Bab VI Kesimpulan dan Saran

VI.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagaimana berikut:

1. Perangkat Arduino *Pro Micro* Leonardo dapat diprogram menjadi USB *password stealer* menggunakan Arduino IDE dan *tools* dari Nirsoft.net. Ketika USB *password stealer* dihubungkan dengan komputer target, program akan berjalan untuk mengambil data *username* dan *password* yang tersimpan pada *browser* menggunakan ChromePass dan PasswordFox. *Output* dari penelitian ini adalah didapatkannya *login data* yang dikirimkan kepada penyerang melalui *email*.
2. Pengambilan data dari Google Chrome dan Mozilla Firefox dapat dilakukan dengan menggunakan ChromePass dan PasswordFox sehingga tingkat keamanan dari menyimpan *username* dan *password* pada *browser* cukup rentan. Berdasarkan proses pengambilan data yang dilakukan menggunakan USB *password stealer*, versi *browser* yang digunakan adalah Google Chrome versi 83.0.4103.116 dan Mozilla Firefox versi 77.0.1. Penyerangan ini dapat dilakukan pada seluruh versi kedua *browser* dibawahnya namun belum tentu dapat digunakan pada versi terbaru nantinya dikarenakan mungkin akan ada peningkatan keamanan dari masing-masing *browser*
3. Rekomendasi untuk meminimalisir terjadinya penyerangan seperti ini berdasarkan aspek pengguna adalah memperhatikan komputer agar tidak dihubungkan dengan perangkat USB yang mencurigakan, mematikan atau mengunci komputer saat sedang ditinggalkan, tidak menyimpan *username* dan *password* pada *browser* apapun, dan menggunakan fitur 2-step verification pada akun pribadi baik tersimpan maupun tidak pada *browser*. Adapun dari sisi keamanan sistem dapat dilakukan pembaruan pada *browser* Google Chrome dan Mozilla Firefox, menggunakan aplikasi BPM pihak ketiga, mematikan *port* USB pada perangkat komputer dan melakukan *disable port* SMTP

VI.2 Saran

Untuk penelitian lebih lanjut, terdapat saran-saran yang dapat membantu untuk mengembangkan penelitian dimasa yang akan datang, yaitu:

1. Melanjutkan pengujian USB *Attack* dengan target pengambilan data *browser* yang lebih luas seperti *history, bookmark,* dan *cache*.
2. Memperhatikan versi *tools* penyerangan yang disediakan Nirsoft.com, selalu usahakan untuk menggunakan versi terbaru untuk setiap program yang digunakan.
3. Melakukan penelitian menggunakan *antivirus* selain Windows *Defender* untuk mencegah berjalannya program yang mencurigakan pada komputer.