PROYEK AKHIR

ANALISIS *EMAIL PHISING* DAN KARAKTERISTIK *MALWARE* DI KEMENTRIAN KOMUNIKASI DAN INFORMATIKA

Oleh :

RIZKI CAHYA PUTRA

NIM : 203310046

PROGRAM STUDI TEKNOLOGI KOMPUTER
PROGRAM DIPLOMA TIGA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2023

PROYEK AKHIR

ANALISIS *EMAIL PHISING* DAN KARAKTERISTIK *MALWARE* DI KEMENTRIAN KOMUNIKASI DAN INFORMATIKA

Diajukam sebagai salah satu syarat untuk menyelesaikan studi

Program Diploma

Program Studi Teknologi Komputer

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Yogyakarta

Oleh :

RIZKI CAHYA PUTRA

NIM : 203310046

PROGRAM STUDI TEKN-OLOGI KOMPUTER

PROGRAM DIPLOMA TIGA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2023

PERNYATAAN KEASLIAN PROYEK AKHIR

Dengan ini saya menyatakan bahwa naskah Proyek Akhir ini belum pernah diajukan untuk memperoleh gelar Ahli Madya Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 2 Februari 2023

Rizki Cahya Putra

NIM : 203310046

HALAMAN PERSEMBAHAN

Dengan mengucap rasa syukur kehadirat Illahi Rabbi Alhamdulillah tugas akhir ini penulis persembahkan untuk :

- Bapak Adi Kusjani, S.T., M.Eng., selaku Ketua Program Studi Diploma Tiga Teknologi Komputer Fakultas Teknologi Informasi.
- Bapak Totok Budioko, S.T, M.T. yang membimbing hingga terselesainya tugas akhir ini.
- Orang Tua Saya yang telah membesarkan saya dengan kasih sayang yang hangat dan selalu mendoakan saya.
- PT. Kereta Api Indonesai (PERSERO) Daop 6 Yogayarta divisi Sistem Informasi, yang telah memberikan kesempatan untuk mengerjakan proyek ini, semoga dapat berguna dan bermanfaat.
- Bapak Manager dan Assistant Manager Sistem Informasi Daop 6, Kak Pandu, Kak Fatah, Kak Aufa, Kak Okta, Ibu Ningrum, dan orang-orang berhati baik yang sudah membantu saya selama melakukan PKL.
- Anggita Citra yang telah membantu banyak dalam pengerjaan laporan proyek akhir ini.
- Digitalent Schloarship, yang telah memberikan kesempatan untuk magang, semoga dapat berguna dan bermanfaat.
- Teman – teman seperjuangan TK 2020.
- Peserta Magang Talent Schoting Academy di KOMINFO.
- Serta semua pihak yang selalu mendukung saya.

HALAMAN MOTTO

Rahasia kesuksesan adalah mengetahui yang orang lain tidak ketahui

~ Aristotle Onassis ~

Untuk melihat sesuatu yang baru, kau harus membuka jalanmu sendiri

~ Kiy ~

Mimpi tidak berarti apa-apa jika kau tidak menggapainya dengan tanganmu sendiri.

~ Kiy ~

Jangan terlalu ambil hati dengan ucapan seseorang, kadang manusia punya mulut tapi belum tentu punya pikiran.

-Albert Einstein-

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya, penulis dapat menyelesaikan tugas akhir dengan judul: "ANALISIS EMAIL PHISING DAN KARAKTERISTIK *MALWARE* DI KEMENTRIAN KOMUNIKASI DAN INFORMATIKA".

Penulis menyadari bahwa tugas akhir ini masih jauh dari kesempurnaan tanpa bantuan dan bimbingan berbagai pihak sangatlah sulit bagi penulis untuk menyelesaikan tugas akhir ini. Oleh karena itu, Penulis mengucapkan terima kasih kepada:

1. Bapak Adi Kusjani, S.T., M.Eng., selaku Ketua Program Studi Diploma Tiga Teknologi Komputer Fakultas Teknologi Informasi.
2. Bapak Totok Budioko, S.T, M.T., selaku dosen pembimbing yang telah meluangkan waktunya untuk membimbing penulis menyelesaikan tugas akhir.
3. Bapak Herfiedhantya Bhagaskara, selaku mentor Magang dan Studi Independent Bersertifikat di Kementrian Komunikasi dan Informatika.
4. Bapak Antonius Duty Susilo dan Ibu Susmini Indriani Lestariningati, selaku instructor Magang dan Studi Independent Bersertifikat di Kementrian Komunikasi dan Informatika.
5. Kedua Orang tua saya yang memberikan doa dan dukungan dalam hal menuntut Ilmu.
6. Anggita Citra Ayu Fadlika selaku rekan yang telah memberikan support dan motivasi selama Magang/Kerja Praktek (KP) di Kementrian Komunikasi dan Informatika.
7. Dan seluruh pihak yang tidak bisa disebutkan satu persatu yang selalu memberikan dukungan.

Akhir kata, penulis berharap semoga Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu dan semoga laporan hasil Magang/Kerja Praktek (KP) Program Merdeka Belajar Kampus Merdeka ini membawa manfaat.

Yogyakarta, 23 November 2022

Penulis

Rizki Cahya Putra

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Phising secara sederhana dapat diartikan sebagai sebuah penipuan dengan memanfaatkan akun untuk menguak informasi sensitif korban. Phishing memiliki beberapa jenis diantaranya adalah Email Phishing, Spear Phishing, Whaling, Voice Phishing, SMS Phishing, dan masih banyak lagi. Pada email phising biasanya juga terdapat file lampiran yang mengandung *Malware*, *Malware* sendiri adalah software yang dibuat dengan tujuan memasuki dan terkadang merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya.

Analisis *malware* dapat menggunakan metode *dynamic analysis* dengan memanfaatkan beberapa tools dari website seperti talosintelligence, virus total, dan any run untuk analisis lebih mendalam dengan memperhatikan detail mulai dari *ip source email phising, domain,* dan file lampiran untuk mendeteksi apakah *source* tersebut merupakan *malicious* atau tidak.

Analisis *Malware* dapat menghasilkan informasi yang mendetail dari data penyerang seperti alamat IP dan domain yang digunakan apakah terkoneksi dengan *malware* atau tidak. Analisis juga menghasilkan bagaimana cara kerja dan karakteristik dari suatu *malware*.

Kata Kunci : Analisa; *Malware*; *phising*.

ABSTRACT

Phishing in simple terms can be interpreted as a fraud by using an account to uncover sensitive victim information. Phishing has several types including Email Phishing, Spear Phishing, Whaling, Voice Phishing, SMS Phishing, and many more. Phishing e-mails usually contain attached files containing malware. Malware itself is software created with the aim of entering and sometimes damaging computer systems, networks or servers without the owner knowing.

Malware analysis can use the dynamic analysis method by utilizing several tools from websites such as talosintelligence, total virus, and any run for a more in-depth analysis by paying attention to details starting from the ip source of phishing emails, domains, and file attachments to detect whether the source is malicious or not.

Malware Analysis can generate detailed information from attacker data such as IP addresses and domains used whether connected to malware or not. Analysis also produces how to work and the characteristics of a malware.

Keywords: Analysis; malware; phishing.