ANALISIS ANCAMAN SERANGAN PHISHING VIA ZOOM MENGGUNAKAN METODE REPLIKASI WEBSITE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

diajukan oleh

Fadhil Bima Pradipa

18.83.0192

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

ANALISIS ANCAMAN SERANGAN PHISHING VIA ZOOM MENGGUNAKAN METODE REPLIKASI WEBSITE

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

diajukan oleh

Fadhil Bima Pradipa

18.83.0192

Kepada

PROGRAM SARJANA

PROGRAM STUDI TEKNIK KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PERSETUJUAN
SKRIPSI

PENCEGAHAN SERANGAN PHISHING VIA ZOOM MENGGUNAKAN METODE REPLIKASI WEBSITE

yang disusun dan diajukan oleh

Fadhil Bima Pradipa

18.83.0192

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 6 Juli 2022

Dosen Pembimbing,

Senie Destya, ST., M.Kom
NIK. 190302312

HALAMAN PENGESAHAN
SKRIPSI

PENCEGAHAN SERANGAN PHISHING VIA ZOOM MENGGUNAKAN METODE REPLIKASI WEBSITE

yang disusun dan diajukan oleh

Fadhil Bima Pradipa

18.83.0192

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Juli 2022

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	
Senie Destya, ST.,M.Kom **NIK. 190302312**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 21 Juli 2022

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Fadhil Bima Pradipa
NIM : 18.83.0192

Menyatakan bahwa Skripsi dengan judul berikut:

PENCEGAHAN SERANGAN PHISHING VIA ZOOM MENGGUNAKAN METODE REPLIKASI WEBSITE

Dosen Pembimbing : Senie Destya, ST., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH dinjukan 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 Juli 2022>

Yang Menyatakan,

Fadhil Bima Pradipa

HALAMAN PERSEMBAHAN

Dengan mengucap Alhamdullilah Skripsi ini penulis Persembahkan kepada yang pertama orang tua, lalu kepada dosen pembimbing, dan Teman-teman yang telah membantu dan memberikan dukungan semangat, demi kesuksesan penulis.

Teman-Teman Teknik Komputer 2018.

Almamater Program studi Teknik Komputer.

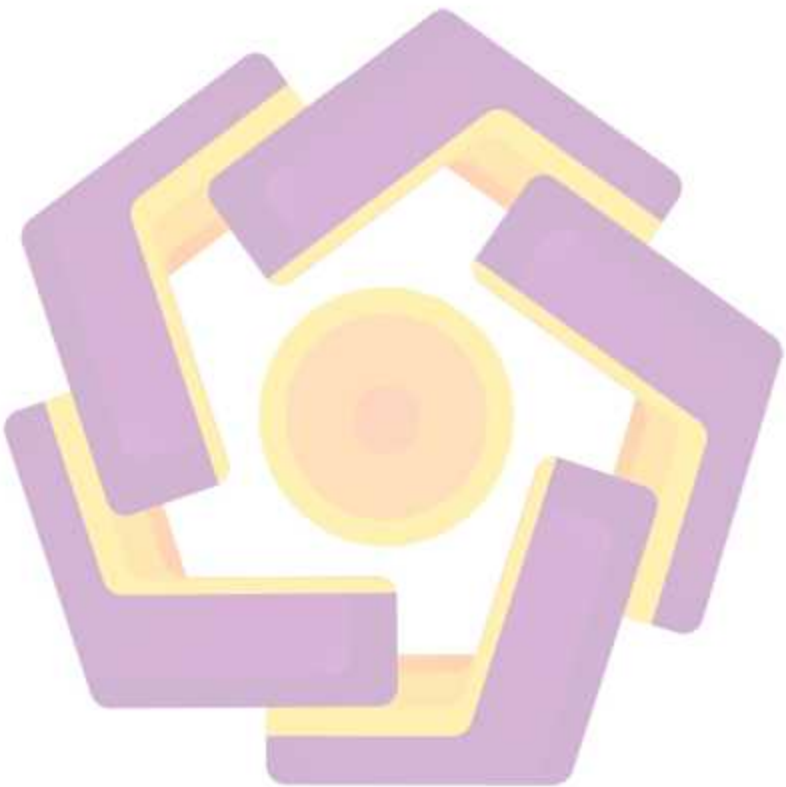
Fakultas Ilmu Komputer.

Universitas Amikom Yogyakarta

Yogyakarta

MOTTO

Ada harga yang harus di bayar untuk sebuah tujuan



KATA PENGANTAR

Pertama tama penulis panjatkan puji syukur atas rahmat dan ridho allah SWT, karena tanpa rahmat dan ridhonya, kami tidak dapat menyelesaikan skripsi ini dengan baik dan selesai tepat waktu.

Tidak lupa penulis ucapkan terima kasih kepat Ibu Senie Destya, ST., M.Kom selaku dosen pembimbing yang membimbing dalam pengerjaan skripsi ini. Penulis juga mengucapkan terima kasih kepada orang tua, teman dan sahabat, serta orang terdekat yang selalu mendukung dalam menyelesaikan skripsi ini.

Mungkin dalam pembuatan skripsi ini terdapat kesalahan yang belum kami ketahui. Maka dari itu penulis mohon saran dan kritik dari teman-teman maupun dosen. Demi terciptanya skripsi yang sempurna.

Yogyakarta, <tanggal bulan tahun>
Penulis

DAFTAR ISI

HALAMAN PERSETUJUAN ---- ii
HALAMAN PENGESAHAN ---- iii
HALAMAN PERSEMBAHAN ---- v
KATA PENGANTAR ---- vii
DAFTAR ISI ---- viii
DAFTAR TABEL ---- x
DAFTAR GAMBAR ---- xi
DAFTAR ISTILAH ---- xii
INTISARI ---- xiii
Abstract ---- xiv
BAB I PENDAHULUAN ---- 1
1.1 Latar Belakang ---- 1
1.2 Rumusan masalah ---- 3
1.3 Tujuan Penelitian ---- 3
1.4 Batasan Masalah ---- 3
1.5 Manfaat Penelitian ---- 4
1.6 Metodologi Penelitian ---- 4
BAB II TINJAUAN PUSTAKA ---- 5
2.1 Literature Review ---- 5
2.2 Landasan Teori ---- 10
2.2.1 Pengertian Phishing ---- 11
2.2.2 Teknik yang biasa digunakan pelaku ---- 12
2.2.3 Metode Eksperimen ---- 14
2.2.4 Identifikasi ---- 14
2.2.5 Platform video meeting ---- 15
2.2.4 Framework ---- 16
2.2.5 Flutter ---- 16
2.2.6 Bahasa Pemrograman ---- 16
2.2.7 Dart ---- 17
2.2.8 Media Pesan ---- 17
BAB III METODOLOGI PENELITIAN ---- 18

3.1 Deskripsi Objek ---- 18
3.2 Alat dan Bahan ---- 18
3.3 Alur Penelitian ---- 18
3.3.1 Alur Simulasi Penyerangan dari sisi penyerang ---- 20
3.3.2 Alur Simulasi Identifikasi dari sisi korban ---- 21
3.3.3 Metode Pengambilan data pada Aplikasi ---- 22
3.4 Metode Analisis ---- 23
3.5 Perancangan Website Phishing ---- 23
3.5.1 Pembuatan struktur *website* ---- 23
3.5.2 Menghubungkan *website* dengan *database* ---- 27
3.5.3 Pengambilan data ---- 29
BAB IV HASIL DAN PEMBAHASAN ---- 31
4.1 Hasil Tampilan Website ---- 31
4.2 Pengujian ---- 33
4.2.1 Simulasi Penyerangan ---- 33
4.2.2 Simulasi Identifikasi ---- 35
4.3 Responder ---- 38
BAB V KESIMPULAN DAN SARAN ---- 41
5.1 Kesimpulan ---- 41
5.2 Saran ---- 41
DAFTAR PUSTAKA ---- 42
LAMPIRAN ---- 43

DAFTAR TABEL

Tabel 2.1 Jurnal Penelitian 5
Tabel 3.1 Alat dan Bahan 17
Tabel 4.1 Tabel hasil penelitian 38

DAFTAR GAMBAR

Gambar 1.1 Grafik jumlah pengguna zoom(Sumber: Playstore) 1
Gambar 1.2 Artikel 26 Maret 2022 2
Gambar 2.1 Contoh tools phishing, HiddenEye 10
Gambar 2.2 Contoh tools phishing, Gopish 11
Gambar 2.3 Contoh phishing SMS 13
Gambar 2.4 Halaman login zoom 15
Gambar 2.5 Halaman login google meet 16
Gambar 3.1 Alur Penelitian 19
Gambar 3.2 Alur dari sisi penyerang 20
Gambar 3.3 Alur dari sisi Korban 21
Gambar 3.4 Flowchart Metode pengambilan data 22
Gambar 3.5 Pembuatan struktur website 23
Gambar 3.6 Struktur website 24
Gambar 3.7 Script code 24
Gambar 3.8 Bagian website 24
Gambar 3.9 Isi folder assets 25
Gambar 3.10 Penambahan package 25
Gambar 3.11 Perintah eksekusi code 25
Gambar 3.12 GreyappBar class 26
Gambar 3.13 Temp class 26
Gambar 3.14 Formulir class 27
Gambar 3.15 Perintah 1 27
Gambar 3.16 Perintah 2 28
Gambar 3.17 Perintah 3 28
Gambar 3.18 Perintah 4 28
Gambar 3.19 Controller 29
Gambar 3.20 Textfield dari Email Address 29
Gambar 3.21 Texfield widget dari Password 29
Gambar 3.22 Submit button widget 30
Gambar 4.1 Tampilan website phishing zoom. 31
Gambar 4.2 Tampilan palsu login form SSO 31
Gambar 4.3 Tampilan palsu login form Apple 32
Gambar 4.4 Tampilan palsu login form Google 32
Gambar 4.5 Tampilan palsu login form Facebook 33
Gambar 4.6 Contoh penyebaran link phishing 33
Gambar 4.7 Tampilan web palsu 34
Gambar 4.8 Korban memasukan data akun 34
Gambar 4.9 Informasi data akun korban dan sandi masuk ke database 35
Gambar 4.10 Pesan email pada korban berisi link phishing 35
Gambar 4.11 Perbadaan domain website phishing dan website asli 36
Gambar 4.12 Perbedaan tampilan website 37
Gambar 4.13 Responder 38
Gambar 4.13 Responder 38

DAFTAR ISTILAH

Phishing	Serangan yang menargetkan ketidak telitian korban
Zoom	Platform aplikasi video meeting
Bahasa Pemrograman	Intruksi standar untuk memerintah computer
Pemrograman	Proses penulisan, pengujian aplikasi dan pemeliharaan kode
Dart	Bahasa pemrograman yang dibuat oleh google
Flutter	Framework yang di tulis menggunakan Bahasa pemrograman dart
Website	Sekumpulan halaman yang di desain dengan Bahasa pemrograman tertentu
Login	Proses memasukan dan validasi data
Simulasi	Percobaan dengan cara reka adegan, atau mem-praktekan

INTISARI

Di masa pandemic covid 19 ini, kita dipaksa untuk mengikuti perkembangan teknologi. Baik pelajar, mahasiswa, guru, dosen, entrepreneur, hingga pemilik perusahaan tentunya harus menggunakan teknologi sebagai sarana untuk menghindari kontak langsung yang mana itulah yang menjadi penyebab utama penularan *covid* 19. Oleh karena itu, di buatlah *inovasi* sebagai pengaplikasian teknologi terhadap lingkungan sosial, yaitu aplikasi pertemuan via video. Contohnya *zoom*, *zoom* adalah aplikasi *video meeting* yang di dalam-nya dapat tercipta lingkungan kerja tanpa harus ada kontak fisik langsung yang dapat menjadi sebab penularan *covid* 19.

Nah, setelah adanya teknologi seperti ini, tentunya akan muncul juga ancaman di dalamnya. Karena seperti yang kita tahu, didalam setiap *inovasi* tentunya ada sisi positif dan juga negatif-nya. Yang akan saya bahas pada penelitian ini adalah kasus kejahatan *siber* yang sering terjadi di lingkungan dunia maya. Serangan ini disebut *phishing*. Seperti Namanya, *phishing* diambil dari kata Bahasa inggris "*fishing*" yang berarti memancing. Serangan ini banyak terjadi di karenakan pengguna atau *user* tidak teliti dalam memperhatikan detail pesan yang dikirimkan oleh seseorang, sehingga dengan mudah tertipu dan menginputkan datanya sendiri kedalam sebuah "jebakan" yang di buat oleh pengirim atau pelaku kejahatan.

Ada beberapa metode yang dilancarkan penyerang untuk melakukan *phising*. Salah satunya adalah yang akan di bahas pada penelitian ini, yaitu *phishing* yang menggunakan metode *replikasi web*.

Kata kunci: *Phishing, Teknologi, Lingkungan Sosial, Aplikasi*

Abstract

In this period of Covid 19 pandemic, we were forced to followed the progression of technology. Whether students, university students, teacher, lecturer, entrepreneur, to the company owners, indeed have to use technology as a means to avoid direct contact which is the main cause of covid 19 transmission.

Therefore, innovation is created as the application of technology to the social environment, namely video meeting application. For an example, zoom is a video meeting application which can create working environment without having direct physical contact which is the main cause of virus transmission. With this technological advancement, we still have the threat within it after all. Because as we know, in every innovation there is positif and negative side within it. In this research I am going to analyze about cyber crime case that still happening in the internet. This attack known as Phishing. As it's name, phishing is taken from the English word "fishing" which means baiting something. This attack is often occurred because user is not carefully in notice detail in messages send by someone, so that they are easily being fooled and inputting their own data to something called "trap" that made by sender or perpetrator.

There are several methods used by attackers to do phishing. One of it will be analyze in this research is phishing using web replication method.

Kata kunci: *Phishing, Technology, Social Environment, Application*