

**IMPLEMENTASI PI-HOLE
UNTUK MEMBANGUN SISTEM PERTAHANAN JARINGAN
DARI SERANGAN MALVERTISING**

TUGAS AKHIR

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



Disusun oleh:

NINDYA DWI ANGGANA

182104009

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2021**

HALAMAN PENGESAHAN

TUGAS AKHIR

**IMPLEMENTASI PI-HOLE
UNTUK MEMBANGUN SISTEM PERTAHANAN JARINGAN
DARI SERANGAN MALVERTISING**

Diajukan oleh:

NINDYA DWI ANGGANA

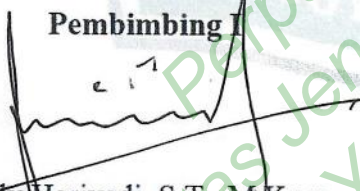
182102009

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: 29 Agustus 2022

Mengesahkan:

Pembimbing I


Dedy Hariyadi, S.T., M.Kom.
NIDN: 0518108001

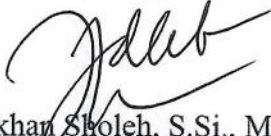
Pembimbing II


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

Penguji I


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

Penguji II


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

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



Chanief Budi Setiawan, S.T., M.Eng.
NPP: 2008.13.0021

PERNYATAAN

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

Nama : Nindya Dwi Anggana
NPM : 182104009
Program Studi : Teknologi Informasi (S-1)
Judul Tugas Akhir : Implementasi Pi-Hole untuk Membangun Sistem Pertahanan Jaringan dari Serangan *Malvertising*

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 penelitian 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, 24 Agustus 2022



Nindya Dwi Anggana

KATA PENGANTAR

Puji syukur kehadirat Allah SWT sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul “Implementasi Pi-Hole untuk Membangun Sistem Pertahanan Jaringan dari Serangan *Malvertising*”. Penulisan laporan ini merupakan salah satu syarat untuk menyelesaikan studi pada program studi Teknologi Informasi (S-1) di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat terwujud atas bimbingan dan dukungan dari berbagai pihak yang bersangkutan. Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Ketua Program Studi Teknologi Informasi (S-1) Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Dedy Hariyadi, S.T., M.Kom. dan Bapak Rama Sahtyawan, S.T., M.Cs. selaku Dosen Pembimbing Tugas Akhir;
4. 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;
5. Ibu, ayah, dan kakak penulis yang telah memberikan dukungan semangat serta doa restu, sehingga penulis dapat menyelesaikan studi;
6. Snowy, kucing kesayangan penulis, telah menjadi penyemangat hidup penulis dan berpengaruh besar dalam peningkatan *mood* penulis selama pengerjaan tugas akhir;
7. Sahabat terbaik penulis, Reta dan Alula, yang sudah menjadi *support system* saat penulis ada di titik terendah dan selalu menjadi teman yang paling peduli dengan apapun yang terjadi kepada penulis;
8. Seluruh rekan di Widya Security, atas segala dukungan dan bimbingannya kepada penulis selama mengerjakan tugas akhir ini, menjadi keluarga kedua

penulis, dan menjadi tempat penulis berkembang dan mempelajari banyak hal baru;

9. Seluruh sahabat penulis dalam sebuah *group chat* PS²K yang saling memberikan dukungan selama penulisan tugas akhir ini;
10. Teman-teman mahasiswa Teknologi Informasi (S-1) di Universitas Jenderal Achmad Yani Yogyakarta, terlebih kepada teman-teman seperjuangan penulis 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 adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 24 Agustus 2022

Nindya Dwi Anggana

DAFTAR ISI

Halaman Judul	i
Halaman Pengesahan	ii
Halaman Pernyataan	iii
Kata Pengantar.....	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	xi
Daftar Singkatan	xii
Intisari	xiii
<i>Abstract</i>	xiv
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah.....	3
1.3 Pertanyaan Penelitian	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Hasil Penelitian	4
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	5
2.1 Tinjauan Pustaka	5
2.2 Landasan Teori	8
2.2.1 Sistem Jaringan Komputer	8
2.2.2 WWW (<i>World Wide Web</i>).....	9
2.2.3 <i>Malvertising</i>	9
2.2.4 DNS <i>Query</i>	10
2.2.5 <i>OSI Layer</i>	11
2.2.6 <i>Single-Board Computer</i>	13
Bab 3 Metode Penelitian	14
3.1 Bahan Penelitian.....	14
3.2 Alat Penelitian	14

3.2.1	Raspberry Pi	14
3.2.2	Pi-Hole.....	16
3.3	Jalan Penelitian.....	18
Bab 4	Hasil Penelitian	24
4.1	Hasil Penelitian	24
4.1.1	Instalasi Sistem Operasi Raspberry Pi OS.....	24
4.1.2	Konfigurasi Pi-Hole pada Raspberry Pi 3 model B+	26
4.1.3	Konfigurasi Jaringan Pada Raspberry Pi 3 Model B+.....	34
4.1.4	Pengujian Sistem	34
4.1.5	<i>Update Blocklist</i>	38
4.2	Pembahasan	41
Bab 5	Kesimpulan dan Saran.....	55
5.1	Kesimpulan.....	55
5.2	Saran.....	55
Daftar Pustaka.....		57
Lampiran.....		60

DAFTAR TABEL

Tabel 4.1 Hasil Pengujian <i>Client</i> pada PC.....	52
Tabel 4.2 Hasil Pengujian <i>Client</i> pada Perangkat <i>Smartphone</i>	53
Tabel 4.3 Pengujian <i>Client</i> pada Aplikasi <i>Mobile</i>	54

Perpustakaan
Universitas Jenderal Achmad Yani
Yogyakarta

DAFTAR GAMBAR

Gambar 2.1 <i>Domain Name System (DNS) Server</i>	10
Gambar 2.2 <i>OSI Layer</i>	11
Gambar 3.1 Raspberry Pi 3 Model B+	15
Gambar 3.2 <i>Arsitektur Pi-Hole</i>	17
Gambar 3.3 <i>Topologi Jaringan Sebelum Implementasi Sistem Pertahanan Menggunakan Pi-Hole</i>	18
Gambar 3.4 <i>Topologi Jaringan dengan Implementasi Sistem Menggunakan Pi-Hole</i>	19
Gambar 3.5 <i>Alur Penelitian</i>	20
Gambar 4.1 <i>Raspberry Pi Imager</i>	25
Gambar 4.2 <i>Aktivasi SSH pada Raspberry Pi 3 model B+</i>	27
Gambar 4.3 <i>PuTTY</i>	28
Gambar 4.4 <i>Terminal Raspberry Pi 3 model B+ pada PuTTY</i>	29
Gambar 4.5 <i>Pengaturan Upstream DNS Provider</i>	30
Gambar 4.6 <i>Pengaturan Internet Protocol</i>	30
Gambar 4.7 <i>Pengaturan Instalasi Web Admin Interface</i>	31
Gambar 4.8 <i>Pengaturan Log Query</i>	31
Gambar 4.9 <i>Pengaturan Privasi FTL Pi-Hole</i>	32
Gambar 4.10 <i>Informasi Akhir pada Konfigurasi Pi-Hole</i>	33
Gambar 4.11 <i>Dashboard Web Admin Pi-Hole</i>	35
Gambar 4.12 <i>Pengujian DNSLeakTest Sebelum Terhubung ke Jaringan FTTH Universitas Jenderal Achmad Yani Yogyakarta</i>	36
Gambar 4.13 <i>Pengujian DNSLeakTest Setelah Terhubung ke Jaringan FTTH Universitas Jenderal Achmad Yani Yogyakarta</i>	37
Gambar 4.14 <i>Adlist Pi-Hole</i>	38
Gambar 4.15 <i>Blacklist Pi-Hole</i>	39
Gambar 4.16 <i>Update Gravity</i>	40
Gambar 4.17 <i>Informasi Log Query Pi-Hole</i>	42
Gambar 4.18 <i>Grafik Query Log Pi-Hole</i>	43

Gambar 4.19 <i>Domain</i> yang Paling Sering Diblokir Pi-Hole.....	44
Gambar 4.20 <i>Domain</i> yang Paling Sering Diakses <i>Client</i>	45
Gambar 4.21 <i>Client</i> yang Paling Banyak Melakukan Akses <i>Internet</i>	46
Gambar 4.22 Situs inet.detik.com yang Mengandung <i>Malvertising</i>	47
Gambar 4.23 Situs inet.detik.com Terbebas dari <i>Malvertising</i>	47
Gambar 4.24 Situs parapuan.co yang Mengandung <i>Malvertising</i>	48
Gambar 4.25 Situs parapuan.co Terbebas dari <i>Malvertising</i>	49
Gambar 4.26 Aplikasi HitungKalori yang Mengandung <i>Malvertising</i>	50
Gambar 4.27 Aplikasi HitungKalori Terbebas dari <i>Malvertising</i>	51

Perpustakaan
Universitas Jenderal Achmad Yani
Yogyakarta

DAFTAR LAMPIRAN

Lampiran 1 Surat Ijin Penelitian.....	60
Lampiran 2 Jadwal Penelitian	61
Lampiran 3 Lembar Bimbingan Dosen	62
Lampiran 4 Hasil Cek Plagiarisme.....	63

Perpustakaan
Universitas Jenderal Achmad Yani
Yogyakarta

DAFTAR SINGKATAN

API	<i>Application Programming Interface</i>
APJII	<i>Asosiasi Penyelenggara Jasa Internet Indonesia</i>
CLI	<i>Command Line Interface</i>
DHCP	<i>Dynamic Host Configuration Tool</i>
DMZ	<i>Demilitarized Zone</i>
DNS	<i>Domain Name System</i>
DoH	<i>DNS-over-HTTPS</i>
FTL	<i>Faster Than Light</i>
GUI	<i>Graphical User Interface</i>
I/O	<i>Input/Output</i>
IP	<i>Internet Protocol</i>
ISP	<i>Internet Service Provider</i>
NAT	<i>Network Address Translator</i>
PC	<i>Personal Computer</i>
QoS	<i>Quality of Service</i>
SBC	<i>Single-Board Computer</i>
SoC	<i>System-on-a-Chip</i>
TCP/IP	<i>Transmission Control Protocol/Internet Protocol</i>
URL	<i>Uniform Resource Locators</i>
WWW	<i>World Wide Web</i>