

**ANALISIS LOG MIKROTIK UNTUK MENDETEKSI SERANGAN DAN
TRAFIK ANOMALI DI JARINGAN LABORATORIUM JARINGAN
PRODI TEKNOLOGI INFORMASI**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Informasi



Disusun oleh:

KHOERUL ANAM

202104015

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2024**

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS LOG MIKROTIK UNTUK MENDETEKSI SERANGAN DAN
TRAFIK ANOMALI DI JARINGAN LABORATORIUM JARINGAN
PRODI TEKNOLOGI INFORMASI

Diajukan oleh:

KHOERUL ANAM
202104015

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

Tanggal: 11 Juli 2024

Mengesahkan:

Pembimbing I



Arief Ikhwan Wicaksono, S.Kom., M.Cs.
NIDN: 0512128401

Pembimbing II



Chanief Budi Setiawan, S.T., M.Eng.
NIDN: 0514068101

Penguji I



Adkhan Sholeh, S.Si., M.Cs.
NIDN: 0510127501

Penguji II



Rama Sahtyawan, S.T., M.Cs.
NIDN: 0518058001

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta



Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.0150

PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Khoerul Anam
NPM : 202104015
Program Studi : S-I Teknologi Informasi
Judul Tugas Akhir : Analisis Log Mikrotik Untuk Mendeteksi Serangan Dan Trafik Anomali Di Jaringan Laboratorium Jaringan Prodi Teknologi Informasi

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 26 Juli 2024



Khoerul Anam

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmatNya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Analisis Log Mikrotik Untuk Mendeteksi Serangan Dan Trafik Anomali Di Jaringan Laboratorium Jaringan Prodi Teknologi Informasi”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi Teknologi Informasi (S-1) Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat terselesaikan berkat bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini, penulis dengan rendah hati mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Arief Ikhwan Wicaksono, S.Kom., M.Cs. selaku Dosen Pembimbing Tugas Akhir;
4. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Ketua Laboratorium jaringan Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta.
5. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;

6. Ayah, Ibu, Kaka dan Adik saya, yang telah memberikan dukungan semangat serta doa restu kepada saya, sehingga dapat menyelesaikan studi saya;
7. Diri saya, Khoerul Anam yang sudah mampu mau berjuang dan mampu bertanggung jawab untuk menyelesaikan dari apa yang sudah dimulai.
8. Rekan-rekan mahasiswa Teknologi Informasi (S-1) di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu, dengan segala kerendahan hati, penulis sangat menghargai kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktunya untuk membaca laporan tugas akhir ini.

Yogyakarta, 11 Juli 2024

Khoerul Anam

DAFTAR ISI

Halaman Judul	i
Halaman Pengesahan	ii
Pernyataan	iii
Kata Pengantar	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	x
Daftar Singkatan	xi
Intisari	xii
Abstrack	xiii
Bab 1 Pendahuluan.....	1
1.1 Latar Belakang	1
1.1.1 Perumusan Masalah.....	3
1.1.2 Manfaat Hasil Penelitian.....	3
1.1.3 Perrtanyaan Penelitian	3
1.2 Tujuan Penelitian.....	4
Bab 2 Tinjauan Pustaka dan Landasan Teori	5
2.1 Tinjauan Pustaka	5
2.2 Landasan Teori	7
2.2.1 Keamanan jaringan.....	7
2.2.2 Analisi log.....	8
2.2.3 Ancaman.....	9
2.3 Istilah-istilah dalam serangan jaringan	9
2.3.1 Anomali	9
2.3.2 Low Rate Ddos	9
2.3.3 Packet sniffer	10
2.3.4 Botnet	10

2.3.5 Flood Attack	11
2.4 Router Mikrotik.....	11
2.5 Splunk.....	12
Bab 3 Metode Penelitian	13
3.1 Alat Penelitian	14
3.1.1 Router Mikrotik.....	14
3.1.2 Splunk.....	15
3.1.3 Low Orbit Ion Cannon (LOIC).....	16
3.1.4 Hping3	16
3.2 Jalan Penelitian	16
Bab 4 Hasil Penelitian	20
4.1 Ringkasan Hasil Penelitian.....	20
4.2 Implementasi dan Konfigurasi firewall	20
4.2.1 Konfigurasi Firewall.....	20
4.3 Analisis Aturan Firewall.....	24
4.3.1 Identifikasi Serangan	24
4.3.2 Mitigasi Serangan	27
4.4 Implementasi Splunk.....	27
4.4.1 Instal Splunk.....	27
4.4.2 Input Data	28
4.4.3 Visualisasi Hasil	29
Bab 5 Kesimpulan dan Saran.....	33
5.1 Kesimpulan.....	33
5.2 Saran.....	33
Daftar Pustaka	34
Lampiran.....	36

DAFTAR TABEL

Tabel 3.1 Kebutuhan Sistem Splunk	18
---	----

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR GAMBAR

Gambar 3.1 Proses <i>Port Mirroring</i>	13
Gambar 3.2 Proses Jalanya Penelitian	16
Gambar 4.1 Pengaturan <i>Firewall Filter Rules</i>	21
Gambar 4.2 Pengaturan <i>Firewall Raw</i>	23
Gambar 4.3 Penerapan Filter <i>Firewall</i>	24
Gambar 4.4 Log Mikrotik (1)	25
Gambar 4.5 Log Mikrotik (2)	26
Gambar 4.6 Sumber Alamat IP.....	27
Gambar 4.7 Install Splunk	28
Gambar 4.8 Data Log Pada Splunk.....	28
Gambar 4.9 Data Log Pada Splunk.....	29
Gambar 4.10 Aturan Jumlah <i>Event</i> Per Detik.....	29
Gambar 4.11 Hasil Pengelompokan Berdasarkan Grafik	30
Gambar 4.12 Hasil Pengelompokan Berdasarkan Data Tabel.....	30
Gambar 4.13 Hasil Jumlah <i>Event</i> Berdasarkan Menit.....	31

DAFTAR LAMPIRAN

Lampiran 1 Surat Peminjaman Alat	36
Lampiran 2 Kartu Bimbingan TA.....	37
Lampiran 3 Jadwal Penelitian.....	38
Lampiran 4 Cek Plagiarisme	39

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

IP	<i>Internet Protocol</i>
HTML	<i>Hypertext Markup Language</i>
FTTI	Fakultas Teknik & Teknolongi Informasi
UNJAYA	Universitas Jenderal Achmad Yani Yogyakarta
VPN	<i>Virtual Private Network</i>
IDS	<i>Intrusion Detection System</i>
IPS	<i>Intrusion Prevention System</i>
WIFI	<i>Wireless Fidelity</i>
DDOS	<i>Distributed Denial Of Service</i>
SIEM	<i>Security Information Event and Management</i>
IRC	<i>Internet Relay Chat</i>
C&C	<i>Comand and Control</i>
PC	<i>Personal Computer</i>