Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Team project ©2017
Dony Pratidana S. Hum | Bima Agus Setyawan S. IIP

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan dalam bidang komputer merupakan hal krusial yang dapat merugikan banyak orang jika seseorang atau sebuah organisasi berhasil menemukan celah dan melakukan eksploitasi terhadap sistem tersebut. Celah yang sangat sering dimanfaatkan oleh para penyerang adalah *password*. Hal ini dikarenakan setiap individu memiliki keterbatasan daya ingat dalam hal mengingat *password* (Silver dkk., 2014).

Password merupakan sebuah kunci keamanan yang dapat melindungi detil pengguna seperti nomor rekening bank, nomor kartu kredit, dan informasi mengenai pengguna. Oleh karena itu, *password* menjadi sesuatu yang akan diserang pertama kali oleh para penyerang. Penelitian membuktikan bahwa setiap individu memiliki keterbatasan daya ingat dalam hal mengingat *password* sehingga banyak pengguna yang menggunakan *password* yang sama di setiap akun. Akun tersebut dapat mengandung informasi sensitif mengenai pengguna sehingga hal ini dapat menjadi sangat berbahaya bagi pengguna jika penyerang berhasil mendapatkan *password* pengguna (Nikose dkk., 2014). Salah satu celah keamanan yang dapat dimanfaatkan oleh penyerang adalah lemahnya kualitas *password* yang dimiliki oleh pengguna sehingga memungkinkan penyerang untuk melakukan *password attack*.

Password stealing attack merupakan sebuah kegiatan mencuri *password* seseorang dengan tujuan untuk mendapatkan informasi sensitif dari korban seperti detil dari kartu kredit. *Password stealing* dapat dilakukan dengan berbagai cara

Implementasi Wi-Fi Password..., Hansen Edrick Harianto, FTI UMN, 2018

seperti *phishing, password stealing program, social engineering,* dan penggunaan *Trojan*. *Password stealing program* dibagi menjadi 2 yaitu *keylogger program* dan *malicious code* (Venkadesh.S & K.Palanivel, 2015). *Malicious code* merupakan sekumpulan kode yang bertujuan untuk mengeksploitasi kelemahan dalam aspek keamanan baik di jaringan atau komputer. *Malicious code* sudah dimanfaatkan di banyak kasus kejahatan *cyber* seperti *Love Bug* yang tergolong *mobile code virus* dan menyebar sangat cepat dengan menggunakan bahasa pemrograman *VB script*. Sementara *Trinoo* adalah contoh lain dari pemanfaatan *malicious code* yang tergolong *remote-control attack script* dan tersebar secara luas pada tahun 2000 (McGraw & Morrisett, 2000).

Microcontroller Universal Serial Bus (USB) merupakan suatu teknologi yang memiliki *interface* USB dengan fungsi untuk melakukan komunikasi *machine to machine* terhadap komputer maupun server (Raj, Rahman, & Anand, 2016). Salah satu contoh dari *microcontroller Universal Serial Bus* adalah USB *Rubber Ducky.* USB *Rubber Ducky* memanfaatkan kelemahan yang ada pada komputer karena komputer menganggap setiap *input* yang dilakukan oleh pengguna merupakan sesuatu yang aman. USB *Rubber Ducky* merupakan sebuah *flashdisk* yang dapat menjalankan sekumpulan perintah yang dikompilasi menjadi sebuah *payload* hanya dengan memasang *flashdisk* tersebut ke dalam sebuah komputer. Hal ini dapat menjadi sangat berbahaya karena tingkat kesadaran masyarakat mengenai benda ini masih sangat sedikit. USB *Rubber Ducky* memiliki bentuk yang sangat menyerupai *flashdisk* pada umumnya sehingga tanpa memasang *flashdisk* tersebut ke dalam komputer benda ini hampir tidak dapat dikenali sebagai USB *Rubber Ducky* (Tyler, 2015). Terlebih lagi sekitar 85% dari komputer yang menggunakan sistem operasi

Windows menggunakan akun *administrator* untuk melakukan tugas sehari-hari (Motiee dkk., 2010). Penggunaan akun *administrator* memungkinkan penyerang untuk mengeksekusi perintah yang membutuhkan *administrator privilege*.

USB *Rubber Ducky* sudah mulai dimanfaatkan oleh para penyerang sebagai alat bantu dalam melakukan penyerangan terhadap korban. Salah satu contoh penyerangan yang dilakukan adalah *malware installation* terhadap sebuah komputer dengan menggunakan USB *Rubber Ducky*. Hal ini dapat dilakukan dengan menyiapkan sebuah *web server* yang memiliki kapabilitas untuk melakukan kegiatan *upload & download* sehingga penyerang dapat mengunduh *malware* dan *malware* tersebut dapat mengirimkan informasi sensitif kembali ke *web server*. Pemanfaatan USB *Rubber Ducky* terletak pada kegiatan mengunduh *malware* tersebut dari *web server* dengan menuliskan sebuah perintah pada *powershell* yang memerintahkan komputer untuk mengunduh sesuatu dari sebuah halaman web (Benjamin Cannols & Ahmad Ghafarian, 2017).

Selain pemanfaatan di atas, USB *Rubber Ducky* juga sudah dimanfaatkan untuk mengambil *logon password* dengan penggunaan Mimikatz secara *remote*. Hal ini dilakukan dengan cara membangun sebuah koneksi ke sebuah *web server* yang memiliki mimikatz.exe dan sekurlsa.dll. Setelah membangun koneksi tersebut maka penyerang dapat memanfaatkan USB *Rubber Ducky* untuk mengunduh data sekurlsa.dll lalu menjalankan mimikatz.exe secara *remote*. Pemanfaatan USB *Rubber Ducky* di atas dapat menghindari deteksi *antivirus* sehingga meningkatkan tingkat keberhasilan penyerang untuk mendapatkan *logon password* (Benjamin Cannols & Ahmad Ghafarian, 2017).

USB *Rubber Ducky* juga dapat dimanfaatkan untuk melewati kode keamanan dari sebuah perangkat *mobile*. Dengan memanfaatkan akses fisik terhadap perangkat *mobile*, USB *Rubber Ducky* dapat mengadopsi metode *brute force*. Teknik ini dapat melewati kode keamanan dalam waktu kurang dari 17 jam untuk menebak 4 digit PIN. Meskipun setiap perangkat *mobile* memiliki sistem proteksi yang membuat penyerang harus memberikan jeda waktu 30 detik untuk melakukan percobaan berikutnya (Neely, 2016).

Berdasarkan permasalahan di atas, dilakukan implementasi *Wi-Fi password stealing program attack* dengan menggunakan perangkat *Rubber Ducky* untuk meneliti tingkat keberhasilan program yang telah dibuat.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut.

1. Bagaimana cara mengimplementasikan *Wi-Fi password stealing program attack* untuk mendapatkan daftar informasi *Wi-Fi* dari sebuah komputer dengan menggunakan perangkat *Rubber Ducky*?
2. Bagaimana tingkat keberhasilan *Wi-Fi password stealing program attack* dalam mendapatkan daftar informasi *Wi-Fi* dari sebuah komputer dengan menggunakan perangkat *Rubber Ducky*?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut.

1. *Platform* sistem operasi yang digunakan adalah sistem operasi Windows.
2. Komputer yang diserang harus memiliki koneksi internet.
3. Komputer sedang menggunakan akun *administrator*.

4. Penyerang memiliki *physical access* terhadap komputer dan korban tidak berada di lokasi penyerangan.

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut.

1. Mengimplementasikan *password stealing program attack* untuk mendapatkan daftar informasi *Wi-Fi* yang tersimpan pada sebuah komputer dengan menggunakan perangkat *Rubber Ducky*.
2. Mengukur tingkat keberhasilan *Wi-Fi password stealing program attack* dalam mendapatkan daftar informasi *Wi-Fi* dari sebuah komputer dengan menggunakan perangkat *Rubber Ducky*.

1.5 Manfaat Penelitian

Manfaat dilakukannya penelitian ini adalah sebagai berikut.

1. Menyadarkan masyarakat mengenai bahaya dari perangkat *Rubber Ducky*.
2. Menyadarkan masyarakat mengenai pentingnya menjaga keamanan *password.*

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari lima bab, yaitu sebagai berikut.

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini menjelaskan landasan teori dari penelitian yang dilakukan, seperti infrastruktur perangkat *Rubber Ducky*, bahasa yang digunakan perangkat *Rubber Ducky*, *Wi-Fi*, *password*, *password stealing attack*, Zxcvbn *password analysis library* dan *system hacking*.

BAB III METODOLOGI DAN PERANCANGAN PROGRAM

Bab ini berisi tentang metode penelitian yang digunakan dan perancangan program yang direpresentasikan dengan perancangan *flowchart*, proses penyusunan perangkat Rubber Ducky, proses *system hacking* dan eksperimen perancangan program.

BAB IV IMPLEMENTASI DAN UJI COBA

Bab ini berisi tentang implementasi dan uji coba aplikasi yang dibangun.

BAB V SIMPULAN DAN SARAN

Bab ini berisi simpulan dari hasil pengujian aplikasi dan saran untuk pengembangan aplikasi selanjutnya.

UNIVERSITAS
MULTIMEDIA
NUSANTARA