

**RANCANG BANGUN *REMOTE-EVIL-TWIN-ATTACK* BERBASIS
OPENWRT DAN TAILSCALE UNTUK ANALISIS PAKET DATA
JARINGAN WI-FI MENGGUNAKAN ARKIME**

Tugas Akhir

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



Disusun oleh:

Yuha Nazhif Zuhair

212104014

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK DAN TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA
2025**

HALAMAN PENGESAHAN

Tugas Akhir

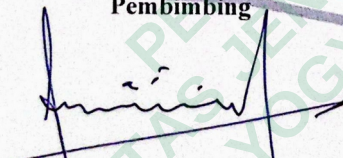
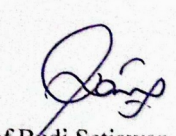
**RANCANG BANGUN *REMOTE-EVIL-TWIN-ATTACK* BERBASIS
OPENWRT DAN TAILSCALE UNTUK ANALISIS PAKET DATA
JARINGAN WI-FI MENGGUNAKAN ARKIME**

Diajukan oleh:

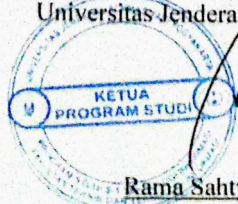
Yuha Nazhif Zuhair
212104014

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik dan Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta
Tanggal: 14 Juli 2025

Mengesahkan:

Pembimbing	Penguji
 <u>Ir. Dedy Hariyadi, S.T., M.Kom.</u> NIDN: 0518108001	 <u>Chanief Budi Setiawan, S.T., M.Eng.</u> NIDN: 0514068101

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



Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.00150

PERNYATAAN

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

Nama : Yuha Nazhif Zuhair
NPM : 212104014
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Rancang Bangun *Remote-Evil-Twin-Attack* Berbasis OpenWRT dan Tailscale untuk Analisis Paket Data Jaringan Wi-Fi Menggunakan Arkime

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, 14 Juli 2025



Yuha Nazhif Zuhair

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Rancang Bangun *Remote-Evil-Twin-Attack* Berbasis OpenWRT dan Tailscale untuk Analisis Paket Data Jaringan Wi-Fi Menggunakan Arkime”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Ibu Nurlaely, selaku ibu dari penulis yang telah memberikan doa restu, dukungan, semangat, motivasi, dan segalanya yang diberikan dengan tiada henti, sehingga penulis dapat menyelesaikan studi dengan tepat waktu;
2. Adzkia Jasmine Ramadhania, selaku adik penulis yang telah memberikan doa, dukungan dan semangat kepada penulis, sehingga penulis dapat menyelesaikan studi dengan tepat waktu;
3. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs., selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
4. Bapak Rama Sahtyawan, S.T., M.Cs., selaku Ketua Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Bapak Ir. Dedy Hariyadi, S.T., M.Kom., selaku Dosen Pembimbing Akademik dan Dosen Pembimbing Tugas Akhir yang telah memberikan dukungan semangat, ilmu pengetahuan, bimbingan, motivasi, teman diskusi, teman cerita, dan teman ngopi selama penulis menjadi mahasiswa

di Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;

6. Para Bapak/Ibu Dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
7. Para Saudara/Saudari yang telah memberikan semangat dan doa kepada penulis;
8. Para penghuni Kontrakan Tekno 21 yang telah memberikan semangat, tempat berkumpul dan bercerita serta saksi dalam perjuangan penulis selama menyelesaikan studi;
9. Rekan-rekan Mahasiswa/Mahasiswi Program Studi S-1 Teknologi Informasi angkatan 2021 di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan, semangat, tempat mengukir cerita dan berbagi pengalaman selama penulis menyelesaikan studi.

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, 14 Juli 2025

Yuha Nazhif Zuhair

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
DAFTAR ISI.....	vi
DAFTAR TABEL.....	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN.....	xi
DAFTAR SINGKATAN.....	xii
INTISARI.....	xiv
ABSTRACT.....	xv
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	3
1.3 Batasan Penelitian.....	4
1.4 Pertanyaan Penelitian.....	4
1.5 Tujuan Penelitian.....	5
1.6 Manfaat Hasil Penelitian.....	5
BAB 2 TINJAUAN PUSTAKA DAN LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Landasan Teori.....	13
2.2.1 Jaringan Nirkabel.....	13
2.2.2 Kerentanan Keamanan Jaringan.....	14
2.2.3 <i>Network Penetration Testing</i>	15
2.2.4 Serangan <i>Man in the Middle</i> (MitM).....	16
2.2.5 <i>Evil Twin Attack</i>	18

2.2.6 OpenWRT.....	19
2.2.7 Arkime.....	20
2.2.8 <i>Cyber Kill Chain</i>	21
BAB 3 METODE PENELITIAN.....	23
3.1 Bahan dan Alat Penelitian.....	24
3.1.1 Bahan Penelitian.....	24
3.1.2 Alat Penelitian.....	24
3.2 Jalan Penelitian.....	27
3.3 Rancangan Sistem.....	30
3.3.1 Diagram Blok Pengembangan Alat.....	30
3.3.2 Topologi Sistem Pengujian.....	31
BAB 4 HASIL PENELITIAN.....	34
4.1 Ringkasan Hasil Penelitian.....	34
4.2 Identifikasi dan Penentuan Jaringan Wi-Fi.....	36
4.3 Perancangan dan Integrasi Sistem Pengujian.....	42
4.3.1 Perancangan Sumber Daya.....	42
4.3.2 Konfigurasi OpenWRT.....	43
4.3.3 Integrasi Tailscale.....	48
4.3.4 Konfigurasi Arkime.....	55
4.3.5 <i>Mounting Secure Shell File System (SSHFS)</i>	59
4.4 Pengujian <i>Evil Twin Attack</i>	62
4.5 Analisis Paket Data Hasil Pengujian.....	72
BAB 5 KESIMPULAN DAN SARAN.....	103
5.1 Kesimpulan.....	103
5.2 Saran.....	104
DAFTAR PUSTAKA.....	105
LAMPIRAN.....	109

DAFTAR TABEL

Tabel 2.1 Perbandingan Penelitian.....	9
Tabel 2.2 Spesifikasi Jaringan Wi-Fi.....	14
Tabel 4.1 Hasil Identifikasi Jumlah Korban.....	74
Tabel 4.2 Hasil Identifikasi Akses <i>Port</i> Pada Alamat IP Korban.....	80
Tabel 4.3 Hasil Identifikasi Sesi <i>Port</i> 80 Pada Alamat IP Korban.....	92
Tabel 4.4 Hasil Identifikasi Pencarian Data Sensitif Korban.....	98

DAFTAR GAMBAR

Gambar 2.1 Proses <i>Evil Twin Attack</i>	19
Gambar 2.2 Tahapan <i>Cyber Kill Chain</i>	22
Gambar 3.1 Tahapan Penelitian.....	23
Gambar 3.2 Diagram Blok Pengembangan Alat.....	30
Gambar 3.3 Topologi Sistem Pengujian.....	32
Gambar 4.1 Hasil Tangkapan Jaringan Wi-Fi Menggunakan WiGLE Wi-Fi.....	38
Gambar 4.2 Akses Internet Jaringan Wi-Fi Terbuka.....	39
Gambar 4.3 Data Frekuensi 2,4 GHz.....	40
Gambar 4.4 Data Frekuensi 5 GHz.....	41
Gambar 4.5 Hasil Perancangan Sumber Daya.....	43
Gambar 4.6 Pembuatan Antarmuka Baru Untuk Modem GSM.....	47
Gambar 4.7 Pengaturan <i>Firewall Settings</i>	47
Gambar 4.8 Daftar Perangkat Pada Akun Tailscale.....	50
Gambar 4.9 Konfigurasi <i>Firewall</i> Untuk Tailscale.....	52
Gambar 4.10 Hasil <i>Remote</i> OpenWRT Menggunakan Nama <i>Host</i> Tailscale.....	53
Gambar 4.11 Hasil <i>Remote</i> LuCI OpenWRT Menggunakan IP Tailscale.....	54
Gambar 4.12 Verifikasi Arkime <i>Viewer</i>	57
Gambar 4.13 Tampilan Antarmuka <i>Website</i> Arkime <i>Viewer</i>	58
Gambar 4.14 Hasil <i>Mounting</i> SSHFS.....	61
Gambar 4.15 Proses Pengujian Lantai 1.....	63
Gambar 4.16 Hasil Arkime <i>Viewer</i> Lantai 1.....	66
Gambar 4.17 Proses Pengujian di Lantai 2.....	67
Gambar 4.18 Proses Pengujian di Lantai 3.....	68
Gambar 4.19 Proses Pengujian di Lantai 4.....	69
Gambar 4.20 Proses Pengujian di Gazebo.....	71
Gambar 4.21 Identifikasi Jumlah Korban Pada Fitur <i>Sessions</i>	73

Gambar 4.22 Identifikasi Akses <i>Port</i> Pada Alamat IP Korban.....	79
Gambar 4.23 Identifikasi Sesi Komunikasi <i>Port</i> 80 Pada Alamat IP Korban.....	91
Gambar 4.24 Identifikasi Data Sensitif Korban Pada Fitur <i>Hunt</i>	97

PERPUSTAKAAN
UNIVERSITAS JENDRAL ACHMAD YANI
YOGYAKARTA

DAFTAR LAMPIRAN

Lampiran 1 Jadwal Penelitian.....	109
Lampiran 2 Surat Izin Penelitian.....	112
Lampiran 3 Kartu Bimbingan Tugas Akhir.....	113
Lampiran 4 Hasil Cek Plagiarisme.....	114

PERPUSTAKAAN
UNIVERSITAS JENDRAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

Wi-Fi	<i>Wireless Fidelity</i>
AP	<i>Access Point</i>
IEEE	<i>Institute of Electrical and Electronics</i>
MitM	<i>Man in the Middle</i>
SCADA	<i>Supervisory Control and Data</i>
SSID	<i>Service Set Identifier</i>
NTA	<i>Network Traffic Analysis</i>
DSR	<i>Design Science Research</i>
WIDS	<i>Wireless Intrusion Detection System</i>
PTES	<i>Penetration Testing Execution Standard</i>
DoS	<i>Denial of Service</i>
OWASP	<i>Open Web Application Security Project</i>
OSTMM	<i>Open Source Security Testing Methodology Manual</i>
NIST	<i>National Institute Standards and Technology</i>
CKC	<i>Cyber Kill Chain</i>
ARP	<i>Address Resolution Protocol</i>
DNS	<i>Domain Name System</i>
SSL	<i>Secure Sockets Layer</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
HTTP	<i>Hypertext Transfer Protocol</i>
LuCI	<i>Lua Configuration Interface</i>
CLI	<i>Command Line Interface</i>
C2	<i>Command & Control</i>
IoT	<i>Internet of Things</i>
GSM	<i>Global System for Mobile Communication</i>
SIM	<i>Subscriber Identity Module</i>

SSHFS	<i>Secure Shell File System</i>
SSH	<i>Secure Shell</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
USB	<i>Universal Serial Bus</i>
VPN	<i>Virtual Private Network</i>
IP	<i>Internet Protocol</i>
GPG	<i>GNU Privacy Guard</i>
MAC	<i>Media Access Control</i>

PERPUSTAKAAN
UNIVERSITAS JENDRAL ACHMAD YANI
YOGYAKARTA