DAFTAR SINGKATAN

BAT	:	*Batch*
CMD	:	*Command prompt*
CPU	:	*Center Processing Unit*
DVD	:	*Digital Versatile Disc*
DOS	:	*Denial Of Service*
HID	:	*Human interface device*
I/O	:	*Input/Output*
IC	:	*Integrated Circuit*
IDE	:	*Integrated Development Environment*
RAM	:	*Read Access Memory*
ROM	:	*Read Only Memory*
USB	:	*Universal Serial Bus*

Bab I PENDAHULUAN

I.1 Latar Belakang

Hampir setiap jenis komputer termasuk komputer desktop, laptop, tablet, dan *smartphone* melakukan pemrosesan dan memerlukan input dari manusia melalui keyboard. Semua jenis komputer tersebut merupakan contoh dari *Human Interface Device* (HID). *Human Interface Device* (HID) adalah metode yang digunakan manusia untuk berinteraksi dengan melakukan input pada komputer (Dale Janssen, 2019). Pada umumnya, perangkat USB secara otomatis akan terdeteksi dan diterima oleh sistem operasi seperti *Windows*, *Mac OS*, dan *Linux*. *Universal Serial Bus* (USB) merupakan jenis konektor yang bertujuan untuk menghubungkan alat eksternal seperti printer, scanner, dan keyboard ke perangkat komputer. USB dibuat dengan tujuan untuk menyederhanakan koneksi antar komputer dan perangkat tambahan. (Votcamejo, 2018).

Selain sebagai perangkat pendukung proses komputer USB juga dapat digunakan sebagai alat untuk melakukan penyerangan. Hal ini menyebabkan pada beberapa organisasi, penggunaan USB flash drive sangat dibatasi. USB flash drive berpotensi besar untuk melakukan peretasan terhadap sistem yang ada di organisasi. Pada tahun 2000-an, serangan berbasis USB telah muncul yang dikenal dengan *Bad* USB (Librianty, 2018). Perangkat *Bad* USB dibuat dalam beberapa jenis perangkat. Perangkat *Bad* USB memungkinkan penyerang untuk melakukan aktivitas rahasia tanpa diketahui oleh pengguna yang sah. Permasalah pada USB tidak hanya terbatas pada flash drive yang teridentifikasi virus. Perangkat apapun yang berkomunikasi melalui USB akan rentan terhadap serangan.

Salah satu strategi praktis digunakan oleh para peretas adalah dengan memasang stik USB ke komputer. Strategi ini dapat dilakukan dengan menggunakan perangkat USB yang dideteksi oleh komputer korban sebagai *Human Interface Device* (HID). Selain itu startegi ini dapat menjalankan kode tanpa sepengetahuan atau persetujuan korban.

Salah satu contoh dari *Bad* USB adalah Rubber Ducky. Rubber Ducky adalah platform serangan injeksi *keystroke* komersial yang dirilis pada tahun 2010. Setelah

terhubung ke komputer, Rubber Ducky berperan sebagai *keyboard* dan menyuntikkan urutan *keystroke* yang dimuat. Rubber Ducky mendukung bahasa *scripting* sederhana yang memungkinkan peretas untuk membuat payload yang mampu mengubah pengaturan sistem, melakukan backdoor, mengambil data, memulai ulang *powerShell*. Rubber Ducky pada dasarnya dapat dicapai dengan akses fisik yang semuanya bersifat otomatis dan dapat dijalankan dihitungan detik (Nissim, 2017). Peretas dapat melakukan implementasi penetrasi ke komputer yang berbasis *Windows* melalui USB Rubber Ducky. Mekanisme ini memungkinkan peretas untuk menyerang komputer yang tidak memiliki keamanan dalam menyimpan file yang bersifat rahasia seperti identitas pengguna dan kata sandi yang jelas dari komputer pengguna. Peretas Memanfaatkan beberapa alat dan teknologi seperti *PowerShell*, bahasa *scripting*, server web dan teknologi PHP. Rubber ducky dapat diimplementasikan dengan memanfaatkan perangkat Arduino. Arduino adalah platform elektronik yang berbasis *open-source* pada perangkat lunak. Script Rubber Ducky di implementasikan pada arduino. Perbedaan pada kedua platform ini adalah USB rubber ducky menggunakan platform Raspberry, sementara penelitian ini menggunakan Arduino. Arduino digunakan karena perangkat yang mudah didapat dan harga murah, dibandingkan USB Rubber Ducky yang sulit untuk didapatkan dan harga yang tergolong mahal.

Penyerangan pada penelitian ini menggunakan jenis penyerangan *Fork Bomb*. Jenis penyerangan *Fork Bomb* menggunakan perangkat Arduino Pro Micro. *Fork Bomb* merupakan serangan Denial of Service (DoS) yang bekerja dengan cara menciptakan proses baru secara berulang dan menghabiskan sumber daya sistem (Incapsula, 2018). Selama proses penyerangan *Fork Bomb input* dari *keyboard* akan di abaikan. Pada dasarnya penyerangan *Fork Bomb* bersifat mengunci sistem sehingga pengguna tidak dapat memberikan masukkan apapun kepada sistem. *Fork Bomb* akan memberatkan sistem kerja *CPU* dan memori, lalu sumber daya dari sistem akan habis sebelum sistem operasi mencapai proses maksimum yang telah diizinkan dan akan menghasilkan "*Kernel Panic"*, yaitu sistem operasi dari inti (*kernel*) tidak dapat mengatasi dan akan menyebabkan *crash* pada sistem operasi. Pada penelitian ini diharapkan dapat

mengetahui dampak dari penyerangan *Fork Bomb*. Penyerangan *Fork Bomb* pada penelitian ini menggunakan sistem operasi *Microsoft Windows.*

I.2 Rumusan Masalah

Dari berbagai uraian yang terdapat pada latar belakang, maka dapat ditarik rumusan sebagai berikut :

1. Bagaimana cara melakukan serangan *Fork Bomb* pada sistem operasi Windows dengan menggunakan Arduino?
2. Bagaimana melakukan implementasi *Fork Bomb* dengan menggunakan Arduino pada sistem operasi Windows?
3. Apa dampak serangan *Fork Bomb* pada sistem operasi Windows?

I.3 Tujuan

Adapun tujuan dari pembuatan Arduino adalah sebagai berikut :

1. Melakukan implementasi menggunakan Arduino pada sistem operasi Windows.
2. Melakukan serangan *Fork Bomb* pada sistem operasi Windows.
3. Melakukan analisis dampak serangan *Fork Bomb* pada sistem operasi Windows.

I.4 Manfaat

Adapun manfaat yang di dapatkan dari pembuatan Arduino, yaitu :

1. Mengetahui celah keamanan dari sistem operasi Windows.
2. Meningkatkan keamanan yang ada di sistem operasi Windows dari serangan *Fork Bomb*

I.5 Batasan Masalah

Adapun Batasan masalah dari pengimplementasian Arduino adalah sebagai berikut :

1. Arduino digunakan untuk melakukan penyerangan *Fork Bomb* pada Windows dibatasi dengan jumlah aplikasi yang terbuka.

2. Penyerangan *Fork Bomb* dibuat untuk sistem operasi Windows 8.
3. *Fork Bomb* dirancang untuk menyerang DOS (Denial Of Service).

Bab II LANDASAN TEORI

II.1 Definisi Arduino

Arduino adalah platform elektronik yang berbasis *open-source* pada perangkat lunak. Arduino dibuat di lvrea Interaction Design Institute sebagai alat untuk pembuatan prototipe yang cepat, ditujukan untuk siswa yang tidak memiliki latar belakang dalam elektronik dan pemograman. Arduino dapat berjalan pada platform Mac, Windows dan Linux.

Papan arduino dapat membaca inputan, jari yang berada di atas *button* seperti *keyboard* dan *mouse*, dan mengubahnya menjadi *output*. Mengirimkan inputan seperti yang dikatakan sebelumnya, harus menggunakan bahasa pemograman Arduino dan arduino *software* (IDE). (Arduino, 2018)

Arduino merupakan platform yang terdiri dari *software* dan *hardware*. *Hardware* arduino sama dengan mikrokontroler pada umumnya. Pada arduino ditambahkan penamaan yang berbeda dari mikrokontoler lainnya agar mudah untuk diingat.

II.2 Mikrokontroler

Mikrokontroler adalah komputer yang terintegrasi dari unit memori, unit aritmatika dan logika, dan unit kontrol. Ketiga komponen tersebut digabungkan menggunakan konsep dari teknologi mikrokontroler yaitu arsitektur *internal*, arsitektur *eksternal* dan antarmuka *input* dan *output* (Ferreira, 2015). Mikrokontroler terdiri dari CPU, RAM, RWM, I/O paralel, I/O seri, dan rangkaian *clock* dalam satu chip. Mikrokonktroler digunakan dalam produk dan alat yang dikendalikan secara otomatis, seperti sistem kontrol mesin, *remote control*, peralatan rumah tangga, alat berat, dan mainan (Wahyudi, 2017). Pada dasarnya, sebuah sistem minimum mikrokontroler memiliki prinsip dasar yang sama dan terdiri dari 4 bagian, yaitu :

1. *Processor.*
2. Rangkaian *reset*.
3. Rangkaian *clock*.
4. Rangkaian catu daya.

Berdasarkan pemaparan dari hasil penelitian sebelumnya, maka mikrokontroler adalah sebuah sistem komputer yang terintegrasi dari unit memori, unit aritmatika dan logika, dan unit kontrol membentuk suatu sistem komputer yang dapat diisikan sebuah aplikasi yang sifatnya sudah ditetapkan.

II.3 Universal Serial Bus (USB)

Universal Serial Bus (USB) adalah antarmuka yang menggunakan *plug and play* antara komputer dan perangkat tambahan seperti, pemutar media, *keyboard*, telepon, flash drive dan printer. USB mendukung *hot-swapping*, maksudnya adalah perangkat baru dapat ditambahkan ke komputer tanpa harus menambahkan kartu adaptor ataupun mematikan komputer. Standar bus perifer USB dikembangkan oleh perusahaan Compaq, IBM, Intel, Microsoft dan NEC (Rouse, 2012).

Universal Serial Bus (USB) adalah interkoneksi yang bermanfaat dalam dunia komputasi personal. USB menawarkan kecepatan transfer data. Setiap versi dari USB yang dikembangkan memiliki kecepatan transfer data yang berbeda seperti, USB 1.0 memiliki kecepatan transfer data 12 Mbps, USB 2.0 memiliki kecepatan transfer data 60 Mbps, USB 3.0 memiliki kecepatan transfer data 640 Mbps. Saat ini perkembangan teknologi USB sudah mencapai USB 3.1 dengan kecepatan transfer data 10Gbps (Intel, 2017).

II.4 *Software* Arduino IDE

Software Arduino IDE (Integrated Developtment Environment) adalah salah satu text editor yang berguna untuk menulis kode, area pesan, konsol teks dengan toolbar yang memiliki fungsi umum pada serangkaian menu. Program yang ditulis menggunakan *software* arduino IDE disebut dengan sketsa. Sketsa yang ditulis dalam teks editor disimpan dengan ekstensi .ino (Arduino, 2015).

Arduino adalah serangkaian kit elektronik yang bersifat *open-source* yang di dalamnya terdapat komponen utama yaitu sebuah chip mikrokontroler dengan jenis

AVR dari perusahaan Atmel. Arduino menggunakan bahasa pemograman C (Effendi, 2014). IC (Integrated Cirkuit) mikrokontroler arduino telah ditanamkan suatu program yang bernama Bootlader. IC (Integrated Cirkuit) berfungsi sebagai penengah antara *compiler* arduino dengan mikrokontroler.

II.5 Bahasa Pemrograman C

Bahasa Pemograman C adalah bahasa pemograman yang berada antara bahasa yang memiliki tingkat rendah dan tingkat tinggi (Jamila, 2015). Bahasa tingkat rendah itu ialah bahasa yang digunakan oleh mesin, membutuhkan kecermatan dan ketelitian yang tinggi karena perintahnya harus rinci. Sedangkan bahasa pemograman tingkat tinggi ialah bahasa yang mudah digunakan, karena ditulis dengan menggunakan bahasa manusia sehingga mudah dimengerti dan tidak tergantung pada mesin.

Bahasa pemrograman C adalah sebuah bahasa pemograman komputer yang bisa digunakan untuk membuat berbagai aplikasi, mulai dari sistem operasi, antivirus, hingga *compiler* untuk bahasa pemrograman. Bahasa pemrograman C sangat cepat dan efisien karena bahasa ini berkomunikasi langsung dengan *hardware* (Sujarwo, 2017).

II.6 Memori

Memori merupakan istilah umum yang mengacu ke perangkat fisik dari komputer yang mampu menyimpan data baik secara permanen maupun sementara. Memori termasuk komponen penting dalam sebuah komputer. Karena performa dari sebuah komputer salah satunya ditentukan oleh memori. Semakin besar ruang penyimpanan dan kecepatan dari memori, maka akan semakin bagus performa yang dihasilkan oleh komputer.

Memori utama digunakan untuk mengakses data secara cepat oleh prosesor dan tidak berfungsi sebagai tempat penyimpanan permanen melainkan sebagai tempat penyimpanan sementara dalam proses yang berada pada komputer.

1. Memori Utama

   Memori utama dibagi atas 2 bagian, yaitu:

a. Read Only Memori (ROM)

   Read Only Memori merupakan jenis memori yang kontennya tidak akan hilang ketika komputer mati. Memori ini hanya bisa dibaca saja dan tidak bisa dihapus prosesnya serta kontennya sudah di isi oleh pabrik pembuat. Intruksi yang ada di ROM diantaranya adalah intruksi untuk membaca sistem operasi, memeriksa semua komponen dari komputer dan menampilkan pesan layar.

b. Random Access Memori (RAM)

   Random Access Memori merupakan tempat penyimpanan sementara dari komputer saat dijalankan dan dapat diakses secara acak. RAM juga merupakan kumpulan chip memori berupa IC(*Integrated Circuit*) yang terdiri dari jutaan transistor dan kapasitor. Konten yang berada pada RAM dapat dirubah dan bersifat folatile. Fungsinya adalah untuk mempercepat pemrosesan data karena dapat disimpan dan diambil kembali dengan sangat cepat. Semakin besar RAM yang dimiliki oleh komputer, maka akan semakin cepat pula kinerja dari komputer tersebut.

2. Memori Sekunder

   a. Optical Storage Device

      Perangkt penyimpanan data permanen yang berbentuk kecil dan portable serta dapat diperoleh dengan mudah dan murah dipasaran. Metode penyimpanan nya menggunakan sinar laser untuk melakukan penyimpanan maupun pengambilan datanya dari media optik.Contoh dari optical storage device adalah compact disk, DVD, Blu-ray disc.

   b. Magnetic Storage Device

      Magnetic Storage Device merupakan media penyimpanan perangkat yang bersifat magentis yang melakukan penyimpanan data dalam bentuk titik – titik kecil bermagnet. Titik – titik ini dibuat, dibaca dan dihapus menggunakan medan magnet yang diciptakan oleh elektromagnet yang sangat kecil. Contoh dari magnetic storage device adalah hard drive, hard drive portabel, pita magnetik, floppy disc, zip disc.

II.7 USB Rubber Ducky

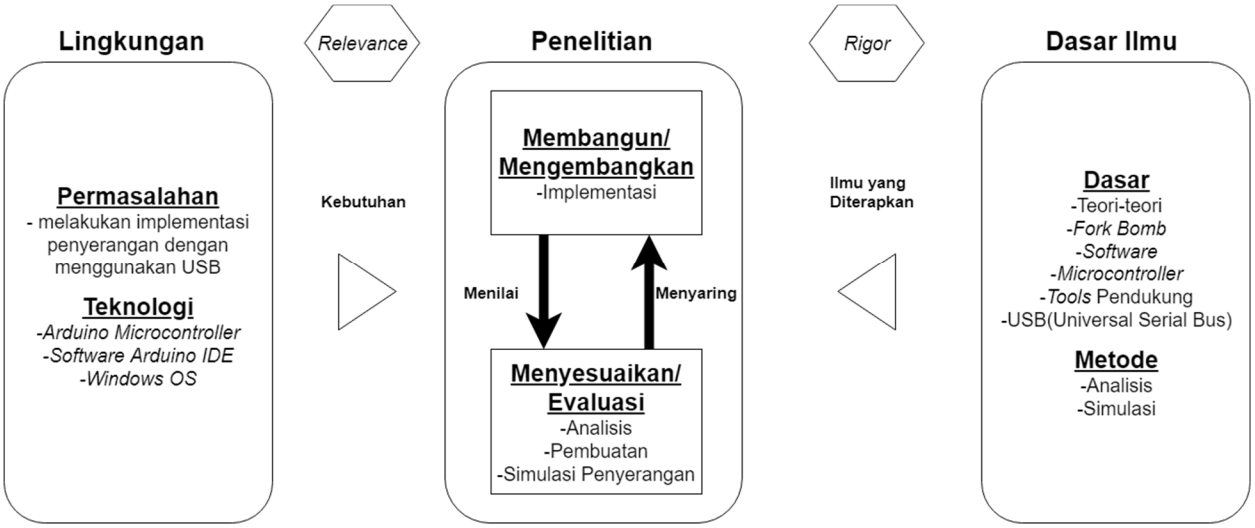
Rubber Ducky adalah platform serangan injeksi *keystroke* komersial yang dirilis pada tahun 2010. Setelah terhubung ke komputer, Rubber Ducky berperan sebagai *keyboard* dan menyuntikkan urutan *keystroke* yang dimuat. Rubber Ducky mendukung bahasa *scripting* sederhana yang memungkinkan peretas untuk membuat payload yang mampu mengubah pengaturan sistem, melakukan *backdoor*, mengambil data, memulai ulang *powerShell*. Rubber Ducky pada dasarnya dapat dicapai dengan akses fisik yang semuanya bersifat otomatis dan dapat dijalankan dihitungan detik (Nissim, 2017).

USB Rubber Ducky merupakan alat yang digunakan untuk menjalankan Ducky Script yang berada pada USB. Sementara Ducky Script adalah bahasa pemograman yang sederhana. Penulisan Ducky Script bisa menggunakan teks editor seperti notepad, notepad++, nano dan vi pada linux. Setiap perintah harus ditulis dengan baris baru dan menggunakan huruf kapital. Perintah pada Ducky Script harus memiliki penundaan atau jeda dalam penulisannya. Perintah yang paling umum digunakan adalah *DELAY* dan *STRING.* Perintah DELAY sangat penting dalam pembuatan Ducky Script karena USB RUBBER DUCKY sangat cepat dalam menjalankan Script. Sementara perintah STRING berfungsi untuk memproses Script yang sudah dibuat.

Bab III METODOLOGI PENELITIAN

III.1 Metode Konseptual

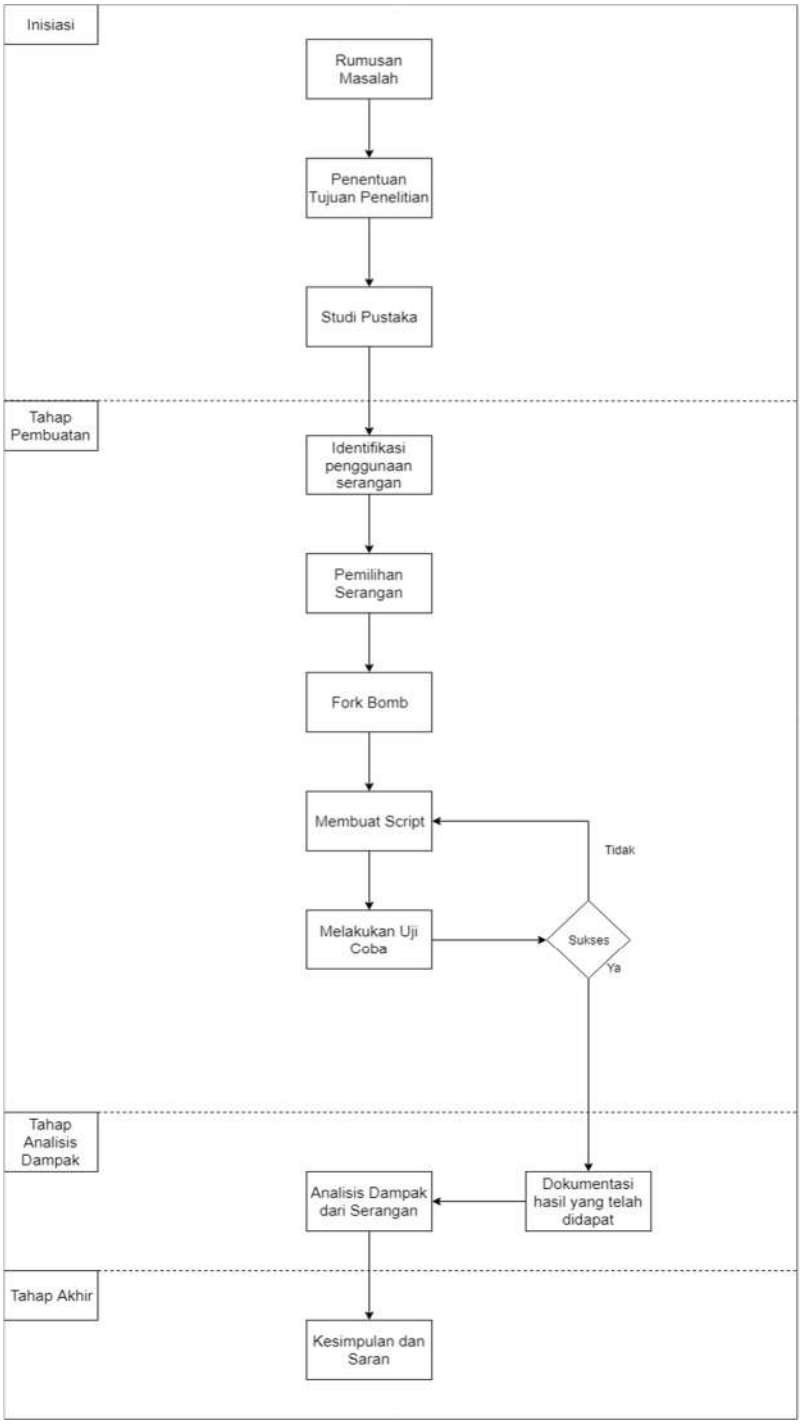
Model konseptual penelitian adalah suatu model konseptual yang menunjukkan hubungan logis antara faktor atau variabel yang telah diidentifikasi penting untuk menganalisis masalah penelitian (Yusrizalfirzal, 2010). Model konseptual merupakan suatu diagram yang menghubungkan faktor-faktor yang dapat memberikan dampak terhadap hasil penelitian. Model konseptual juga menggambarkan hubungan antara permasalahan dan solusi yang ditawarkan dalam penelitian dengan acuan pada sebuah metode atau dasar ilmu yang digunakan.



Gambar III–I Model Konseptual

Berdasarkan gambar 1 model konseptual, untuk mencapai tujuan dari penelitian ini diperlukan banyak percobaan untuk mendapatkan hasil yang maksimal. Penyerangan menggunakan jenis serangan *Fork Bomb* yang merusak pada sistem *resource* dari komputer korban. *Fork Bomb* adalah serangan Denial of Service (DoS) yang digunakan secara rekrusif sampai semua sumber daya sistem menjalankan perintah (Hope, 2017). Sistem akan kelebihan beban dan tidak dapat menanggapi masukan apapun termasuk untuk *logout* sekalipun.

III.2 Sistematika Penelitian



Gambar III–II Sistematika Penelitian

III.2.1 Inisiasi

Penelitian dimulai dari tahap inisiasi. Pada tahap ini peneliti akan membuat rumusan masalah, kemudian menentukan tujuan dari penelitian yang dilakukan dan dibatasi oleh ruang lingkup yaitu USB *Attack* Rubber Ducky. Pada tahap ini digunakan untuk memahami mengenai teori yang digunakan pada penelitian. Studi pustaka berisikan tentang teori-teori yang mendukung pengerjaan USB *Attack* Rubber Ducky.

III.2.2 Pembuatan

Pada bagian ini, sebelum membuat USB *Attack* peneliti melakukan identifikasi penggunaan serangan atau jenis serangan-serangan yang ingin digunakan pada USB nantinya. Selanjutnya peneliti akan melakukan pemilihan serangan terlebih dahulu sebelum melakukan instalasi *script* pada USB tersebut. Setelah memilih serangan untuk sistem operasi windows, maka peneliti sudah bisa untuk melanjutkan ke tahap membuat *script* untuk USB. Pembuatan menggunakan Arduino IDE dengan bahasa pemograman C menggunakan alat yaitu USB mikrokontroler yang berjenis Pro Micro. Jika setelah uji coba masih terdapat kekurangan, maka selanjutnya melakukan proses *update* untuk *script* tersebut. Jika sudah cukup peneliti bisa langsung melakukan dokumentasi dari penyerangan USB.

III.2.3 Analisis Data

Pada bagian ini, dilakukan dokumentasi dari data hasil uji coba penyerangan USB. Setelah itu melakukan analisa dampak dari penyerangan tersebut terhadap komputer. Data hasil tersebut dapat digunakan untuk mencegah penyerangan dengan jenis tersebut.

III.2.4 Akhir

Pada bagian akhir, penulis akan menuliskan beberapa kesimpulan yang dapat diambil dari penelitian ini dan juga beberapa saran untuk mengembangkan penelitian selanjutnya. Penelitian akan menghasilkan dampak dari penyerangan menggunakan USB.

Bab IV Perancangan Sistem dan Skenario Penyerangan

IV.1 Peralatan Utama dan Pendukung

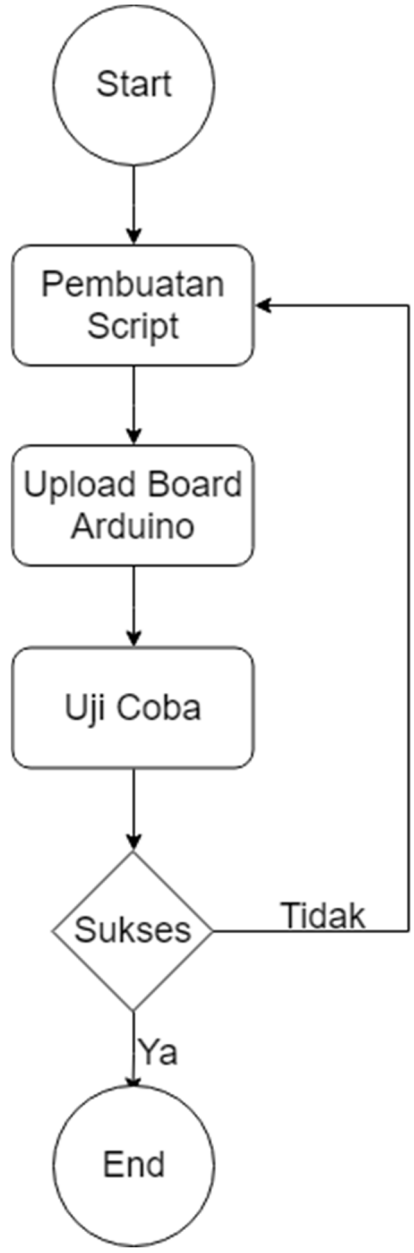
Pada bagian ini dibutuhkan peralatan untuk merancang *Fork Bomb*, sebagai berikut :

1. Dua perangkat Laptop dengan masing-masing spesifikasi sebagai berikut:
   a. Komputer yang digunakan untuk perancangan dengan spesifikasi Processore Intel (R) Core(TM) i7-6700HQ CPU @ 2.60GHz (8 CPUs), ~2.6GHz dengan RAM (*Random Access Memory*) Sebesar 16384 MB RAM DDR4, Windows 10 OS.
   b. Komputer yang digunakan untuk target penyerangan dengan spesifikasi Processore Intel (R) Core(TM) i7-3631QM CPU @2.20GHz (8 CPUs), Turbo Boost 3.20GHz dengan RAM (*Random Access Memory*) Sebesar 3819 MB RAM DDR3, Windows 8 OS.
2. Software Arduino IDE untuk membuat *script* USB.
3. *Arduino Pro Micro* adalah perangkat keras untuk melakukan penyerangan.
4. Sistem operasi Windows 8 untuk target penyerangan.

IV.2 Perancangan

Pelaksanaan penelitian ini bertujuan untuk melumpuhkan komputer korban / serangan yang mengganggu operasi layanan komputer dengan mengonsumsi banyak sumber daya komputasi, agar komputer korban tersebut akan kehilangan data penting yang ada di dalam komputer. Pada proses perancangan USB Attack, arduino yang sudah diberikan *script* akan dihubungkan ke komputer korban dengan menggunakan kabel USB. Setelah Arduino terhubung dengan komputer korban, arduino akan menjalankan *script* yang sudah tertanam di dalam arduino dan akan menjalankannya dengan otomatis tanpa persetujuan dari korban. Kemudian program akan jalan terus-menerus sampai RAM yang ada di komputer korban habis dan tidak bisa menjalankan program lainnya. Untuk mendapatkan kembali komputer harus melakukan reebot paksa dengan menekan tombol *power*. Pada perancangan ini menggunakan Microsoft Paint untuk membuat serangan menggunakan *Fork Bomb.* Karena aplikasi Microsoft paint merupakan aplikasi

bawaan dari Windows, tidak memerlukan memori yang besar untuk menjalankan aplikasi tersebut, jarang dihapus oleh *user* dan korban tidak memikirkan bahwa aplikasi ini merupakan target dari penyerangan.



Gambar IV–I Perancangan