

**MEMBANGUN MODEL *HUMAN FIREWALL*
MENGUNAKAN METODE POHON KEPUTUSAN**

SKRIPSI



Disusun oleh:

Muhammad Zulfahmi Huwaidi

17.83.0123

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

**MEMBANGUN MODEL *HUMAN FIREWALL*
MENGUNAKAN METODE POHON KEPUTUSAN**

SKRIPSI

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Sarjana Komputer
Pada Jenjang Program Sarjana – Program Studi Teknik Komputer



Disusun oleh:

Muhammad Zulfahmi Huwaidi
17.83.0123

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

HALAMAN PERSETUJUAN
SKRIPSI
MEMBANGUN MODEL *HUMAN FIREWALL* MENGGUNAKAN METODE
POHON KEPUTUSAN

yang dipersiapkan dan disusun oleh

Muhammad Zulfahmi Huwaidi

17.83.0123

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 27 Agustus 2021

Dosen Pembimbing,

Sumarni Adi, S.Kom, M.Cs
NIK. 190302038

HALAMAN PENGESAHAN SKRIPSI

MEMBANGUN MODEL *HUMAN FIREWALL* MENGGUNAKAN METODE POHON KEPUTUSAN

yang dipersiapkan dan disusun oleh

Muhammad Zulfahmi Huwaidi

17.83.0123

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 September 2021

Nama Penguji

Susunan Dewan Penguji

Tanda Tangan

Eli Pujastuti, M.Kom
NIK. 190302227

Arifiyanto Hadinegoro, S.Kom, MT
NIK. 190302289

Sumarni Adi, S.Kom, M.Cs
NIK. 190302256

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 September 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Zulfahmi Huwaidi
NIM : 17.83.0123

Menyatakan bahwa Skripsi dengan judul berikut:

MEMBANGUN MODEL HUMAN FIREWALL MENGGUNAKAN METODE POHON KEPUTUSAN

Dosen Pembimbing : Sumarni Adi, S.Kom, M.Cs

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 21 September 2021

Yang Menyatakan,



Muhammad Zulfahmi Huwaidi

KATA PENGANTAR

Dengan mengucapkan Alhamdulillah segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT, karena berkat rahmat dan hidayah-Nya penyusunan skripsi yang berjudul “Analisis dan Penanganan Serangan *Social Engineering* dengan *Firewall*” ini dapat diselesaikan guna memenuhi salah satu persyaratan dalam menyelesaikan pendidikan pada Jurusan Teknik Komputer Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.

Perjalanan panjang telah penulis lalui dalam rangka menyelesaikan penulisan skripsi ini. Banyak hambatan yang dihadapi dalam penyusunannya, namun berkat kehendak-Nyalah sehingga penulis berhasil menyelesaikan penulisan skripsi ini. Oleh karena itu, dengan penuh kerendahan hati, pada kesempatan ini patutlah kiranya penulis mengucapkan terima kasih kepada :

1. Kedua Orang Tua.
2. Sumarni Adi, S.Kom, M.Cs selaku Dosen Pembimbing.
3. Dosen Penguji.

Semua pihak yang telah banyak membantu dalam penyusunan skripsi ini yang tidak bisa penulis sebutkan semuanya.

Akhir kata, penulis mengharapakan skripsi ini dapat memberikan manfaat bagi penulis khususnya dan bagi pembaca pada umumnya.

Yogyakarta, 9 Desember 2021

Muhammad Zulfahmi Huwaidi

DAFTAR ISI

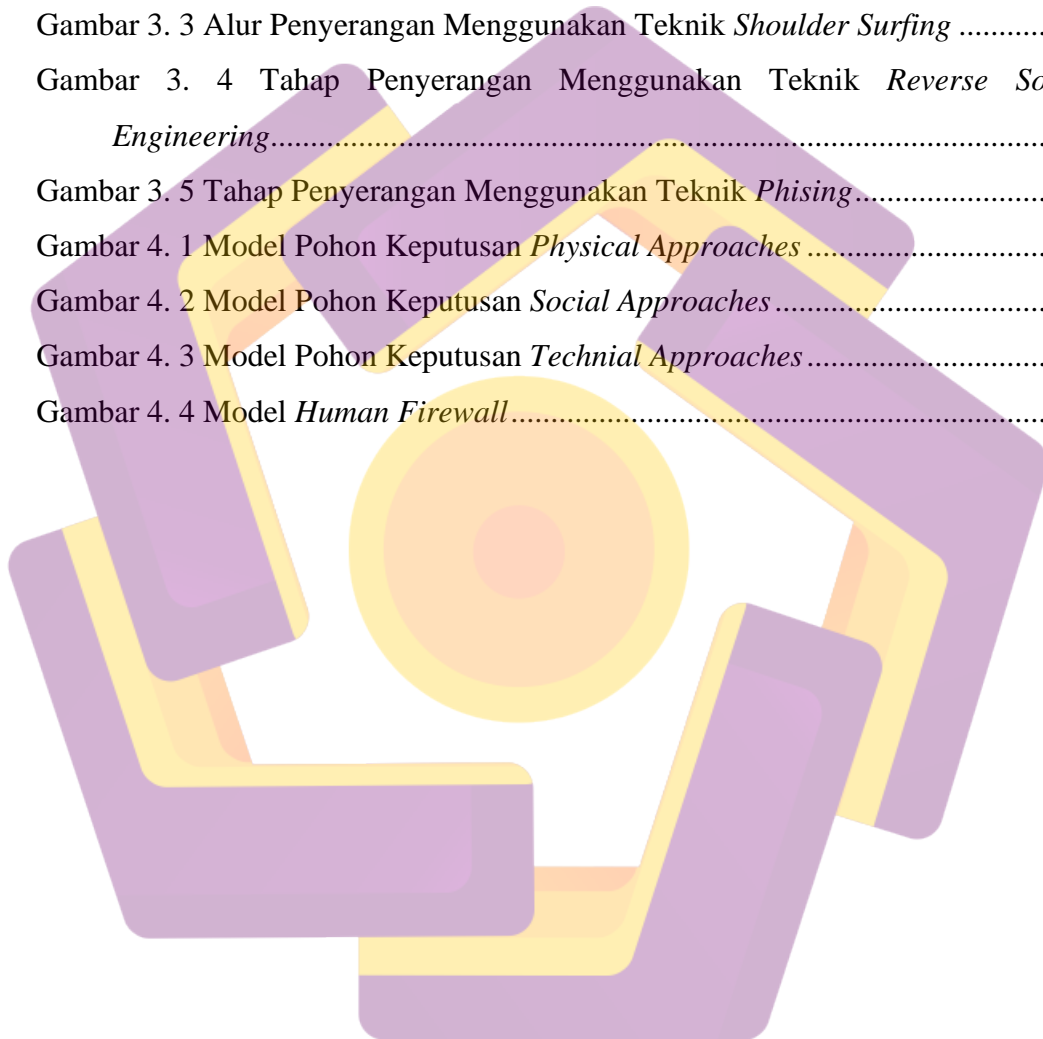
HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	i
HALAMAN PENGESAHAN.....	ii
SKRIPSI.....	ii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iii
KATA PENGANTAR	iv
DAFTAR ISI.....	v
DAFTAR GAMBAR	vii
INTISARI.....	viii
ABSTRACT.....	ix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	4
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan Pustaka.....	7
2.2 Dasar Teori.....	9
BAB III METODOLOGI PENELITIAN.....	21
3.1 Tinjauan Umum	21
3.2 Alat dan Bahan Penelitian.....	21
3.5 Metode Penelitian	22
BAB IV PEMBAHASAN.....	35
4.1 Pohon Keputusan	35
4.2 Hasil Implementasi dan Pengujian Model	40
4.3 Pembentukan <i>Human Firewall</i>	48
BAB V PENUTUP.....	51
5.1 Kesimpulan	51
5.2 Saran	51

DAFTAR TABEL

Tabel 2.1 Perbandingan penelitian.....	8
Tabel 3. 1 Spesifikasi Perangkat Keras dan Perangkat Lunak.....	21
Tabel 3. 2 Pengelompokan Serangan Rekayasa Sosial.....	24
Tabel 3. 3 Pertanyaan Emosi Individu.....	29
Tabel 3. 4 Pertanyaan dan Pilihan Keputusan Serangan Rekayasa Sosial (<i>Physical Approaches</i>).....	30
Tabel 3. 5 Pertanyaan dan Pilihan Keputusan Serangan Rekayasa Sosial (<i>Social Approaches</i>).....	31
Tabel 3. 6 Pertanyaan dan Pilihan Keputusan Serangan Rekayasa Sosial (<i>Technical Approaches</i>).....	33
Tabel 4. 1 Ke-stabilan Emosi Responden.....	40
Tabel 4. 2 Hasil Keputusan Responden untuk <i>Human Firewall</i> (Pendekatan Fisik).....	42
Tabel 4. 3 Hasil Keputusan Responden untuk <i>Human Firewall</i> (Pendekatan Sosial).....	43
Tabel 4. 4 Hasil Keputusan Responden untuk <i>Human Firewall</i> (Pendekatan Teknik).....	46
Tabel 4. 5 Data Responden (Keputusan Kurang Tepat).....	47
Tabel 4. 6 Hasil Pembentukan <i>Human Firewall</i>	49

DAFTAR GAMBAR

Gambar 3. 1 Alur Penelitian.....	22
Gambar 3. 2 Alur Penyerangan Menggunakan Teknik <i>Shoulder Surfing</i>	25
Gambar 3. 3 Alur Penyerangan Menggunakan Teknik <i>Shoulder Surfing</i>	26
Gambar 3. 4 Tahap Penyerangan Menggunakan Teknik <i>Reverse Social Engineering</i>	27
Gambar 3. 5 Tahap Penyerangan Menggunakan Teknik <i>Phising</i>	28
Gambar 4. 1 Model Pohon Keputusan <i>Physical Approaches</i>	35
Gambar 4. 2 Model Pohon Keputusan <i>Social Approaches</i>	36
Gambar 4. 3 Model Pohon Keputusan <i>Technial Approaches</i>	37
Gambar 4. 4 Model <i>Human Firewall</i>	39



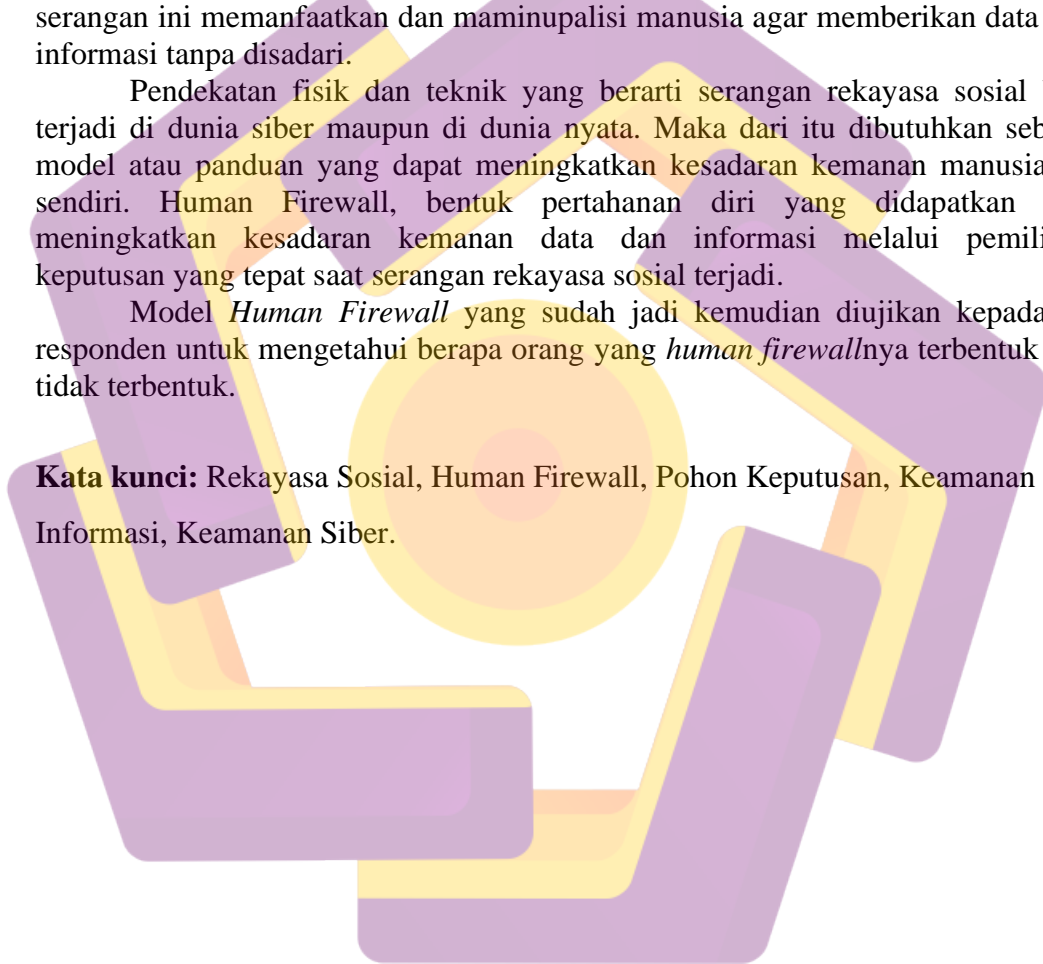
INTISARI

Manusia adalah elemen paling rentan yang ada pada sistem keamanan informasi. Seringkali orang menganggap bahwa apa yang dibagikan di dunia maya atau dunia siber adalah hal yang tidak penting, tetapi bagi sebagian orang, data dan informasi yang sangat banyak di internet bisa digunakan untuk tindak kejahatan yang membuat kerugian yang besar. Salah satu teknik yang digunakan pelaku tindak kejahatan dunia siber disebut dengan teknik rekayasa sosial. Hal ini menuntut orang-orang agar selalu waspada dan berhati-hati karena pada dasarnya serangan ini memanfaatkan dan manipulasi manusia agar memberikan data dan informasi tanpa disadari.

Pendekatan fisik dan teknik yang berarti serangan rekayasa sosial bisa terjadi di dunia siber maupun di dunia nyata. Maka dari itu dibutuhkan sebuah model atau panduan yang dapat meningkatkan kesadaran keamanan manusia itu sendiri. Human Firewall, bentuk pertahanan diri yang didapatkan dari meningkatkan kesadaran keamanan data dan informasi melalui pemilihan keputusan yang tepat saat serangan rekayasa sosial terjadi.

Model *Human Firewall* yang sudah jadi kemudian diujikan kepada 48 responden untuk mengetahui berapa orang yang *human firewall*nya terbentuk dan tidak terbentuk.

Kata kunci: Rekayasa Sosial, Human Firewall, Pohon Keputusan, Keamanan Informasi, Keamanan Siber.



ABSTRACT

Humans are the most vulnerable element in the information security system. Often people think that what is shared in cyberspace or cyberspace is unimportant, but for some people, the vast amount of data and information on the internet can be used for crimes that cause huge losses. One of the techniques used by cybercriminals is called social engineering. This requires people to always be vigilant and careful because basically this attack utilizes and manipulates humans to provide data and information without realizing it.

Physical and technical approaches that mean social engineering attacks can occur in the cyber world as well as in the real world. Therefore we need a model or guide that can increase awareness of human security itself. Human Firewall, a form of self-defense obtained from increasing awareness of data and information security through making the right decisions when social engineering attacks occur.

The finished Human Firewall model was then tested on 48 respondents to find out how many people the human firewall had and did not form.

Keyword: *Social Engineering, Human Firewall, Decision Tree, Information Security, Cyber Security.*

