Bab I Pendahuluan

I.1 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 penyerangan berupa pengambilan data *browser* Google Chrome dan Mozilla Firefox dari komputer dengan sistem operasi Windows menggunakan perangkat Arduino *Pro Micro* Leonardo sebagai USB *Password Stealer*. Mekanisme ini memungkinkan penyerang untuk terhubung dengan komputer target menggunakan USB *Human Interface Device* (HID) berupa *keyboard* kemudian mengambil *username* dan *password* yang disimpan pada *browser* dari komputer target menggunakan program ChromePass dan PasswordFox melalui *Command Prompt* (CMD) dan Powershell. Data yang telah diambil dari *browser* kemudian dikirimkan melalui *email*. Disini penulis memanfaatkan beberapa alat dan teknologi seperti Arduino *Pro Micro* Leonardo, Arduino *Integrated Development Environment* (IDE), ChromePass, dan PasswordFox.

I.2 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?

I.3 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.

I.4 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*.
2. Praktis.

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

I.5 Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu:

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

I.6 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 sistem dan skenario 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.