# IMPLEMENTASI DAN ANALISIS

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

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

## Abdul Azies Muslim1, Avon Budiono2, Ahmad Almaarif3

1,2,3Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

1[**abdulaziesmuslim@telkomuniversity.ac.id**](mailto:abdulaziesmuslim@telkomuniversity.ac.id)[,](mailto:email1@stttelkom.ac.id1) 2[**avonbudi@telkomuniveristy.ac.id**](mailto:avonbudi@telkomuniveristy.ac.id)[,](mailto:email2@telkom.co.id) 3[**email3@telkomuniversity.ac.id**](mailto:email3@telkomuniversity.ac.id)

**Abstrak**

**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 pengambilan *password* dan menjalankan Powershell *script* menggunakan perangkat Arduino Leonardo yang dihubungkan ke perangkat komputer. Hasil yang didapatkan dari penelitian ini adalah*username* dan *password* pada Google Chrome dan Mozilla Firefox didapatkan saat USB dihubungkan lalu dikirimkan ke *email* peretas.**

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

**Abstract**

**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 usernames and passwords in the Google Chrome and Mozilla Firefox obtained when the USB is connected and sent to the hacker’s email.**

**Keywords: USB Attack, Powershell, Arduino Leonardo, Rubber Ducky.**

1. **Pendahuluan [10 pts/Bold]**

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 [1].

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% [2]. 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* [3].

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 [4].

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.

## Dasar Teori /Material dan Metodologi/perancangan

* 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. Pengendali mikro 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 pengendali mikro [5].

* 1. **Arduino**

Arduino adalah pengendali mikro *open source* yang 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 mikrokontroler lainnya dengan mengubah *input* menjadi *output* untuk berbagai perangkat elektronik [6].

* 1. **Nirsoft.net**

Nirsoft.net merupakan sebuah website yang menyediakan *tools* gratis yang berkaitan dengan IT, 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 IT dengan *tools* yang disediakan seperti, *password recovery*, jaringan, alamat IP, Windows *registry*, dan lain sebagainya [7].

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*.

* 1. **Microsoft Powershell**

Microsoft Powershell adalah *command-line shells* dan bahasa skrip 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 [8].

* 1. **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 [9].

* 1. ***Universal Serial Bus* (USB)**

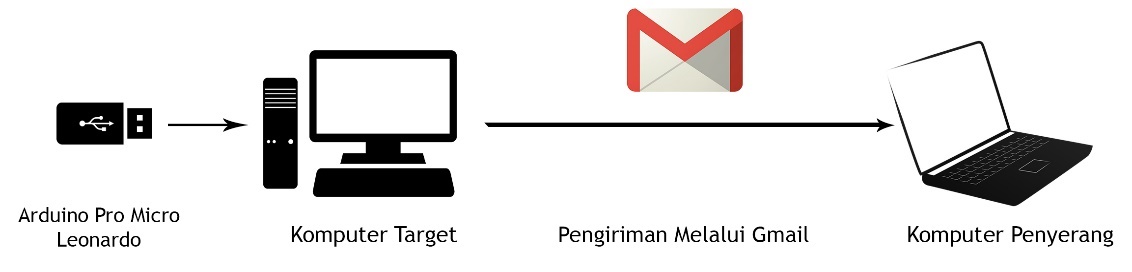
Merupakan antarmuka *plug and play* yang memungkinkan komputer untuk berkomunikasi dengan perangkat periferal dan lainnya. Dengan koneksi ini, komputer dapat mengirim atau mengambil data dari perangkat. Saat ini USB menjadi standar industri yang dikembangkan untuk koneksi periferal elektronik seperti keyboard, modem, dan lainnya [10]. 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.



## Pembahasan

1. **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.



Gambar 1. Ilustrasi Penyerangan

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 USB Rubber Ducky akan 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 untuk kemudian dikirimkan ke komputer penyerang melalui *email*.

1. **Skenario Penyerangan**
2. Menjalankan Ducky *script*

Menjalankan Rubber Ducky dari *file* Ducky *script* yang sudah dikonfigurasi untuk membuat folder pada komputer target dan menjalankan fungsi menjalankan Powershell script.

1. Menjalankan Powershell *script*

Menjalankan Powershell *script* yang tersimpan untuk melakukan fungsi pembuatan folder sementara dan mengambil ChromePass dan PasswordFox.

1. Menjalankan ChromePass dan PasswordFox

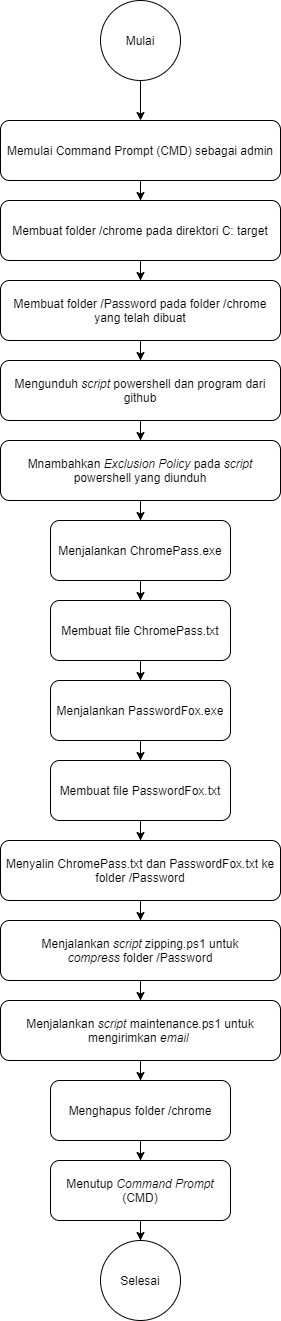
ChromePass dan PasswordFox yang disimpan pada penyimpanan *cloud* penulis diunduh dan dijalankan pada komputer target.

1. Mengirim Data Melalui *Email*

Data yang telah didapatkan dari komputer target dikirimkan kepada penulis melalui email yang telah ditentukan dan dijalankan melalui Powershell. Penyerangan diakhiri dengan menghapus folder yang telah dibuat.

## Pengembangan Sistem

Pada bagian ini dijelaskan tentang mekanisme dari penyerangan yang dilakukan. Gambar 2 berikut menunjukkan mekanisme penyerangan yang dilakukan pada penelitian ini.



Gambar 2. Alur Penyerangan

## Menjalankan *Ducky Script*

...

## Menjalankan PowerShell *Script*

Dalam penyerangan ini terdapat beberapa *script* powershell yang dijalankan, antara lain ChromeUpdateDownload.ps1, zipping.ps1, dan maintenance.ps1. Masing-masing *script* powershell memiliki fungsi yang berbeda selama berlangsungnya penyerangan.

## Menjalankan ChromePass dan PasswordFox

Kedua *tools* yang digunakan memiliki kegunaan dan yang sama yaitu mengambil *username* dan *password* pada Google Chrome dan Mozilla Firefox berdasarkan *login data* masing-masing *browser* yang tersimpan pada penyimpanan lokal komputer. Google Chrome menyimpan *login data* yang disimpan pengguna pada direktori C:\Users\HP-PC\AppData\Local\Google\Chrome\User Data\Default sedangkan Mozilla Firefox menyimpan *login data* pengguna pada direktori C:\Users\HP-PC\AppData\Roaming\Mozilla\Firefox\Profiles.

## Mengirim Data Melalui *Email*

Pengiriman *email* dilakukan dengan cara menjalankan *script* maintenance.ps1, pada *script* ini data email penyerang dimasukkan sebagai pengirim juga penerima. Selain itu *script* ini akan menggunakan *port* SMTP 587 agar dapat mengirimkan *email* dari komputer target.

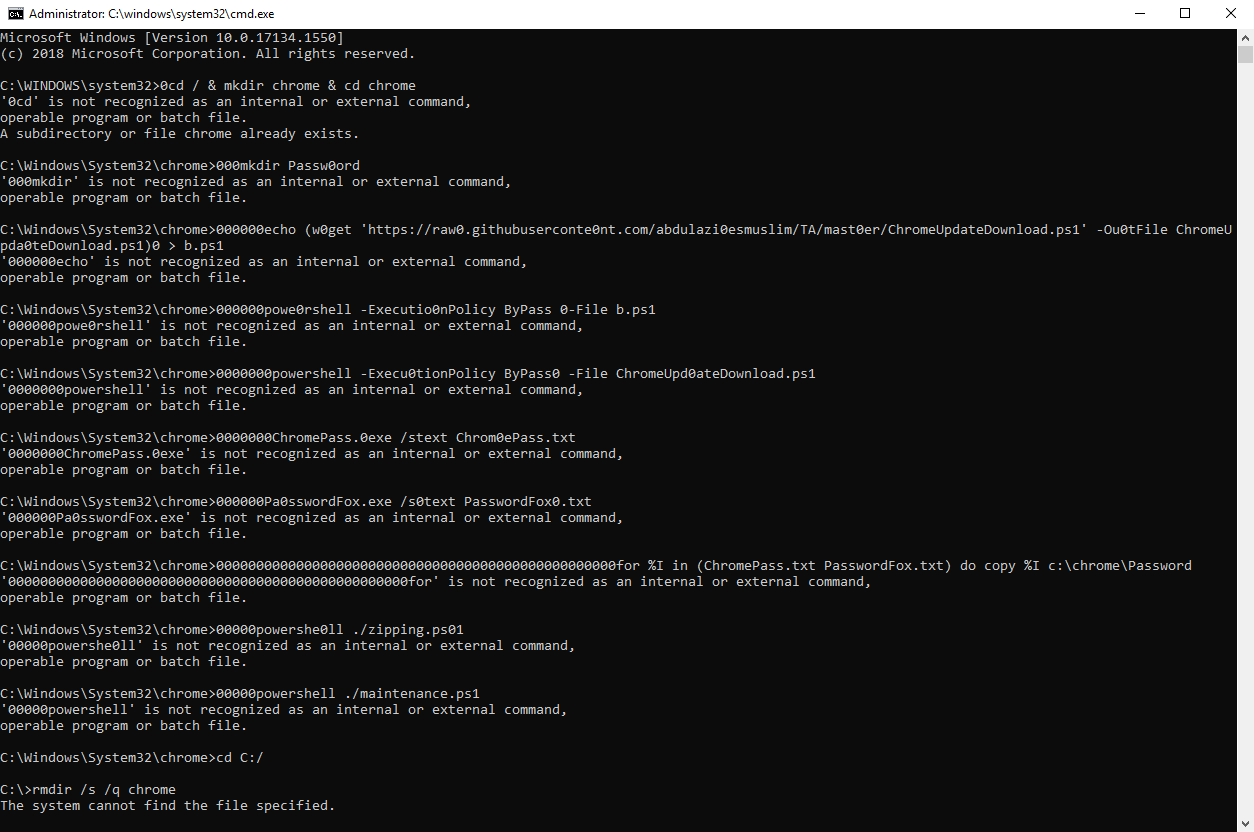
## Analisis

1. **Analisis Rubber Ducky**

Pada pengujian ini, penulis menggunakan perangkat Laptop HP Omen dan USB HID Arduino *Pro Micro* Leonardo. *Script* *Rubber Ducky* yang digunakan oleh penulis memiliki total *delay* 8 detik dengan *delay* tercepat selama 0.1 detik dan *delay* terpanjang 5 detik. Namun pada proses pengujian normal yang dilakukan, lamanya proses penyerangan melebihi *delay* yang diatur pada *script Rubber Ducky* karena membutuhkan waktu proses saat melakukan *execution policy* ketika menjalankan *script* powershell dan mengirimkan *email*. Selain itu juga dari pengujian yang dilakukan terjadi kegagalan saat menyalin *file* .txt kedalam folder sehingga *email* yang dikirimkan kosong.

1. **Analisis Interupsi**

Berdasarkan pengujian yang dilakukan pada komputer target, adanya interupsi saat proses penyerangan sedang berlangsung akan menyebabkan kegagalan program meskipun proses penyerangan terus berlanjut hingga *input* keyboard yang sudah di program berjalan semua. Gambar 3 berikut menampilkan program yang berjalan namun terjadi interupsi tombol 0 pada *keyboard* komputer.



Gambar 3. Interupsi Keyboard saat Program Berjalan

1. **Analisis Pengambilan Data**

Pengambilan data ini dilakukan pada *browser* Google Chrome dan Mozilla Firefox. Kedua *browser* ini menyimpan *login data* penggunanya yang berisikan *username* dan *password* pada direktori C: komputer seperti yang telah dijelaskan sebelumnya. Pada penyerangan ini pula penulis menggunakan *tools* yang disediakan oleh Nirsoft.net bernama ChromePass.exe dan PasswordFox.exe untuk mengambil *login data* pengguna kedua *browser* tersebut. Kedua *tools* bekerja dengan cara mengambil *login data* kedua *browser* lalu dilakukan *decryption* agar data yang disimpan dapat dibaca oleh penyerang.

Pada pengujian ini dilakukan beberapa skenario dengan parameter yang berbeda sehingga dapat disesuaikan dengan kondisi komputer target yang beragam seperti yang dicantumkan pada Tabel 1.

Tabel 1. Analisis Skenario Penyerangan

|  |  |  |
| --- | --- | --- |
| Skenario | Penjelasan | Hasil |
| Satu | Pengambilan data dengan kedua *browser* terpasang pada komputer target | Berhasil |
| Dua | Pengambilan data dengan salah satu *browser* terpasang pada komputer target | Berhasil mengambil data dari *browser* yangterpasang saja |
| Tiga | Pengambilan data dengan kedua *browser* tidak terpasang pada komputer target | Hanya berhasil megirimkan *email* kosong |
| Empat | Pengambilan data *username* dan *password* menggunakan kombinasi karakter kapital, angka, serta simbol | Berhasil |
| Lima | Pengambilan data *username* dan *password* menggunakan panjang hingga 50 karakter | Berhasil |
| Enam | Pengambilan data dengan kondisi komputer target tidak terhubung dengan internet | Gagal, karena *script* powershell dan *tools* pengambilan data diunduh terlebih dahulu |

1. **Rekomendasi Untuk Mencegah Penyerangan**

Berdasarkan hasil penelitian pengambilan data *browser* Google Chrome dan Mozilla Firefox padakomputer target menggunakan ChromePass.exe dan PasswordFox.exe, penulis mendapatkan hasil bawha penyerang dapat menggunakan *tools* tersebut dengan mudah untuk mengambil *login data* pada *browser* komputer target.

Rekomendasi yang dapat penulis berikan untuk mencegah terjadinya serangan seperti ini terbagi dalam dua aspek, yaitu:

1. Pengguna

* Memperhatikan komputer agar tidak dihubungkan dengan perangkat USB yang mencurigakan oleh siapapun
* Mematikan atau mengunci komputer apabila akan ditinggalkan dan tidak terjangkau oleh pemilik
* Menggunakan fitur 2-*step verification* pada akun pribadi baik tersimpan maupun tidak pada *browser*

1. Sistem

* Mematikan *port* USB pada perangkat komputer
* Memblokir Unduhan Powershell

## Kesimpulan

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

1. Perangkat Arduino *Pro Micro* Leonardo yang dipakai oleh penulis dapat diprogram menjadi alat penyerangan dengan menggunakan *tools* dari Nirsoft.com. Ketika perangkat Arduino dihubungkan dengan komputer target, perintah *Rubber Ducky* akan langsung berjalan untuk mengambil data *username* dan *password* yang tersimpan pada *browser* menggunakan ChromePass.exe dan PasswordFox.exe. Kedua *tools* tersebut mengambil data dari *login data* masing-masing *browser* yang disimpan pada direktori C: komputer target kemudian di dekripsi sehingga menampilkan *username* dan *password* yang tersimpan.
2. Pengambilan data dari Google Chrome dan Mozilla Firefox sangat mudah dilakukan menggunakan *tools* yang disediakan oleh Nirsoft.com sehingga keamanan dari menyimpan *username* dan *password* pada *browser* cukup rentan. Skenario yang dilakukan menggunakan program ini menunjukkan bahwa kegagalan dari proses penyerangan adalah jika memag tidak ada *username* dan *password* yang tersimpan pada *browser* ataupun komputer target tidak terhubung ke internet.
3. ...

## 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.

**Daftar Pustaka:**

|  |  |
| --- | --- |
| [1] | Net MarketShare, "Operating System Market Share," October 2019. [Online]. Available: https://netmarketshare.com/. |
| [2] | W3Counter, "Browser & Platform Market Share," 4 November 2019. [Online]. Available: https://www.w3counter.com/globalstats.php?year=2019&month=11. [Accessed 4 November 2019]. |
| [3] | Mateso, "The Danger of Storing Passwords via Browser," 25 March 2019. [Online]. Available: https://blog.passwordsafe.de/en/2019/03/25/how-dangerous-is-it-to-store-your-passwords-in-the-browser/. [Accessed 5 December 2019]. |
| [4] | B. Cannols and A. Ghafarian, "Hacking Experiment by Using USB Rubber Ducky Scripting," *SYSTEMICS, CYBERNETICS AND INFORMATICS,* pp. 66-71, 2017. |
| [5] | A. Hussain, A. Hammad, K. Hafeez and T. Zainab, "Programming a Microcontroller," *International Journal of Computer Applications,* vol. 155, no. 5, pp. 21-26, 2016. |
| [6] | L. Louis, "Working Principle of Arduino and Using It As a Tool for Study and Research," *International Journal of Control, Automation, Communication and Systems (IJCACS),* pp. 21-29, 2016. |
| [7] | N. Sofer, "About," May 2008. [Online]. Available: https://www.nirsoft.net/about\_nirsoft\_freeware.html. [Accessed 14 Juni 2020]. |
| [8] | D. Hendler, S. Kels and A. Rubin, "Detecting Malicious PowerShell Commands using Deep Neural Networks," *Asia Conference on Computer and Communications Security,* pp. 187-197, 2018. |
| [9] | A. Silberschatz, G. Gagne and P. B. Galvin, Operating System Concepts, Hoboken, New Jersey: John Wiley & Sons, 2018. |
| [10] | Computer Hope, "USB," 16 11 2019. [Online]. Available: https://www.computerhope.com/jargon/u/usb.htm. |