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.

BAB II

LANDASAN TEORI

2.1 Infrastruktur USB Rubber Ducky

USB *Rubber Ducky* terdiri dari berbagai komponen yang didesain untuk menjalankan sekumpulan *script* yang telah ditulis oleh penyerang seperti pada Gambar 2.1. Komponen-komponen yang dimaksud adalah sebagai berikut.

1. *Micro SD Storage*
2. *Replay Button*
3. *LED Indicator*
4. *Type a Plug*
5. *60 MHz 32-Bit CPU*
6. *Covert Case*
7. *Optional Decal*

Micro SD storage merupakan tempat dimana *memory card* yang berisi *payload* akan diletakkan. Hal ini merupakan salah satu bagian terpenting dari USB *Rubber Ducky* karena *payload* merupakan sekumpulan perintah yang akan dijalankan pada saat USB *Rubber Ducky* tersebut dipasang ke dalam komputer. *Payload* memegang peran yang sangat penting dalam hal penggunaan USB *Rubber Ducky* karena dapat memberikan perintah sesuai dengan keinginan penyerang.

Replay button merupakan tombol yang jika ditekan maka akan menjalankan perintah yang terdapat dalam *payload* sekali lagi. Tombol ini digunakan pada saat USB telah terpasang ke dalam komputer. Namun, penyerang ingin menjalankan ulang perintah yang terdapat pada *payload*.

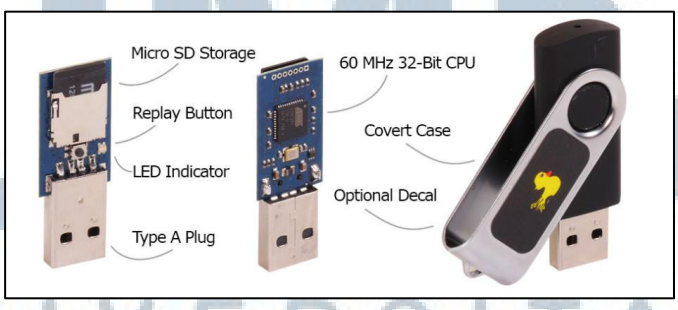
Implementasi Wi-Fi Password..., Hansen Edrick Harianto, FTI UMN, 2018

LED indicator merupakan lampu yang menandakan sukses atau gagalnya kegiatan injeksi *payload* ke dalam sebuah komputer. Lampu ini akan membantu penyerang dalam menentukan kegiatan apa yang akan dilakukan selanjutnya oleh penyerang.

Type a plug merupakan USB yang akan menjadi penghubung antara CPU di dalam USB *Rubber Ducky* dengan sebuah komputer. USB *interface* yang digunakan adalah *type* A. USB sangat dibutuhkan agar CPU dan komputer korban dapat saling berkomunikasi.

60 MHz 32-Bit CPU merupakan otak dari USB *Rubber Ducky* yang akan menjalankan sekumpulan *script* yang telah dikompilasi menjadi sebuah *payload.* Pada saat USB *Rubber Ducky* dipasang ke dalam komputer maka CPU akan menjalankan *payload* tersebut.

Covert case dan *optional decal* merupakan sebuah penutup USB guna menyamarkan USB *Rubber Ducky* sebagai USB biasa. Penutup ini dapat mengambil peran besar dalam hal mendapatkan kepercayaan korban agar dapat mendapatkan akses fisik ke perangkat korban (Tyler, 2015).



Gambar 2.1 Komponen USB Rubber Ducky
(Sumber : *USB Rubber Ducky Analysis*, 2015)

UNIVERSITAS MULTIMEDIA NUSANTARA

2.2 Bahasa yang Digunakan USB Rubber Ducky

USB *Rubber Ducky* menggunakan bahasa yang sangat sederhana yang sebagian besar terdiri dari bahasa yang terdapat pada *keyboard*. Perintah-perintah yang perlu diketahui dalam USB *Rubber Ducky* adalah sebagai berikut.

1. REM : untuk memberikan komentar
2. WINDOWS : memiliki kegunaan yang sama dengan tombol *windows* pada keyboard
3. DELAY : untuk menunda aktivitas yang akan dijalankan sesudah suatu perintah dijalankan
4. STRING : untuk menuliskan sebuah kalimat
5. ENTER : memiliki kegunaan yang sama dengan tombol *enter* yang ada pada keyboard

Selain hal yang disebutkan di atas, penyerang juga dapat menggunakan sebutan yang sama dengan *keyboard* untuk memberikan suatu perintah. Jika ingin menutup sebuah aplikasi maka cukup dengan menuliskan “ALT F4”. Contoh lain yang dapat dilakukan adalah dengan menuliskan “WINDOWS R” untuk menjalakan fungsi run (Tyler, 2015).

2.3 Wi-Fi

Wi-Fi merupakan salah satu teknologi *wireless* yang sedang memimpin dalam kehidupan sehari-hari. *Wi-Fi* memungkinkan perangkat elektronik berkomunikasi satu sama lain tanpa perlu terhubung sebuah kabel. Teknologi ini memiliki 2 komponen utama untuk dapat dikenali yaitu SSID dan *authentication*. SSID merupakan nama dari sebuah jaringan yang akan dipancarkan secara terus menerus agar klien dapat menemukan jaringan tersebut. Sementara *authenthication*

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

digunakan untuk melakukan otentikasi terhadap *user* dengan menggunakan metode enkripsi tertentu terhadap sebuah *password*. Teknologi *authenthication* ini mulai berkembang dengan hadirnya *Wired Equivalent Privacy* (WEP). WEP menggunakan algoritma RC4 dalam melakukan teknik enkripsi yang setelah diteliti tergolong tidak aman sehingga dikembangkanlah protokol *Wi-Fi Protected Access* (WPA/WPA2).

WPA/WPA2 menggunakan *Temporal Key Integrity Protocol* (TKIP) sebagai teknik enkripsi yang secara terus menerus dan otomatis akan mengubah kunci yang digunakan oleh klien dan *access point*. Namun masih terdapat kelemahan pada TKIP yang memungkinkan penyerang untuk melakukan dekripsi terhadap paket tertentu sehingga dapat dimanfaatkan di penyerangan berikutnya. Berikutnya dikembangkanlah WPA2-PSK yang menggunakan teknik enkripsi *Advanced Encryption System* (AES) yang dapat dikategorikan aman untuk saat ini (WNDW, 2013).

Wi-Fi sudah banyak dimanfaatkan dan dianggap sebagai aspek terpenting yang akan dilihat oleh banyak orang. Sekitar 42% *Wi-Fi* tidak memiliki mekanisme keamanan sehingga menimbulkan banyak sekali celah yang dapat dimanfaatkan oleh penyerang untuk melakukan kejahatan *cyber* (Muppavarapu, 2014).

2.4 Password

Password merupakan sebuah mekanisme otentikasi yang digunakan untuk mendapatkan akses terhadap suatu sistem. *Password* pada umumnya terdiri dari beberapa jenis karakter yaitu huruf kecil, huruf besar, angka, simbol, dan *unicode* (Devillers, 2010). Tingkat kecocokan sebuah *password* berdasarkan beberapa *regular expression* dengan menggunakan *italian dataset* (IT), *finnish dataset* (FI),

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

dan *myspace dataset* (MS) dapat dilihat pada Tabel 2.1. Untuk meningkatkan keamanan sebuah *password* setiap individu dianjurkan untuk mengganti *password* secara berkala, menjaga kerahasiaan *password*, serta menggunakan *password* yang berbeda untuk setiap sistem. Sistem yang dapat menjaga keamanan *password* dengan baik akan menyimpan *password* yang sudah terenkripsi sehingga keamanan *password* tetap terjaga sekalipun penyerang berhasil mendapatkan akses ke daftar *password* (Robert Morris & Ken Thompson, 1979). Sistem yang baik juga akan menerapkan beberapa peraturan saat pengguna membuat sebuah *password* pada sebuah sistem. Peraturan yang dibuat oleh sebuah sistem pada umumnya adalah sebagai berikut (Venkadesh.S & K.Palanivel, 2015).

1. *Password syntax*: sebuah *password* diharuskan memiliki batas panjang minimal, batas minimal jumlah digit, dan batas minimal jumlah huruf.
2. *Dictionary words*: sebuah *password* tidak boleh terdapat pada kamus.
3. *Password re-use*: sebuah *password* diharuskan berbeda dari beberapa *password* terakhir yang didaftarkan.
4. *Most common password*: sebuah *password* tidak boleh digunakan jika terdapat pada daftar *password* yang sering digunakan.
5. *Popular password*: sebuah *password* tidak boleh digunakan jika terdapat populasi yang cukup besar dalam sebuah sistem yang menggunakan *password* yang sama.

UNIVERSITAS MULTIMEDIA NUSANTARA

Tabel 2.1 Persentase Kecocokan *Password* terhadap *Regular Expression* (Sumber : *Password Strength: An Empirical Analysis*, 2010)

Expression	Example	IT	FI	MS
[a-z] +	abcdef	51.21%	53.06%	1.09%
[A-Z] +	ABCDEF	0.29%	0.17%	0%
[A-Za-z] +	AbCdEf	53.74%	54.04%	1.09%
[0-9]+	123456	9.10%	3.43%	0.15%
[a-zA-Z0-9] +	A1b2C3	93.43%	95.43%	90.43%
[a-z] + [0-9] +	abc123	14.51%	27.10%	77.39%
[a-z] + 1	abcde1	0.26%	1.43%	19.89%
[a-zA-Z] + [0-9] +	aBc123	16.30%	28.03%	77.48%
[0-9] + [a-zA-Z] +	123aBc	1.80%	2.16%	5.76%
[0-9] + [a-z] +	123abc	1.65%	2.09%	5.75%

2.5 Password Stealing Attack

Password stealing attack merupakan sebuah tindakan yang bertujuan untuk mendapatkan *password* secara *plain text* dari seorang individu dan memanfaatkan *password* tersebut untuk mendapatkan akses ke akun individu tersebut. *Password stealing attack* dibagi menjadi 3 cara yaitu sebagai berikut (Venkadesh.S & K.Palanivel, 2015).

1. *Password stealing program attack*

   Password stealing program attack merupakan sebuah teknik penyerangan dimana penyerang membuat sebuah program yang dapat mengambil informasi mengenai *username* atau *password* yang disimpan oleh pengguna baik dalam sistem operasi dan *password manager* ataupun saat pengguna mengetik informasi tersebut. *Password stealing program attack* dibagi ke dalam beberapa cara yaitu sebagai berikut.

   A. *Keylogger program*

      Keylogger program adalah sebuah program yang merekam setiap *key strokes* yang dilakukan oleh pengguna. Sehingga saat pengguna mengetik

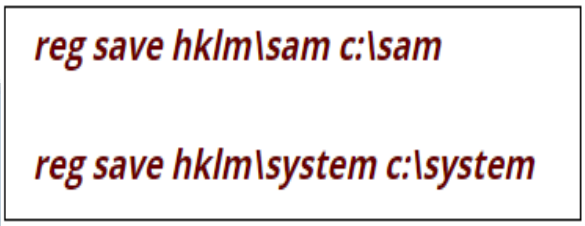
Implementasi Wi-Fi Password..., Hansen Edrick Harianto, FTI UMN, 2018

informasi seperti *username* dan *password* akan terekam di *keylogger program* tersebut.

B. *Malicious code*

Malicious code adalah sebuah kode yang memiliki fungsi untuk mengambil hal sensitif seperti *username* atau *password* dan mengirimkan data tersebut ke server penyerang sehingga penyerang dapat mendapatkan data tersebut secara *remote*. Penyerang memanfaatkan perintah-perintah dalam *powershell* untuk membuat pengguna mengirimkan informasi mengenai sebuah akun tanpa disadari. Contoh program yang digunakan oleh penyerang adalah Mimikatz yang dapat mengambil *logon password* secara *plain text*, sedangkan contoh potongan kode yang dapat digunakan untuk mendapatkan sebuah *password* dari suatu sistem dapat dilihat pada Gambar 2.2. Perintah pada gambar tersebut menjelaskan bagaimana penyerang dapat memanfaatkan *command line* untuk mendapatkan SAM *file* yang menyimpan seluruh informasi mengenai *user* yang pernah berinteraksi dengan komputer tersebut. Penyerang dapat menyembunyikan *malicious code* ke dalam sebuah *Trojan* untuk mempermudah penyerang saat memasukkan *malicious code* tersebut ke dalam komputer korban. Penyerang hanya perlu menunggu korban untuk mengaktifkan *Trojan* tersebut untuk mendapatkan informasi sensitif mengenai korban.

UNIVERSITAS MULTIMEDIA NUSANTARA



Gambar 2.2 Potongan Kode Untuk Mengambil *Security Account Manager* (SAM) File
(Sumber : *A Survey on Password Stealing Attacks and Its Protecting Mechanism*, 2015)

2. *Phishing attack*

   Phishing merupakan sebuah ancaman dengan tujuan untuk mendapatkan informasi seperti *username* dan *password* secara *online*. Penyerang dapat memancing korban untuk memberikan informasi mengenai korban dengan menyebarkan sebuah email yang berisikan sebuah konten yang dapat menarik perhatian korban.

3. *Shoulder surfing attack*

   Shoulder surfing attack merupakan bagian dari *social engineering* dimana penyerang mengintip saat pengguna memasukkan informasi rahasia seperti *username* dan *password*.

2.6 Zxcvbn Password Analysis Library

Password analysis adalah sebuah kegiatan untuk melakukan pengukuran kekuatan terhadap sebuah *password* yang didasari oleh beberapa metrik. Zxcvbn merupakan salah satu *library* yang terkenal dan sudah digunakan oleh Dropbox dalam melakukan pengecekan *password* pada saat proses *sign up*. Zxcvbn memiliki 3 proses utama yaitu *match, score,* dan *search*. Pada proses *match,* zxcvbn

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

melakukan proses *pattern matching* terhadap beberapa aspek sebagai berikut seperti pada Gambar 2.3 (Wheeler, 2016).

1. *Token*

   Mencocokkan *substring* dari *password* terhadap sebuah *dictionary* yang menjadi basis dari pengecekan zxcvbn.

2. *Reversed*

   Mencocokkan *password* yang di-*reversed* terhadap sebuah *dictionary* yang menjadi basis dari pengecekan zxcvbn.

3. *Sequence*

   Menemukan rangkaian karakter dengan *unicode* yang berurutan dalam sebuah *password*.

4. *Repeat*

   Menemukan rangkaian karakter berulang dalam sebuah *password*.

5. *Keyboard*

   Menemukan rangkaian karakter yang bersebelahan pada *keyboard* dalam sebuah *password*.

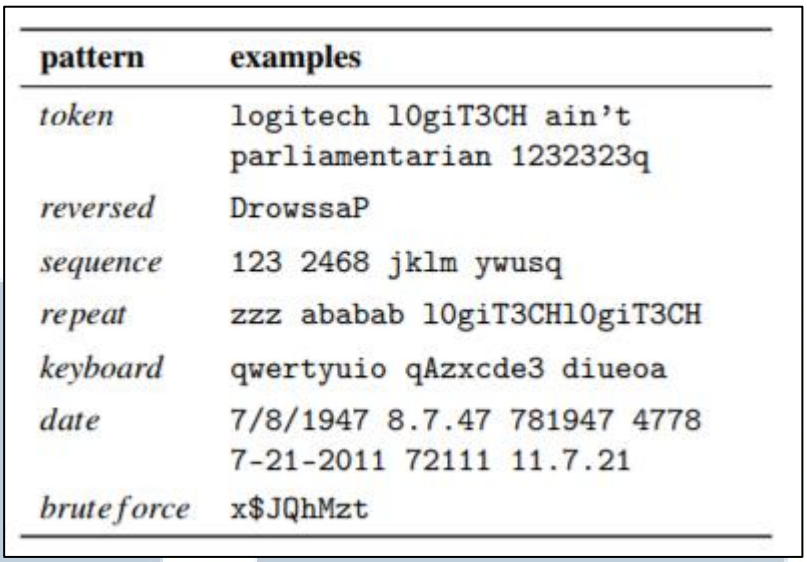
6. *Date*

   Menemukan rangkaian karakter yang membentuk sebuah tanggal pada *password*.

7. *Bruteforce*

   Melakukan estimasi waktu jika dilakukan *bruteforce* terhadap sebuah *password*.

UNIVERSITAS MULTIMEDIA NUSANTARA



pattern	examples
token	logitech l0giT3CH ain't parliamentarian 1232323q
reversed	DrowssaP
sequence	123 2468 jklm ywusq
repeat	zzz ababab l0giT3CHl0giT3CH
keyboard	qwertyuio qAzxcde3 diueoa
date	7/8/1947 8.7.47 781947 4778 7-21-2011 72111 11.7.21
brute force	x$JQhMzt

Gambar 2.3 Zxcvbn *Pattern Matching*
(Sumber : *zxcvbn: Low-Budget Password Strength Estimation*, 2016)

Pada proses *score*, zxcvbn akan melakukan sebuah perhitungan yang didasari pada proses *match* lalu mengembalikan sebuah nilai *integer* yang memiliki kategori tertentu seperti pada Tabel 2.2 (Dropbox, 2016).

Tabel 2.2 Tabel Zxcvbn *Score*
(Sumber : *zxcvbn: Low-Budget Password Strength Estimation*, 2016)

Nilai	Kategori
0	*Too Guessable*
1	*Very Guessable*
2	*Somewhat Guessable*
3	*Safely Unguessable*
4	*Very Unguessable*

Pada proses *search* dilakukan proses estimasi waktu yang dibutuhkan oleh penyerang untuk menebak sebuah *password* dengan asumsi bahwa penyerang sudah mengetahui struktur dari sebuah *password*. Proses *search* ini didasari pada proses *match* yang dilakukan sebelumnya (Wheeler, 2016).

UNIVERSITAS MULTIMEDIA NUSANTARA

2.7 System Hacking

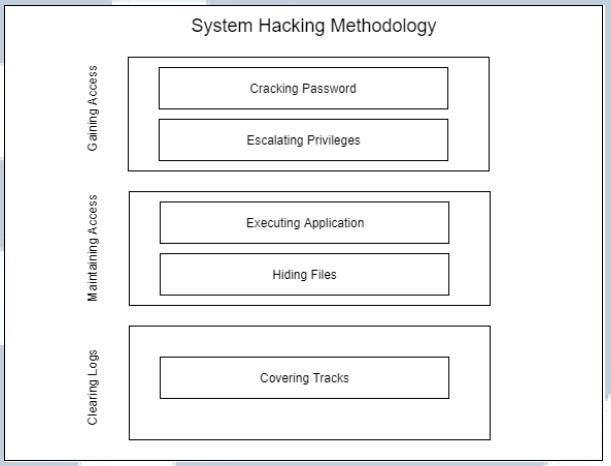
System hacking merupakan sebuah aktivitas yang dilakukan oleh penyerang untuk menguasai sebuah sistem. Tiga langkah dasar dalam melakukan kegiatan *system hacking* adalah *gaining access*, *maintaining access*, dan *clearing logs* seperti pada Gambar 2.4. Pada tahap *gaining access*, penyerang melakukan aktivitas dengan tujuan untuk mendapatkan akses terhadap sebuah komputer dan mendapatkan hak akses tertinggi di komputer tersebut agar penyerang dapat melakukan segala kegiatan yang berhubungan dengan komputer tersebut. Tahap *gaining access* dibagi menjadi dua bagian yaitu *cracking password* dan *escalating privileges*. *Cracking password* merupakan sebuah kegiatan untuk melakukan *recover password* yang dimanfaatkan oleh penyerang untuk mendapatkan akses yang tidak terotorisasi dan dilanjutkan oleh *escalating privileges* untuk menjadi *admin* di komputer tersebut.

Pada tahap *maintaining access*, penyerang akan melakukan aktivitas dengan tujuan untuk mempertahankan akses terhadap komputer tersebut. Pada umumnya tahap *maintaining access* dibagi menjadi dua bagian yaitu *executing application* dan *hiding files*. *Executing application* merupakan aktivitas utama yang dilakukan oleh penyerang untuk memenuhi tujuan dari penyerangan terhadap sebuah komputer. Proses *executing application* dapat dilakukan dengan bantuan *malware* seperti *Trojan*, *spyware*, *backdoor*, atau *keylogger*.

Hiding files merupakan aktivitas yang dilakukan oleh penyerang untuk menyembunyikan aktivitas jahat yang disebabkan oleh penyerang dan dapat dilakukan dengan bantuan *rootkit* dan *steganography*. Pada tahap terakhir yaitu *covering tracks*, penyerang akan berusaha untuk menghapus seluruh jejak atau

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

bukti bahwa telah terjadi sebuah penyerangan di komputer tersebut. Hal ini dilakukan agar korban tidak menyadari bahwa telah terjadi sebuah penyerangan terhadap komputer yang korban miliki. Proses *covering tracks* dapat dilakukan dengan menghapus *file* yang berhubungan dengan penyerangan dan membersihkan *log file* (EC-Council, 2016).



Gambar 2.4 *System Hacking Methodology*
(Sumber : CEHv9 Module 05 System Hacking, 2016)

UNIVERSITAS MULTIMEDIA NUSANTARA