# Bab II Kajian Teori

## II.1 *Microcontroller*

*Microcontroller* (pengendali mikro) adalah sistem komputer dalam sebuah *chip*, perangkat ini dikenal juga dengan sebutan komputer chip tunggal. Disebut mikro karena ukurannya yang kecil dan *controller* karena kemampuannya untuk mengatur objek dan proses. *Microcontroller* bersifat *dedicated* untuk melakukan tugas yang ditentukan dan menjalankan aplikasi tunggal. Produk yang dikontrol secara otomatis seperti, *remote control*, perkakas listrik, mainan, serta perangkat perkantoran seperti mesin fotokopi, *printer*, dan mesin faks diprogram menggunakan *Microcontroller* (Hussain, Hammad, Hafeez, & Zainab, 2016).

## II.2 Arduino

Arduino adalah *Microcontroller* yang bersifat *open source* sehingga dapat dengan mudah diprogram, dihapus dan diprogram ulang kapan saja. Pertama kali diperkenalkan pada tahun 2005, platform Arduino dirancang untuk memberikan kemudahan bagi siapapun untuk membuat perangkat yang berinteraksi dengan lingkungannya menggunakan sensor dan aktuator (alat kontrol mekanis). Arduino merupakan *platform* komputasi yang digunakan untuk membangun program perangkat elektronik dengan bertindak sebagai komputer *mini* seperti *microcontroller* lainnya dengan mengubah *input* menjadi *output* untuk berbagai perangkat elektronik (Louis, 2016).

## II.3 Arduino *Intergated Development Environment* (IDE)

Arduino IDE merupakan *software* resmi yang dikenalkan oleh Arduino.cc yang digunakan untuk *editing*, *compiling*, dan *uploading* kode-kode pada perangkat Arduino. Hampir seluruh modul Arduino kompatibel dengan *software open source* ini. Arduino IDE tersedia untuk sistem operasi seperti MAC, Windows, dan Linux. Terdapat dua bagian dasar pada IDE ini yaitu *Editor* dan *Compiler* dan mendukung bahasa pemrograman C dan C++ (Fezari & Dahoud, 2018).

## II.4 *Password Attack*

Seiring dengan berkembang pesatnya jaringan sosial dan manajemen akun pada teknologi internet, otentikasi pengguna menjadi semakin penting untuk melindungi data pengguna. Otentikasi *password* adalah salah satu metode yang banyak digunakan untuk menjaga keamanan dari penyusup. Dalam skema otentikasi *password*, ID pengguna menentukan bahwa pengguna tersebut memiliki wewenang untuk mengakses sistem dan hak istimewa lainnya. Selain itu ID juga digunakan dalam proses *login* yang disertai dengan *password* untuk kemudian dicocokkan dengan *database* akun sebelum otorisasi diberikan kepada pengguna yang bersangkutan (Han, Wong, & Chao, 2014).

Hampir seluruh *browser* populer seperti Google Chrome, Mozilla Firefox, Safari, dan Microsoft Edge memiliki fitur *browser-based password manager* (BPM) yang dapat dimanfaatkan oleh pengguna untuk menyimpan otentikasi *password* pada suatu *website* agar tidak perlu untuk melakukan otentikasi setiap kali mengakses *website* tersebut. Namun sangat disayangkan seluruh BPM *default* pada masing-masing *browser* memiliki celah keamanan yang cukup berbahaya sehingga sangat memungkinkan untuk diretas dengan berbagai metode seperti *brute force*, USB *attack*, dan lain sebagainya (Zhao & Yue, 2013).

## II.5 Nirsoft.net

Nirsoft.net merupakan sebuah website yang menyediakan *tools* gratis yang berkaitan dengan teknologi informasi, didirikan oleh seorang *developer* yang memiliki pengetahuan mendalam pada C++, framework .NET, windows API, dan *reverse engineering* bernama Nir Sofer pada tahun 2001. Website ini memberikan kemudahan dalam dunia teknologi informasi dengan *tools* yang disediakan seperti, *password recovery*, jaringan, alamat IP, Windows *registry*, dan lain sebagainya (Sofer, 2008).

Pada penelitian ini penulis menggunakan dua buah *tools* yang disediakan oleh nirsoft.net untuk mengambil password yang disimpan pada *browser* Google Chrome dan Mozilla Firefox, yaitu ChromePass.exe dan PasswordFox.exe. kedua *tools* ini akan dijalankan pada komputer target menggunakan USB yang telah

diprogram sebelumnya sehingga dapat mengambil data password untuk kemudian dikirimkan kepada penulis melalui *email*.

## II.6 Microsoft Powershell

Microsoft Powershell adalah *command-line shells* dan bahasa *script* yang secara *default* terinstall pada system operasi Windows. Berdasarkan Microsoft .NET *framework*, termasuk didalam powershell adalah antarmuka yang memungkinkan *programmer* untuk mengakses layanan sistem operasi. Powershell dapat dikonfigurasi oleh *administrator* untuk membatasi akses dan mengurangi kerentanan pada sistem operasi (Hendler, Kels, & Rubin, 2018).

Powershell dibuat berdasarkan kerangka .NET *framework* untuk mengimplementasikan berbagai mancam operasi serta dapat menghasilkan output tidak hanya dalam bentuk text tapi dapat juga berdasarkan .net *object* yang menyebabkan powershell kaya akan *object* dan fungsionalitas. Windows menyediakan wadah untuk menulis dan menguji *script* yang sedang dikerjakan, wadah tersebut adalah Powershell *Integrated Scripting Environtment* (ISE) dan akan menghasilkan Powershell *script*. Ekstensi dari Powershell *script* tersebut adalah .ps1 (Alfarisi, 2017).

## II.7 Sistem Operasi

Sistem operasi merupakan perangkat lunak yang mengelola perangkat keras komputer, sistem ini menyediakan basis untuk program aplikasi dan sebagai penengah antara pengguna komputer dan perangkat keras komputer. Sistem operasi dapat mengatur waktu kerja, pengecekan kesalahan, mengelola input dan output, penyimpanan, komplikasi serta pengolahan data. Secara umum, dapat disimpulkan bahwa sistem operasi merupakan perangkat lunak lapisan pertama pada memori komputer pada saat komputer dinyalakan atau *booting* yang bertugas mengelola sumber daya perangkat keras komputer dan menyediakan layanan untuk aplikasi lainnya (Silberschatz, Gagne, & Galvin, 2018).

## II.8 *Universal Serial Bus* (USB)

Merupakan antarmuka *plug and play* yang memungkinkan komputer untuk berkomunikasi dengan perangkat periferal dan lainnya. Dengan koneksi ini,

komputer dapat mengirim atau mengambil data dari perangkat. Saat ini USB menjadi standar industri yang dikembangkan untuk koneksi periferal elektronik seperti *keyboard*, *modem*, dan lainnya (Computer Hope, 2019). Standar ini dikembangkan untuk mengganti koneksi yang berukuran lebih besar dan lebih lambat seperti port serial dan paralel. Tujuan dikembangkan standar ini adalah untuk mengembangkan antarmuka tunggal yang dapat digunakan di beberapa perangkat dan menghilangkan konektor yang berbeda beda saat ini.

Implementasi USB dapat diaplikasikan menjadi USB *Mass Storage* atau *Flash Disk* yang merupakan suatu perangkat penyimpanan data berbasis *flash memory* yang terintegrasi dengan *interface Universal Serial Bus* (USB). USB *Mass Storage* bersifat *removable dan rewritable* (Arisantoso, Sanwasih, & Pahlevi, 2017). Secara fisik, memiliki ukuran kecil dengan daya tahan yang lama.

### II.9 USB *Rubber Ducky*

USB *Rubber Ducky* merupakan perangkat untuk melakukan percobaan penetrasi atau penyerangan. Saat perangkat ini dihubungkan ke komputer, perangkat akan dianggap oleh laptop atau komputer sebagai *keyboard* USB sehingga memungkinkan untuk menyuntikan script berbahaya. Adapun bahasa yang digunakan adalah *Ducky script* (Cannols & Ghafarian, 2017).

Bahasa *Ducky script* memiliki beberapa syntax yang ditulis dalam huruf kapital, hampir seluruh perintah pada bahasa ini digunakan untuk melakukan kombinasi ketikan *keyboard*, sedangkan perintah lainnya digunakan untuk memberikan jeda. Berikut adalah perintah-perintah pada *Ducky script*.

a. DELAY

   Perintah ini digunakan untuk menciptakan waktu jeda antara perintah sekuensial yang membutuhkan waktu untuk mengambil data pada komputer target untuk diproses. Waktu DELAY ditentukan dalam satuan milisekon dari 1 hingga 10000.

   Contoh: DELAY 500

b. DEFAULT DELAY atau DEFAULTDELAY

   Perintah ini digunakan untuk menentukan berapa lama (milisekon) untuk waktu jeda di antara setiap perintah berikutnya. DEFAULT_DELAY harus

berada di awal Ducky script dan berifat opsional. Perintah ini akan lebih berguna saat digunakan saat melakukan debugging.

Contoh: DEFAULT_DELAY 100

c. REM

Perintah ini tidak akan diproses karena sifat nya yang hanya sebagai komentar.

Contoh: REM This part is comment

d. STRING

Perintah ini dapat menerima satu atau banyak karakter dengan format string.

Contoh: STRING notepad.exe

e. GUI atau WINDOWS

Perintah ini dapat disebut sebagai Super-key, untuk menekan tombol windows pada *keyboard*

Contoh: GUI r

f. MENU atau APP

Perintah ini menyerupai perintah SHIFT + F10 pada sistem operasi Windows yang menghasilkan menu seperti klik kanan.

g. SHIFT

Perintah ini digunakan ketika ingin melakukan navigasi untuk memilih teks diantara fungsi fungsi lainnya.

Contoh : SHIFT DELETE, HOME, INSERT, PAGEUP, PAGEDOWN, WINDOWS, GUI, UPARROW, DOWNARROW, LEFTARROW, RIGHTARROW, TAB.

h. CTRL atau CONTROL

Perintah ini menyerupai tombol CTRL pada sistem operasi windows.
Contoh : CONTROL/CTRL BREAK, PAUSE, F1…F12, ESCAPE, ESC.

i. ALT

Perintah ini berperan banyak dalam operasi otomasi. Perintah ini menyerupai perintah CONTROL.

Contoh : ALT END, ESC, ESCAPE, F1…F12, Single Char, SPACE, TAB.

j. Tambahan

REPEAT, BREAK or PAUSE, CAPSLOCK, DELETE, END, ESC or ESCAPE, HOME, INSERT, NUMLOCK, PRINTSCREEN, SPACE, PAGEUP, PAGEDOWN.

## II.10 Perbandingan dengan penelitian sebelumnya

Tabel II- 1 Perbandingan penelitian sebelumnya

| No | Nama Penulis | Judul | Tahun | Latar Belakang |
|---|---|---|---|---|
| 1 | Benjamin Cannols, Ahmad Ghafarian | *Hacking Experiment by Using USB Rubber Ducky Scripting* | 2017 | Pentingnya eksperimen dan penelitian yang dilakukan pada jurnal ini adalah agar pembaca mengetahui bahwa hampir seluruh perangkat baik komputer, laptop, tablet, *smartphone* hari ini tidak terlepas dari masukkan dari *keyboard*. Disisi lain setiap standar USB disebut dengan Human Interface Device (HID) yang dapat diartikan bahwa seluruh perangkat USB secara otomatis terdeteksi sebagai *keyboard* HID dan diterima oleh seluruh sistem operasi seperti Windows, Mac OS, Linux, dan Android. Bisa disimpulkan bahwa komputer, laptop, dan perangkat lainnya tidak bisa mendeteksi USB sebagai perangkat yang berbahaya sehingga melakukan *hacking* menggunakan USB bisa sangat mudah dilakukan apabila tidak ada kesadaran dari pemilik perangkat untuk meningkatkan keamanan perangkat itu sendiri. |
| 2 | Myung-gu Kang | *USBWall: A Novel Security Mechanism to Protect Against Maliciously* | 2015 | Penelitian ini diawali dengan keresahan yang dirasakan penulis terkait bahaya dari penggunaan *keylogger* USB, sehingga penulis membuat sebuah metode yang disebut USBWall dengan tujuan mencegah dari serangan tersebut. |

| | | | | |
|---|---|---|---|---|
| | | *Reprogrammed USB Devices* | | |
| 3 | Aufa Tesar Ramadhan | Implementasi Dan Analisis USB *Attack* Berbasis PowerShell Menggunakan P4wnp1 Pada *Personal Computer* | 2019 | Keamanan *password* yang tersimpan pada *browser* Internet Explorer dan Microsoft Edge diuji dengan melakukan penetrasi ke sistem operasi Windows 8.1 dan Windows 10 melalui PowerShell menggunakan P4wnp1. Skenario pengujian pengambilan data dilakukan sebanyak enam kali dengan hasil seluruh percobaan berhasil dijalankan. |