IMPLEMENTASI WI-FI PASSWORD STEALING PROGRAM ATTACK DENGAN MENGGUNAKAN PERANGKAT RUBBER DUCKY

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer (S.Kom.)

Hansen Edrick Harianto
14110110056

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK DAN INFORMATIKA

UNIVERSITAS MULTIMEDIA NUSANTARA

TANGERANG

2018

HALAMAN PENGESAHAN

IMPLEMENTASI WI-FI PASSWORD STEALING PROGRAM ATTACK DENGAN MENGGUNAKAN PERANGKAT RUBBER DUCKY

Oleh

Nama	: Hansen Edrick Harianto
NIM	: 14110110056
Fakultas	: Teknik dan Informatika
Program Studi	: Informatika

Tangerang, 31 Juli 2018

Ketua Sidang

Maria Irmina Prasetiyowati, S.Kom., M.T.

Dosen Penguji

Farica Perdana Putri, S.Kom., M.Sc.

Dosen Pembimbing

Dennis Gunawan, S.Kom., M.Sc.

Ketua Program Studi

Informatika

Seng Hansun, S.Si., M.Cs.

ii

PERNYATAAN TIDAK MELAKUKAN PLAGIAT

Dengan ini saya:

Nama : Hansen Edrick Harianto

NIM : 14110110056

Fakultas : Teknik dan Informatika

Program Studi : Informatika

menyatakan bahwa skripsi yang berjudul "**Implementasi Wi-Fi Password Stealing Program Attack Dengan Menggunakan Perangkat Rubber Ducky**" ini adalah karya ilmiah saya sendiri, bukan plagiat dari karya ilmiah yang ditulis oleh orang lain atau lembaga lain, dan semua karya ilmiah orang lain atau lembaga lain yang dirujuk dalam skripsi ini telah disebutkan sumber kutipannya serta dicantumkan di Daftar Pustaka. Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan skripsi, saya bersedia menerima konsekuensi dinyatakan tidak lulus untuk mata kuliah Skripsi yang telah saya tempuh.

Tangerang, 31 Juli 2018

Hansen Edrick Harianto

iii

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitasi akademik Universitas Multimedia Nusantara, saya yang bertanda tangan di bawah ini:

Nama : Hansen Edrick Harianto

NIM : 14110110056

Program Studi : Informatika

Fakultas : Teknik dan Informatika

Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui dan memberikan izin kepada **Universitas Multimedia Nusantara** hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right)* atas karya ilmiah saya yang berjudul: **Implementasi Wi-Fi Password Stealing Program Attack Dengan Menggunakan Perangkat Rubber Ducky**.

Dengan Hak Bebas Royalti Non-eksklusif ini, pihak Universitas Multimedia Nusantara berhak menyimpan, mengalihmedia atau *format*-kan, mengelola dalam bentuk pangkalan data (*database),* merawat, dan medistribusi serta menampilkan atau mempublikasikan karya ilmiah saya di internet atau media lain untuk kepentingan akademis, tanpa perlu meminta izin dari saya maupun memberikan *royalty* kepada saya, selama tetap mencantumkan nama saya sebagai penulis karya ilmiah tersebut.

Demikian pernyataan ini saya buat dengan sebenarnya untuk dipergunakan sebagaimana mestinya.

Tangerang, 31 Juli 2018

(Hansen Edrick Harianto)

iv

HALAMAN PERSEMBAHAN/MOTTO

Stop saying "I wish",

Start saying "I will".

KATA PENGANTAR

Puji dan syukur dipanjatkan kepada Tuhan Yang Maha Esa, karena atas rahmat-Nya penyusuan laporan skripsi dengan judul "Implementasi Wi-Fi Password Stealing Program Atttack Dengan Menggunakan Perangkat Rubber Ducky" dapat diselesaikan. Laporan skripsi ini disusun sebagai salah satu syarat untuk kelulusan mata kuliah Skripsi.

Beberapa pihak telah membantu dalam melewati rintangan-rintangan yang terjadi selama pembuatan laporan ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Dr. Ninok Leksono, selaku Rektor Universitas Multimedia Nusantara,
2. Hira Meidia, Ph.D., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara,
3. Seng Hansun, S.Si., M.Cs., selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara,
4. Dennis Gunawan, S.Kom., M.Sc., selaku Dosen Pembimbing yang telah membantu dalam menyusun laporan skripsi,
5. Fransiska Elviana Arly, yang telah membantu dan menemani penulis dalam masa-masa sulit,
6. Edwin Handoko, Kenny Wantara, dan Sintya Oktaviani, yang telah mendukung penulis selama proses pembuatan laporan skripsi,
7. Febrian Wilson dan Kevin Alexander, yang telah memberikan saran kepada penulis selama proses pembuatan laporan skripsi,

8. Christine Liviani, Kennard Alcander, dan Samuel Sandro Setiawan, yang telah menemani penulis dalam masa pembuatan laporan skripsi.
9. Adrian Pramudita Dharma, Andri Hardono Hutama, Raymond Anggara, William Darmawi, dan Yudy, yang selalu menyemangati penulis selama proses pembuatan laporan skripsi.
10. Keluarga dan teman-teman yang telah membantu dalam pembuatan laporan ini.

Semoga laporan skripsi ini dapat bermanfaat bagi para pembaca.

Tengerang, 31 Juli 2018

Hansen Edrick Harianto

vii

IMPLEMENTASI WI-FI PASSWORD STEALING PROGRAM ATTACK DENGAN MENGGUNAKAN PERANGKAT RUBBER DUCKY

ABSTRAK

Waktu yang dibutuhkan oleh seorang peretas untuk mendapatkan informasi yang terdapat dalam sebuah komputer seperti *Wi-Fi password* hanyalah 1 menit. Dikarenakan oleh keterbatasan kemampuan manusia untuk mengingat lebih dari 1 *password* yang unik dan kompleks, pengguna cenderung menggunakan *password* yang sama untuk setiap akun yang dimiliki. Oleh karena itu, *Wi-Fi password stealing program* ini dibangun untuk mengimplementasikan *password stealing program attack* dengan menggunakan bahasa USB Rubber Ducky, VB *script*, *web server*, *command prompt*, dan Ducky Toolkit. Berdasarkan uji coba yang dilakukan dapat diketahui bahwa tingkat kesuksesan program mencapai 94.28% dengan 87.87% *password* yang telah didapatkan masih tergolong sebagai *guessable* dan tingkat kesamaan penggunaan *password* mencapai 81.81%. Sehingga, *Wi-Fi password stealing program* dapat menjadi sangat berbahaya karena sebagian besar *password* yang digunakan masih tergolong lemah dan digunakan pada banyak akun yang dimiliki.

Kata Kunci: Pencurian *Password*, Kekuatan *Password*, Kesamaan *Password*, USB Rubber Ducky, *Wi-Fi*

IMPLEMENTATION OF WI-FI PASSWORD STEALING PROGRAM ATTACK USING RUBBER DUCKY DEVICE

ABSTRACT

A minute is all it takes for a hacker to gain information from your computer such as Wi-Fi password. Due to the limited capability of people to remember a lot of complex and unique password, people tend to use same password for most of their account. Therefore, Wi-Fi password stealing program was built to implement password stealing program attack using USB Rubber Ducky Scripting, Visual Basic Script, Web Server, Command Prompt, and Ducky Toolkit to obtain clear text Wi-Fi password that ever connected to the computer. Based on the testing phase, the success rate of Wi-Fi password stealing program reached 94.28% with 87.87% obtained personal password is still categorized as guessable password and the password reuse rate reached 81.81%. Thus, Wi-Fi password stealing program can be very dangerous as most of the personal password used in lots of account and still categorized as guessable.

Keywords: Password Stealing, Password Strength, Password Reuse, USB Rubber Ducky, Wi-Fi

DAFTAR ISI

HALAMAN PENGESAHAN ii
PERNYATAAN TIDAK MELAKUKAN PLAGIAT iii
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH
UNTUK KEPENTINGAN AKADEMIS iv
HALAMAN PERSEMBAHAN/MOTTO v
KATA PENGANTAR vi
ABSTRAK viii
ABSTRACT ix
DAFTAR ISI x
DAFTAR GAMBAR xi
DAFTAR TABEL xii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 5
1.4 Tujuan Penelitian 5
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan 5
BAB II LANDASAN TEORI 7
2.1 Infrastruktur USB Rubber Ducky 7
2.2 Bahasa yang Digunakan USB Rubber Ducky 9
2.3 Wi-Fi 9
2.4 Password 10
2.5 Password Stealing Attack 12
2.6 Zxcvbn Password Analysis Library 14
2.7 System Hacking 17
BAB III METODOLOGI DAN PERANCANGAN PROGRAM 19
3.1 Metodologi Penelitian 19
3.2 Proses Penyusunan USB Rubber Ducky 21
3.3 Metodologi System Hacking pada Wi-Fi Password Stealing Program Attack 22
3.4 Perancangan Wi-Fi Password Stealing Program 23
BAB IV IMPLEMENTASI DAN UJI COBA 33
4.1 Spesifikasi Sistem 33
4.2 Implementasi 33
4.3 Uji Coba 42
BAB V SIMPULAN DAN SARAN 48
5.1 Simpulan 48
5.2 Saran 49
DAFTAR PUSTAKA 50
DAFTAR LAMPIRAN 52

DAFTAR GAMBAR

Gambar 2.1 Komponen USB Rubber Ducky 8
Gambar 2.2 Potongan Kode Untuk Mengambil SAM File 14
Gambar 2.3 Zxcvbn *Pattern Matching* 16
Gambar 2.4 *System Hacking Methodology* 18
Gambar 3.1 Komponen-Komponen Perangkat Rubber Ducky 22
Gambar 3.2 *Disabling Firewall Error Message* 24
Gambar 3.3 FTP *Protection Message* 24
Gambar 3.4 Non-aktivasi *firewall* 25
Gambar 3.5 *Extracting Wi-Fi Information* 26
Gambar 3.6 *Sending* XML *Files* 27
Gambar 3.7 Proses Kompilasi dan Menjalankan _zipIt.vbs 27
Gambar 3.8 *Flowchart* compress & zip directory using VB script 28
Gambar 3.9 Membuka Koneksi FTP 29
Gambar 3.10 Proses Pengunggahan *File* 29
Gambar 3.11 Penutupan Koneksi FTP 29
Gambar 3.12 Proses Aktivasi *Firewall* 31
Gambar 3.13 Model Aplikasi 31
Gambar 3.14 Flowchart *Wi-Fi Password Stealing Program* 32
Gambar 4.1 Potongan Kode Untuk Membuka *Command Prompt* 34
Gambar 4.2 Potongan Kode Untuk Non-aktivasi *Firewall* 34
Gambar 4.3 Potongan Kode Untuk Membuat dan berpindah ke direktori wifi . 35
Gambar 4.4 Potongan Kode *Extract Wi-Fi Information* 35
Gambar 4.5 *Wi-Fi Information XML File* 36
Gambar 4.6 Potongan Kode Pembuatan VB *Script* 37
Gambar 4.7 Potongan Kode *Compress & Zip* 37
Gambar 4.8 Potongan Kode Membuka Koneksi FTP 38
Gambar 4.9 Potongan Kode Mengunggah *File* ke *Server* 38
Gambar 4.10 Potongan Kode Untuk Menutup Koneksi FTP 39
Gambar 4.11 Potongan Kode Untuk Menghapus Direktori wifi 39
Gambar 4.12 Potongan Kode Untuk Menghapus VB *Script* 40
Gambar 4.13 Potongan Kode Untuk Menghapus *Zipped File* 40
Gambar 4.14 Potongan Kode Aktivasi *Firewall* 40
Gambar 4.15 Potongan Kode Untuk Menutup *Command Prompt* 41
Gambar 4.16 Potongan Kode Untuk Melakukan Analisa *Password* 41
Gambar 4.17 Grafik Tingkat Kekuatan *Password* Golongan Korban 43
Gambar 4.18 Grafik Tingkat Kekuatan *Password* Golongan Pengusaha 44
Gambar 4.19 Grafik Tingkat Kekuatan *Password* Golongan Lain-Lain 44
Gambar 4.20 Grafik Tingkat Kekuatan *Password* Golongan Mahasiswa 45
Gambar 4.21 Grafik Tingkat Kesamaan Penggunaan *Password* 46
Gambar 4.22 Grafik Tingkat Kesamaan Penggunaan *Password* Golongan Lain-Lain 47
Gambar 4.23 Grafik Tingkat Kesamaan Penggunaan *Password* Golongan Mahasiswa 47

DAFTAR TABEL

Tabel 2.1 Persentase Kecocokan *Password* terhadap *Regular Expression*..... 12
Tabel 2.2 Tabel Zxcvbn *Score* 16
Tabel 4.1 Tabel Kecocokan *Regular Expression*..... 43
Tabel 4.2 Tabel Kecocokan *Regular Expression* Pengusaha..... 44
Tabel 4.3 Tabel Kecocokan *Regular Expression* Orang Awam 45
Tabel 4.4 Tabel Kecocokan *Regular Expression* Mahasiswa..... 46