**IMPLEMENTASI DAN ANALISIS**

**KELEMAHAN PADA *BROWSER* DENGAN MENGGUNAKAN SERANGAN USB *RUBBER DUCKY* BERBASIS POWERSHELL**

**Oleh**

ABDUL AZIES MUSLIM

NIM : 1202164284

****

**PROGRAM STUDI SISTEM INFORMASI**

**FAKULTAS REKAYASA INDUSTRI**

**UNIVERSITAS TELKOM**

**2020**

# LEMBAR PENGESAHAN

Tugas Akhir dengan judul:

**ANALISIS KELEMAHAN PADA *BROWSER* DENGAN MENGGUNAKAN SERANGAN USB *RUBBER DUCKY* BERBASIS POWERSHELL**

Telah disetujui dan disahkan pada Sidang Tugas Akhir

Program Studi Strata 1 Sistem Informasi

Fakultas Rekayasa Industri Universitas Telkom

**Oleh:**

**ABDUL AZIES MUSLIM**

**1202164284**

Bandung, 09 June 2020

Disetujui oleh,

# LEMBAR PERNYATAAN ORISINALITAS

Pembimbing,

Ahmad Almaarif, S.Kom., M.T.

NIP. 17890112



Nama : Abdul Azies Muslim

NIM : 1202164284

Alamat : Pondok Mega Priangga Sukabirus

No. Tlp : 082213124191

Email : abdulazieS55@gmail.com

Name: Alifahrin Akhmad Thayyib

NIM: 1102100139

Address: Cigebar No.22 RT.02 RW.04 Desa Bojongsari Kec Bojongsoang Kab Bandung

Phone: 089660104986

Email: alifahrin.akhmad@gmail.com

Menyatakan bahwa Tugas Akhir ini merupakan karya orisinal saya sendiri. Atas pernyataan ini, saya siap menanggung risiko atau sanksi yang dijatuhkan kepada saya apabila kemudian ditemukan adanya pelanggaran terhadap kejujuran akademik atau etika keilmuan dalam karya ini, atau ditemukan bukti yang menunjukkan ketidakaslian karya ini.

Bandung, 09 Juni 2020

Abdul Azies Muslim

ABSTRAK

**IMPLEMENTASI DAN ANALISIS KELEMAHAN PADA BROWSER DENGAN MENGGUNAKAN SERANGAN USB RUBBER DUCKY BERBASIS POWERSHELL**

Oleh

**ABDUL AZIES MUSLIM**

**1202164284**

Seiring dengan perkembangan sistem operasi Windows, aplikasi *bowser* juga berkembang pesat. Aplikasi *browser* yang paling banyak digunakan di dunia saat ini adalah Google Chrome. *Browser* ini memiliki fitur penyimpanan *password* sehingga memudahkan pengguna agar tidak perlu selalu melakukan *login* pada *website* tertentu yang diinginkan, namun pada kenyataannya menyimpan *password* pada *browser* cukup berbahaya karena data-data yang tersimpan tidak terenkripsi dan peretas bisa mendapatkannya dengan serangan *brute force*, selain itu *password* yang tersimpan juga mudah dibaca melalui *malware.* *BadUSB* merupakan perangkat USB yang dimanipulasi oleh penyerang, agar saat terdeteksi oleh komputer target perangkat ini akan dikenali sebagai perangkat antar muka USB biasa, seperti keyboard komputer. Terdapat suatu cara untuk mendapatkan *password* pada *browser* dengan menggunakan metode *Rubber Ducky* untuk melakukan *dumping password* dan menjalankan Powershell *script* menggunakan perangkat Arduino Leonardo yang dihubungkan ke perangkat komputer. Hasil yang didapatkan dari penelitian ini adalah *password* pada *browser* berbasis Chromium didapatkan saat *flashdisk* dihubungkan lalu dikirimkan melalui email peretas.

Kata Kunci: USB *Attack*, Powershell, Arduino Leonardo*, Rubber Ducky*.

ABSTRACT

**IMPLEMENTATION AND WEAKNESS ANALYSIS OF BROWSER USING A USB POWERSHELL-BASED RUBBER DUCKY ATTACK**

By

**ABDUL AZIES MUSLIM**

**1202164284**

Along with the development of the Windows operating system, bowser applications are also developing rapidly. The most widely used browser application in the world today is Google Chrome. This browser has a password storage feature that makes it easy for users to not have to always log on to a particular website that is desired, but in fact storing passwords in the browser is quite dangerous because the stored data is not encrypted and hackers can get it with brute force attacks, besides that the password stored ones are also easy to read through malware. BadUSB is a USB device that is manipulated by an attacker, so that when detected by the target computer this device will be recognized as an ordinary USB interface device, such as a computer keyboard. There is a way to get a password on the browser by using the Rubber Ducky method to dump password and run a Powershell script using a Arduino Leonardo device that is connected to a computer device. The results obtained from this study are passwords in the Chromium-based browser obtained when the flash is connected and sent to hacker’s email.

Keyword: USB Attack, Powershell, Arduino Leonardo, Rubber Ducky.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul “Analisis Kelemahan Pada *Browser* dengan Menggunakan Serangan USB *Rubber Ducky* Berbasis PowerShell”.

Dalam penyusunan tugas akhir ini, penulis mendapat dukungan dari beberapa pihak, sehingga tugas akhir dapat diselesaikan dengan baik. Maka dari itu, penulis mengucapkan terima kasih kepada:

1. Kedua orang tua, Tjahjo Sudjadi dan Hilma Sari Indah beserta seluruh keluarga yang selalu memberikan dukungan dan doa kepada penulis.
2. Bapak Ahmad Almaarif, S. Kom., M.T. yang telah bersedia memberikan bimbingan bimbingan, saran, dan kritik dalam penyusunan Tugas Akhir.
3. Bapak Avon Budiyono, S.T., M.T. yang telah bersedia memberikan bimbingan bimbingan, saran, dan kritik dalam penyusunan Tugas Akhir.

Terima kasih semua atas dukungan dan doa selama ini. Penulis menyadari bahwa dalam penulisan Tugas Akhir ini tentu masih terdapat kekurangan karena terbatasnya pengetahuan dan kepustakaan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun untuk kesempurnaan karya tulis ini. Akhirnya, penulis berharap semoga laporan ini dapat bermanfaat bagi semua pihak yang menggunakannya.

Bandung, 05 Desember 2019

Abdul Azies Muslim

DAFTAR ISI

[LEMBAR PENGESAHAN 1](#_Toc37938732)

[LEMBAR PERNYATAAN ORISINALITAS 1](#_Toc37938733)

[ABSTRAK 3](#_Toc37938734)

[ABSTRACT 4](#_Toc37938735)

[KATA PENGANTAR 5](#_Toc37938736)

[DAFTAR ISI 6](#_Toc37938737)

[DAFTAR GAMBAR DAN ILUSTRASI 8](#_Toc37938738)

[DAFTAR TABEL 9](#_Toc37938739)

[Bab I Pendahuluan 10](#_Toc37938740)

[I.1 Latar Belakang 10](#_Toc37938741)

[I.2 Rumusan Masalah 11](#_Toc37938742)

[I.3 Tujuan Penelitian 11](#_Toc37938743)

[I.4 Manfaat Penelitian 12](#_Toc37938744)

[I.5 Batasan Masalah 12](#_Toc37938745)

[I.6 Sistematika Penulisan 12](#_Toc37938746)

[Bab II Kajian Teori 14](#_Toc37938747)

[II.1 Digispark *Board* 14](#_Toc37938748)

[II.2 *Secure Shell* (SSH) 14](#_Toc37938749)

[II.3 Microsoft Powershell 14](#_Toc37938750)

[II.4 Sistem Operasi 15](#_Toc37938751)

[II.5 *Universal Serial Bus* (USB) 15](#_Toc37938752)

[II.6 Arduino Intergated Development Environment (IDE) 16](#_Toc37938753)

[II.7 USB Rubber Ducky 16](#_Toc37938754)

[II.8 *Password Attack* 18](#_Toc37938755)

[II.9 Perbandingan dengan penelitian sebelumnya 18](#_Toc37938756)

[Bab III Metodologi Penelitian 20](#_Toc37938757)

[III.1 Metode Konseptual 20](#_Toc37938758)

[III.2 Sistematika Penelitian 20](#_Toc37938759)

[III.2.1 Inisiasi 22](#_Toc37938760)

[III.2.2 Hipotesis 22](#_Toc37938761)

[III.2.3 Simulasi 22](#_Toc37938762)

[III.2.4 Akhir 22](#_Toc37938763)

[III.2.5 Pelaporan 23](#_Toc37938764)

[Bab IV PERANCANGAN SISTEM DAN SKENARIO PENYERANGAN 24](#_Toc37938765)

[IV.1 Perancangan Sistem 24](#_Toc37938766)

[IV.2 Mekanisme Penyerangan 24](#_Toc37938767)

[IV.3 Pengembangan Sistem 24](#_Toc37938768)

[DAFTAR PUSTAKA 25](#_Toc37938769)

DAFTAR GAMBAR DAN ILUSTRASI

[Gambar III-1 Metode Konseptual 20](#_Toc26430693)

[Gambar III- 2Sistematika Penelitian 21](#_Toc26430694)

# DAFTAR TABEL

[Tabel II- 1 Perbandingan penelitian sebelumnya 18](#_Toc26430686)

# Pendahuluan

## Latar Belakang

Pada saat ini, penggunaan *personal computer* (PC) maupun laptop dalam kegiatan sehari-hari masih banyak ditemukan baik untuk belajar, bekerja, atau sekedar mencari hiburan. Sejak PC pertama kali diluncurkan, terjadi perkembangan yang pesat baik dari sisi perangkat keras maupun perangkat lunak hingga hari ini. Salah satu komponen terpenting pada sebuah PC adalah Sistem operasi sebagai perangkat lunak untuk dapat menjalankan mengeksekusi perintah dari pengguna. Sistem operasi Windows milik Microsoft menempati posisi pertama dari sisi penjualan yaitu sebanyak 87.36% sampai pada Oktober 2019 (Net MarketShare, 2019).

Seiring dengan perkembangan sistem operasi Windows, aplikasi *bowser* juga berkembang pesat. Berbagai aplikasi *browser* bersaing untuk mendapatkan pengguna sebanyak-banyaknya melaui sistem-sistem operasi yang ada. Aplikasi *browser* yang paling banyak digunakan di dunia saat ini adalah Google Chrome dengan pangsa pasar sebesar 59.2%. Posisi Google Chrome saat ini sangatlah kuat dan hampir tidak bisa disaingi karena posisi kedua yang diduduki oleh Safari memiliki pangsa pasar sebesar 14,6% (W3Counter, 2019). Salah satu fitur yang dimiliki oleh *browser* adalah menyimpan password pada *website* tertentu sehingga pengguna tidak perlu melakukan login setiap kali membuka *website* tersebut, fitur ini sangat bermanfaat digunakan pada *website* seperti media sosial ataupun *website* yang membutuhkan akun pengguna untuk menjalankannya. Pada kenyataannya fitur menyimpan password pada *browser* cukup berbahaya karena data-data yang tersimpan tidak terenkripsi dan peretas bisa mendapatkannya dengan serangan *brute force*, selain itu *password* yang tersimpan juga mudah dibaca melalui *malware* (Mateso, 2019).

Saat ini komputer mendukung penyimpanan berkas eksternal yang salah satunya bernama *flashdisk*, perangkat ini terhubung dengan komputer melalui Universal Serial Bus (USB) sehingga *flashdisk* dapat dibaca dan diakses pada komputer yang telah terhubung. USB *interface* sebenarnya merupakan celah yang cukup berbahaya untuk terjadinya penyerangan, bahkan di beberapa organisasi penggunaan USB *flash drive* dilarang dikarenakan sangat berpotensial untuk digunakan sebagai alat *hacking* dalam bentuk USB-*based* *attack* dengan sebutan BadUSB (Cannols & Ghafarian, 2017).

BadUSB merupakan perangkat USB yang dimanipulasi oleh penyerang, agar saat terdeteksi oleh komputer target perangkat ini akan dikenali sebagai perangkat antar muka USB biasa, seperti keyboard komputer. Bentuk serangan dari BadUSB semakin beragam pada saat ini yang meliputi USBdriveby, Evilduino, USBee, USB Killer, dan lain sebagainya.

Penelitian ini menyajikan rincian pendekatan dengan menerapkan penetrasi ke komputer dengan sistem operasi Windows menggunakan perangkat Arduino Leonardo. Mekanisme ini memungkinkan penyerang untuk terhubung dengan komputer target yang dideteksi sebagai USB (*Human Interface Device*) berupa *keyboard* kemudian mengambil *username* dan *password* yang disimpan pada *browser* dari komputer target menggunakan aplikasi yang disediakan pihak ketiga untuk kepentingan edukasi serta dijalankan melalui *Command Prompt* dan Powershell. Data yang telah diambil dari *browser* kemudian dikirimkan via *email*. Disini penulis memanfaatkan beberapa alat dan teknologi seperti Arduino Leonardo, Arduino IDE, ChromePass, dan PasswordFox.

## Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara mendapatkan password yang tersimpan pada *browser* Google Chrome dan Mozilla Firefox menggunakan serangan USB?
2. Bagaimana dampak pengambilan data *password* menggunakan serangan USB pada *browser* Google Chrome dan Mozilla Firefox?
3. Bagaimana cara untuk meminimalisir terjadinya penyerangan?

## Tujuan Penelitian

Berdasarkan rumusan masalah pada penelitian ini, tujuan yang ingin dicapai adalah sebagai berikut:

1. Dapat melakukan serangan USB untuk mendapatkan *password* yang tersimpan pada *browser* Google Chrome dan Mozilla Firefox.
2. Dapat menganalisia dampak pengambilan data *password* menggunakan serangan USB pada *browser* Google Chrome dan Mozilla Firefox.
3. Dapat memberikan rekomendasi yang digunakan untuk meminimalisir terjadinya penyerangan.

## Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan beberapa manfaat baik secara teoritis maupun praktis, yaitu:

1. Teoritis.

Secara teoritis, hasil dari penelitian ini diharapkan menjadi acuan untuk meningkatkan keamanan data pribadi yang tersimpan pada *browser*.

1. Praktis.

Secara praktis, hasil dari penelitian ini diharapkan menjadi pertimbangan bagi *browser* Google Chrome dan Mozilla Firefox dalam meningkatkan keamanan data pribadi yang tersimpan di masa depan.

## Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu:

1. Membahas tentang penyerangan menggunakan USB terhadap sistem operasi Windows 10.
2. Membahas mengenai penyerangan menggunakan *Rubber Ducky*.
3. Melakukan pengambilan *password* pada *browser* Google Chrome dan Mozilla Firefox
4. Menggunakan perangkat Arduino Leonardo.

## Sistematika Penulisan

Sistematika penulisan penelitian ini adalah sebagai berikut :

**Bab I Pendahuluan**

Bab ini meliputi latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup dan sistematika penulisan.

**Bab II Tinjauan Pustaka**

Bab ini menguraikan landasan teori yang berkaitan dengan pembahasan masalah yang akan diteliti.

**Bab III Metodologi Penelitian**

Bab ini menguraikan jenis penelitian yang akan dilakukan, sumber data yang digunakan dalam penelitian, bagaimana cara mendapatkannya dan terakhir menganalisis dari permasalahan yang ada pada penelitian.

**Bab IV Perancangan Sistem dan Skenario Penyerangan**

Bab ini menguraikan detail dari perancangan omput dan omputer penyerangan yang dilakukan.

**Bab V Pengujian Sistem dan Analisis**

Bab ini menguraikan langkah-langkah tahapan pengujuan yang terjadi pada saat penelitian. Hasil dari penelitian, analisis ataupun perancangan dari penelitian tersebut.

**Bab VI Kesimpulan dan Saran**

Bab ini menguraikan tentang kesimpulan dan saran penulis berdasarkan data yang didapatkan dari hasil penelitian.

# Kajian Teori

## Digispark *Board*

Digispark adalah *prototyping board* berbasis mikrokontroller Attiny85. Attiny85 adalah mikrokontroler 8-bit keluaran Atmel dengan frekuensi maksimum 20MHz. Dengan ukurannya yang kecil, harganya yang murah dan mudah didapatkan, Attiny85 selalu menjadi pilihan tepat untuk membuat proyek kecil dan sederhana. Kemudahan yang diberikan Digispark *board* adalah dapat menggunakan Arduino IDE (Haryanto, 2016) sehingga menjadi pilihan yang tepat untuk digunakan dalam penelitian BadUSB.

## *Secure Shell* (SSH)

*Secure Shell* (SSH) pertama kali dikembangkan oleh Tatu Yl nen di Helsinki University of Technology. SSH memberikan alternatif keamanan terhadap remote *session* tradisional dan *file* *transfer protocol* seperti telnet. *Secure Shell* (SSH) merupakan sebuah protokol jaringan yang memungkinkan terjadinya suatu pertukaran data melalui sebuah *secure channel* antar perangkat jaringan (Cahyani, 2010).

SSH juga merupakan protokol jaringan untuk pengamanan *login* dan layanan jaringan jarak jauh menggunakan arsitektur klien/server. SSH membuat *channel* komunikasi aman yang memungkinkan pengguna mengontrol sistem komputer jarak jauh seperti memonitor lalu lintas data, transfer data, log data, kegagalan data, kecepatan data, performa jaringan dan kriteria lainnya pada server SSH yang dapat dipantau melalui klien SSH (Sithara, Chandran, & Padmavathi, 2017).

## Microsoft Powershell

Microsoft Powershell adalah *command-line shells* dan omput skrip yang secara *default* terinstall pada system operasi Windows. Berdasarkan Microsoft .NET *framework*, termasuk didalam powershell adalah antarmuka yang memungkinkan *programmer* untuk mengakses layanan omput operasi. Powershell dapat dikonfigurasi oleh *administrator* untuk membatasi akses dan mengurangi kerentanan pada omput 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 skrip yang sedang dikerjakan, wadah tersebut adalah Powershell *Integrated Scripting Environtment* (ISE) dan akan menghasilkan *file* skrip Powershell. Ekstensi dari *file* skrip Powershell tersebut adalah .ps1 (Alfarisi, 2017).

## Sistem Operasi

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

## *Universal Serial Bus* (USB)

Merupakan antarmuka *plug and play* yang memungkinkan omputer untuk berkomunikasi dengan perangkat omputerl dan lainnya. Dengan koneksi ini, omputer dapat mengirim atau mengambil data dari perangkat. Saat ini USB menjadi standar omputer yang dikembangkan untuk koneksi omputerl 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 omputer. 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.

## 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).

## USB Rubber Ducky

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

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

1. DELAY

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

Contoh: DELAY 500

1. 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

1. REM

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

Contoh: REM This part is comment

1. STRING

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

Contoh: STRING notepad.exe

1. GUI atau WINDOWS

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

Contoh: GUI r

1. MENU atau APP

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

1. 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.

1. CTRL atau CONTROL

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

1. ALT

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

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

1. Tambahan

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

## *Password Attack*

Seiring dengan berkembang pesatnya jaringan omput 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 omput 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* ompute 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 yang ada pada masing-masing *browser* memiliki celah keamanan yang cukup berbahaya yaitu tidak adanya enkripsi terhadap *username* dan *password* yang disimpan sehingga sangat memungkinkan untuk diretas dengan berbagai metode seperti *brute force*, USB *attack,* dan lain sebagainya (Zhao & Yue, 2013).

## Perbandingan dengan penelitian sebelumnya

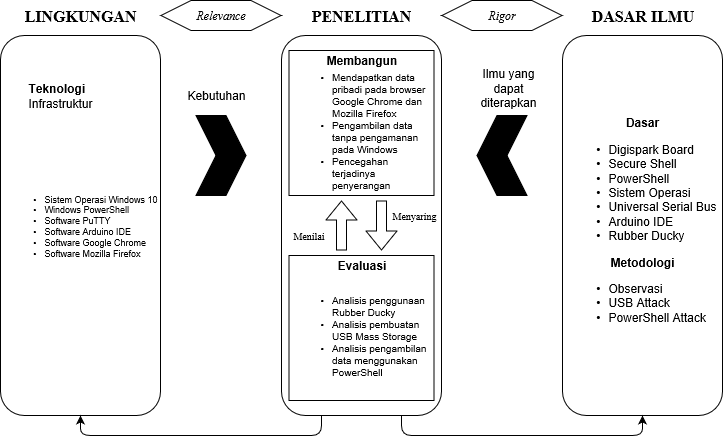
Tabel II- 1 Perbandingan penelitian sebelumnya

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 omput seluruh perangkat baik omputer, 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 omput operasi seperti Windows, Mac OS, Linux, dan Android. Bisa disimpulkan bahwa omputer, 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 Reprogrammed USB Devices | 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. |
| 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. |

# Metodologi Penelitian

## Metode Konseptual

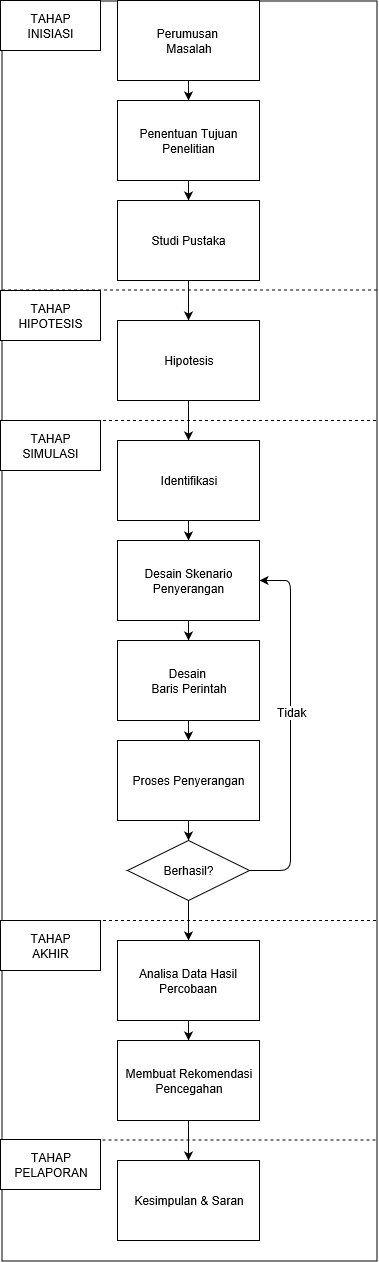
Metode Konseptual merupakan suatu gambaran logis dari suatu masalah yang digambarkan dalam rangkaian konsep berdasarkan aspek hipotesis dan teoritis. Untuk menghasilkan output yang sesuai dengan tujuan penelitian maka dibutuhkan kerangka berpikir yang bisa menjabarkan konsep dalam memecahkan masalah secara ringkas dan teratur. Diagram metode konseptual yang digunakan dapat dilihat pada Gambar III-1.



Gambar III-1 Metode Konseptual

## Sistematika Penelitian

Sistematika penelitian merupakan suatu urutan proses yang terencana dan perlu dilakukan untuk mencapai tujuan penelitian dengan baik. Sistematika penelitian yang digunakan dapat dilihat pada Gambar III-2.



Gambar III- 2Sistematika Penelitian

## Inisiasi

Pada tahap awal penelitian diawali dengan identifikasi masalah dan kemudian dilanjutkan dengan latar belakang masalah dengan mengacu kepada studi literatur. Setelah itu, didapatkan rumusan masalah yaitu mengacu kepada vulnerability yang terdapat pada sistem operasi Windows. Selanjutnya membuat batasan masalah yang digunakan agar ruang lingkup penelitian menjadi lebih fokus.

## Hipotesis

Pada tahap hipotesis, dilakukan proses perkiraan sementara dari hasil penelitian yang akan dilakukan. Pada tahap ini juga dilakukan proses penanggulangan terdahap dampak yang akan dihasilkan dari penelitian yang akan dilakukan.

## Simulasi

Pada tahap simulasi ini, dilakukan pengujian berdasarkan vulnerability yang terdapat pada *browser* Google Chrome dan Mozilla Firefox. Tahap pertama yaitu mengidentifikasi target yang ingin dilakukan penyerangan. Pada browser *browser* Google Chrome dan Mozilla Firefox memiliki celah dapat diaksesnya data username dan password tersimpan menggunakan Powershell oleh pengguna yang tidak memiliki otoritas.

Kemudian pada tahap selanjutnya yaitu perancangan skenario penyerangan yang akan dilakukan. Untuk melakukan penyerangan terhadap data username dan password tersimpan dibutuhkan skrip *payload* dan tools yang akan dijelaskan pada perancangan sistem. Setelah sudah tersusun, maka dilakukan pengujian dengan menjalankan baris perintah yang telah dibuat sebelumnya. Jika terdapat kegagalan atau kejanggalan pada saat proses penyerangan, maka dilakukan kembali proses desain hingga didapatkan hasil yang diharapkan.

## Akhir

Setelah tahap simulasi dilakukan, dilakukan proses analisis dari hasil yang didapatkan pada pengujian yang sudah dilakukan. Hasil dari proses analisis dibuat beserta rekomendasi pencegahan dari tipe serangan USB *Attack* ini.

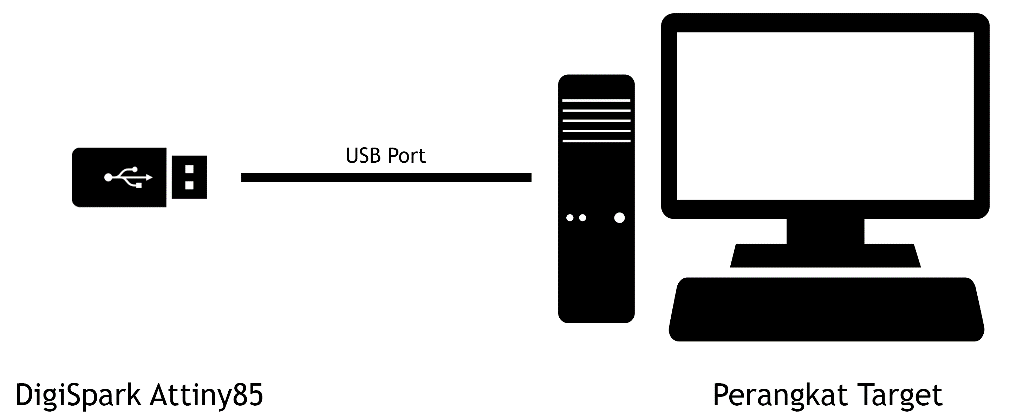
## Pelaporan

Pada tahap ini, penulis menuliskan beberapa kesimpulan dari hasil penelitian yang telah dilakukan dan memberikan beberapa saran yang berguna untuk membantu mengembangkan penelitian selanjutnya.

# PERANCANGAN SISTEM DAN SKENARIO PENYERANGAN

## Perancangan Sistem

Dalam melakukan penyerangan, dibutuhkan hardware dan software yang mendukung. Maka dari itu dilakukan identifikasi arsitektur yang terdiri dari hardware dan software untuk melakukan penyerangan. Spesifikasi hardware dan software yang digunakan dapat dilihat pada Tabel IV-1 dan Tabel IV-2.



Pada Gambar IV-1 ditampilkan ilustrasi penyerangan yang dilakukan untuk melakukan pengambilan data pada komputer target. Penyerangan diawali dengan menghubungkan perangkat Arduino *Pro Micro* Leonardo ke komputer target melalui port USB. Setelah itu DigiKeyboard akan membuat USB Rubber Ducky menjalankan baris kode yang disematkan oleh penyerang ke dalam perangkat Arduino. Hasil dari penyerangan ini akan didapatkan username dan password yang tersimpan pada browser Google Chrome serta Mozilla Firefox.

1. **Spesifikasi *Hardware***

Spesifikasi hardware yang dilakukan dalam penyerangan dapat dilihat pada table IV-1.

|  |  |  |
| --- | --- | --- |
| Komponen | Informasi | |
| Omen by HP Laptop 15-dc0xxx | *Processor* | Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz (12 CPUs), ~2.2GHz |
| *Memory* | 16GB RAM |
| *Hard Disk* | 1TB |
| *Operating System* | Windows 10 Education 64-bit (10.0, Build 17134) |
| Arduino Pro Micro | *Microcontroller* | ATmega32U4 |
| *Flash Memory* | 32 KB |
| SRAM | 2.5 KB |
| *Clock Speed* | 16MHz |

1. **Spesifikasi *Software***

Peralatan perangkat lunak dan tools yang digunakan untuk penelitian ini dapat dilihat pada table IV-2.

|  |  |  |
| --- | --- | --- |
| No | Perangkat Lunak | Fungsi |
| 1 | Vmware Workstation 15.5 PRO | Sebagai sistem operasi virtual untuk melakukan simulasi selama membuat BadUSB |
| 2 | Sistem Operasi Windows 10 | Sebagai sistem operasi yang digunakan pada komputer target penyerangan |
| 3 | Sistem Operasi Femto | Sebagai sistem operasi yang digunakan pada Digispark Attiny85 |
| 4 | Windows Powershell | Sebagai media untuk menjalankan perintah penyerangan pada komputer tujuan. |
| 5 | Google Chrome | Sebagai *browser* tujuan yang akan diambil *username* dan *password* yang tersimpan |
| 6 | Arduino IDE | Sebagai aplikasi untuk menulis kode-kode untuk menjalankan penyerangan |

## Mekanisme Penyerangan

Mekanisme pada penelitian ini terbagi dalam 3 proses utama, yaitu:

1. Menjalankan Ducky *script*

Menjalankan Rubber Ducky dari *file* Ducky *script* yang sudah dikonfigurasi untuk menjalankan fungsi menjalankan Powershell script.

1. Menjalankan Powershell *script*

Menjalankan Powershell *script* yang tersimpan untuk melakukan fungsi pengambilan data yang tersimpan dan mengirim hasil data yang berhasil didapatkan dari komputer target.

## Pengembangan Sistem

# DAFTAR PUSTAKA

Alfarisi, S. (2017, March 2). *Mengenal Powershell dan Fungsionalitasnya*. Diambil dari Netsec ID: https://netsec.id/mengenal-powershell/

Arisantoso, Sanwasih, M., & Pahlevi, M. R. (2017). Penerapan Aplikasi Pengamanan Data/File dengan Metode Enkripsi dan Dekripsi Algoritma 3DES dalam Jaringan Lokal Area. *Seminar Nasional Teknologi Informasi dan Multimedia*, 43-48.

Cahyani, I. D. (2010). SISTEM KEAMANAN ENKRIPSI SECURE SHELL (SSH) UNTUK KEAMANAN DATA.

Cannols, B., & Ghafarian, A. (2017). Hacking Experiment by Using USB Rubber Ducky Scripting. *SYSTEMICS, CYBERNETICS AND INFORMATICS*, 66-71.

Computer Hope. (2019, 11 16). *USB*. Diambil dari Computer Help: https://www.computerhope.com/jargon/u/usb.htm

EthicNinja. (2016, November 18). *USB HID for Penetration Testing*. Diambil dari github.com: https://github.com/EthicNinja/Ninjutsu-USB

Fezari, M., & Dahoud, A. A. (2018). Integrated Development Environment "IDE" For Arduino. *Researchgate*.

Han, A. L., Wong, D. F., & Chao, L. S. (2014). Advances of Password Cracking and Countermeasures in Computer Security. *arXiv: Cryptography and Security*.

Haryanto, T. (2016, January 5). *Menginstal Board Manager Digispark pada Arduino IDE*. Diambil dari Codepolitan: https://www.codepolitan.com/menginstal-board-manager-digispark-pada-arduino-ide

Hendler, D., Kels, S., & Rubin, A. (2018). Detecting Malicious PowerShell Commands using Deep Neural Networks. *Asia Conference on Computer and Communications Security*, 187-197.

Kang, M.-g. (2015). *USBWall: A Novel Security Mechanism to Protect Against Maliciously Reprogrammed USB Devices.* Lawrence, Kansas: University of Kansas.

Mateso. (2019, March 25). *The Danger of Storing Passwords via Browser*. Diambil December 5, 2019, from PasswordSafe: https://blog.passwordsafe.de/en/2019/03/25/how-dangerous-is-it-to-store-your-passwords-in-the-browser/

Net MarketShare. (2019, October). *Operating System Market Share*. Diambil dari Net MarketShare: https://netmarketshare.com/

Silberschatz, A., Gagne, G., & Galvin, P. B. (2018). *Operating System Concepts.* Hoboken, New Jersey: John Wiley & Sons.

Sithara, M., Chandran, M., & Padmavathi, G. (2017). Outlier Detection in Secure Shell Honeypot using Particle Swarm Optimization Technique. *The International Journal of Advanced Networking and Applications (IJANA)*, 3443-3450.

W3Counter. (2019, November 4). *Browser & Platform Market Share*. Diambil November 4, 2019, from W3Counter: https://www.w3counter.com/globalstats.php?year=2019&month=11

Zhao, R., & Yue, C. (2013). All Your Browser-saved Passwords Could Belong to Us: a Security Analysis and a Cloud-based New Design. *Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13)*, 333-340.