BAB II

LANDASAN TEORI

2.1 Malware

Malware adalah perangkat lunak komputer yang dimaksudkan untuk merusak sistem operasi host atau mencuri data sensitif dari pengguna, organisasi atau perusahaan. Malware merupakan kode jahat yang menyebar melalui jaringan dan merupakan ancaman utama terhadap keamanan informasi dalam sistem komputer. (Aru Okereke Eze, 2018). Malware dapat menginfeksi sistem dengan berbagai cara seperti menipu pengguna membuka file yang terdapat malware atau memikat pengguna untuk mengunjungi situs yang menyebarkan malware (Nepal & Jang-Jaccard, 2014). Malware biasanya digunakan untuk mencuri informasi yang dapat segera dimonetisasi, seperti kredensial masuk, kartu kredit dan nomor rekening bank, dan kekayaan intelektual seperti perangkat lunak komputer, algoritma keuangan, dan perdagangan (Aru Okereke Eze, 2018).

2.2 Digispark

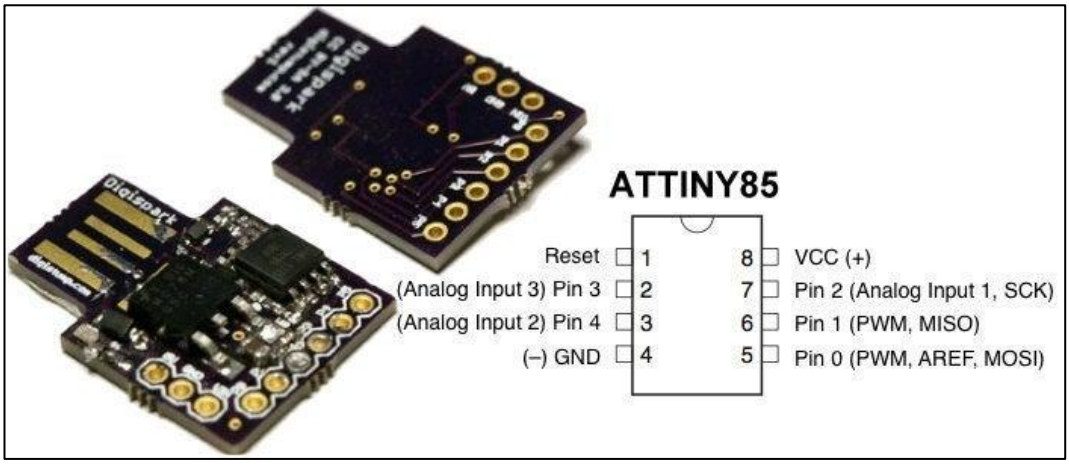
2.2.1 Infrastruktur Digispark

Digispark merupakan papan pengembangan mikrokontroler berbasis Attiny85 mirip dengan garis arduino, hanya sedikit lebih murah dan lebih kecil. Dengan sejumlah besar perisai untuk memperluas fungsionalitasnya dan kemampuan untuk menggunakan IDE Arduino yang akrab, Digispark merpupakan

pilihan yang baik untuk beralih ke elektronik, atau cocok ketika sebuah arduino terlalu besar atau terlalu banyak (Digispark USB Development Board, 2015).

Berikut merupakan spesifikasi dari Digispark.

1. Support untuk Arduino IDE 1.0+ (OSX/Win/Linux)
2. Daya melalui USB atau Sumber Eksternal - 5v atau 7-35v
3. On-board 500ma 5V Regulator
4. Built-in USB
5. 6 I/O Pins
6. 8k Flash Memory
7. I2C and SPI
8. PWM on 3 pins
9. ADC on 4 pins
10. Power LED and Test/Status LED



Gambar 2.1 Komponen Digispark
(Sumber : Digispark USB Development Board, 2015)

2.2.2 Bahasa yang digunakan Digispark

Digispark ditenagai dengan Atmel Attuny85 MCU dan memiliki library khusus untuk Digispark sendiri, salah satu dari library tersebut adalah DigiKeyboard.h. Perintah-perintah yang perlu diketahui sebagai berikut.

1. DigiKeyboard.sendKeyStroke() : digunakan untuk menekan keys ataupun modifiers (enter, windows key, shift, dan lain lain).
2. DigiKeyboard.delay() : digunakan untuk menunda aktivitas dalam kurun waktu milisecond.
3. DigiKeyboard.print("") : digunakan untuk menuliskan sebuah kalimat ataupun kata.

2.3 Firefox Lockwise Password Manager

Firefox Lockwise Password manager merupakan fitur yang hadir pada browser Mozilla Firefox yang digunakan untuk membantu *user* dengan men-*generate* dan me-*manage passwords* untuk alasan keamanan langsung pada browser itu sendiri. *User* dapat mengingat, melihat, edit dan menghapus *password* yang tersimpan (New password security features come to Firefox with Lockwise, 2019).

2.4 Password Stealing Attack

Password Stealing attack merupakan sebuah teknik yang dimanfaatkan oleh penyerang untuk mendapatkan *password* dari korban untuk mendapatkan

akses ke akun korban tersebut. *Password stealing attack* dibagi menjadi 3 cara sebagai berikut (Palanivel & Vankadesh, 2015).

1. *Password stealing program attack*

   Password stealing program attack merupakan sebuah teknik penyerangan dimana program yang dibuat oleh penyerang dimanfaatkan untuk mengambil *username* maupun *password* yang disimpan oleh korban.

2. *Phishing attack*

   Phising adalah suatu metode untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target.

3. *Shoulder Surfing attack*

   Shoulder surfing attack adalah salah satu metode pengamatan langsung, yang digunakan oleh peretas guna mendapatkan informasi tertentu, yang biasanya dilakukan paling efektif di tempat-tempat keramaian.

2.5 Zxcvbn Password Strength Estimation

Password strength estimation merupakan sebuah teknik untuk melakukan pengukuran kekuatan terhadap sebuah password yang diukur dari nilai entropi. Zxcvbn merupakan *library* yang terkenal dan sudah digunakan oleh Dropbox untuk melakukan pengecekan *password* pada saat proses sign up. Zxcvbn mengukur entropi *password* melalui 3 tahap sebagai berikut.

1. Match

   Dengan mencocokkan bagian dari *password* degan pola seperti kata-kata, urutan, tanggal, dan lain-lain.

2. Score

Dengan setiap pola *match* akan memengaruhi perhitungan entropi.

3. Search

Mencari urutan non-overlapping termudah.

Contoh: rumahkita akan dianalisis sebagai dua kata rumah dan kita.

Contoh proses pattern matching terhadap beberapa aspek sebagai berikut seperti pada Tabel 2.1 (Wheeler, 2016).

Tabel 2.1 *zxcvbn Pattern Matching*
(Sumber : zxcvbn*: Low-Budget Password Strength Estimation,2016*)

Pattern	**Examples**
Token	logitech 10giT3CH ain't parliamentarian 1232323q
Reversed	DrowssaP
Sequence	123 2468 jklm ywusq
Repeat	zzz ababab 10giT3CH10giT3CH
Keyboard	qwertyuio qAzxcde3 diueoa
Date	7/8/1947 8.7.47 781947 4778 7-21-2011 72111 11.7.21
Bruteforce	x$JQhMzt

1. Token

Pencocokan substring dari *password* terhadap sebuah dictionary.

2. Reversed

Mencari *password* yang dibalik terhadap sebuah dictionary.

3. Sequence

Pencocokan urutan dimana setiap karakter adalah urutan unicode yang ada dalam sebuah *password*.

4. Repeat

   Mencari *block* dari satu karakter atau lebih yang mengulang dalam sebuah *password*.

5. Keyboard

   Mencari rangkaian karakter yang bersebelahan pada keyboard.

6. Date

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

7. Bruteforce

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

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.

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

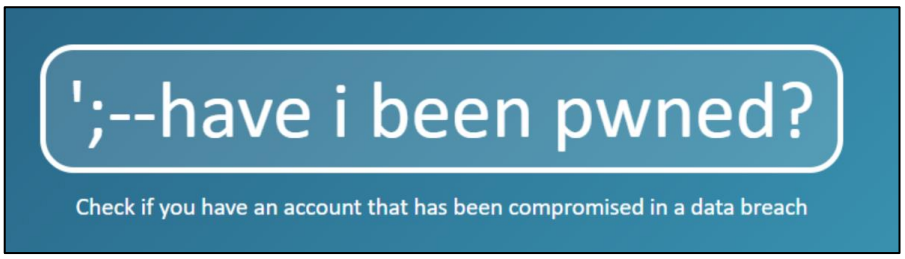
Nilai	Kategori
0	*Too Guessable*
1	*Very Guessable*
2	*Somewhat Guessable*
3	*Safely Unguessable*
4	*Very Unguessable*

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).

2.6 Have I been pwned

Haveibeenpwned merupakan situs yang dibuat karena adanya kebocoran data akun pelanggan yang sangat besar. Layanan *Haveibeenpwned* memberikan sumber daya gratis bagi siapa saja ingin dengan cepat menilai apakah seseorang berisiko karena akun daring dia telah dikompromikan atau "ditodong" dalam kebocoran data (Hunt, 2013). Sejak Haveibeenpwned diluncurkan, tujuan utamanya adalah menambahkan databreach baru secapat cepatnya setelah dibocorkan ke publik. Situs ini telah banyak dipuji sebagai sumber daya berharga bagi pengguna internet yang ingin melindungi keamanan privasi user (There's an easy way to see whether you've been affected by the Ashley Madison leak and previous massive hacks, 2015).



Gambar 2.2 Logo haveibeenpwned
(Sumber : haveibeenpwned.com)

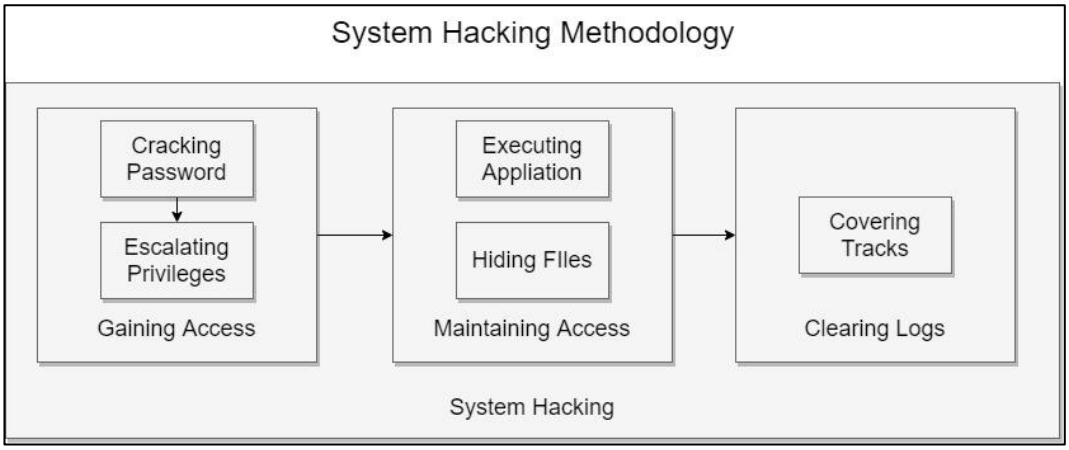
2.7 System Hacking

System hacking merupakan sebuah aktivitas yang dilakukan oleh penyerang untuk menguasai sebuah sistem. Tiga langkah utama dalam melakukan kegiatan *system hacking* adalah *gaining access, maintaining access,* dan *clearing logs* seperti pada Gambar 2.3. Pada tahap *gaining access*, penyerang melakukanaktivitas 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 daripenyerangan 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 bukti bahwa telah terjadi sebuah penyerangan di komputer tersebut. Hal ini dilakukan agar korban tidak menyadari bahwa telah terjadi sebuah penyerangan terhadap komputer yang koban miliki. Proses covering tracks dilakukan dengan menghapus file yang berhubungan dengan penyerangan dan membersihkan logfile (EC-Council, 2018).



Gambar 2.3 *System Hacking Methodology*
(Sumber : CEHv10 Chapter 06 System Hacking, 2018)