambar 3.3 Skenario Pendeteksian Port Scanning 23

Gambar 3.4 Flowchart Alur Sistem Serangan Port Scanning 26

Gambar 3.5 Konfigurasi Sistem Port Scanning 28

Gambar 4.1 Pencarian Bot Father Telegram Bot 38

Gambar 4.2 Proses Pembuatan Newbot 38

Gambar 4.3 Proses Penentuan Nama User Telegram Bot 39

Gambar 4.4 Membuat ID Bot 39

Gambar 4.5 Mendapatkan ID Chat User dan Group 40

Gambar 4.6 Pengujian Port Scanning 42

Gambar 4.7 Notifikasi Port Scanning 42

DAFTAR TABEL

Tabel 3.1 Perangkat Keras dan Perangkat Lunak yang Digunakan 23

Tabel 3.2 Spesifikasi Perancangan Simulasi Jaringan 27

Tabel 4.1 IP Adress Attacker 30