IMPLEMENTASI DAN ANALISIS *USB ATTACK* BERBASIS *POWERSHELL* MENGGUNAKAN P4WNP1 PADA *PERSONAL COMPUTER*

IMPLEMENTATION AND ANALYSIS OF USB ATTACK BASED ON POWERSHELL USING P4WNP1 IN PERSONAL COMPUTER

Aufa Tesar Ramadhan[1], Avon Budiyono[2], Ahmad Almaarif[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]tesarramadhan@telkomuniversity.ac.id, [2]avonbudi@telkomuniveristy.co.id,
[3]ahmadalmaarif@telkomuniversity.ac.id

Abstrak

Sistem operasi *Windows* merupakan salah satu sistem operasi yang populer digunakan saat ini. Pesatnya perkembangan sistem operasi *Windows,* diikuti pula dengan pesatnya perkembangan *browser* yaitu *Microsoft Edge* yang merupakan *browser* bawaan dari sistem operasi *Windows* terbaru yaitu *Windows 10*. Pada *Microsoft Edge* terdapat celah dimana pengguna lain yang tidak memiliki otoritas dapat mengakses *username* dan *password* yang tersimpan dari *Microsoft Edge* menggunakan *method* pada *Powershell. Powershell* menjadi tempat yang populer untuk melakukan *cyber criminals* pada sistem operasi *Windows. BadUSB* merupakan perangkat USB yang dimanipulasi oleh penyerang. Terdapat suatu platform serangan USB yang dinamakan P4wnP1. Penggunaan P4wnp1 memungkinkan untuk melakukan penyerangan melalui *Powershell* dan melakukan pengambilan *username* dan *password* yang tersimpan. Untuk melakukan penelitian menggunakan P4wnP1, dibutuhkan metode *Rubber Ducky* untuk melakukan pembuatan *Custom Drive Letter* dan menjalankan *Powershell script.* Hasil dari penelitian ini adalah proses *Rubber Ducky* berjalan dengan total waktu 8.5 detik dengan *delay* tercepat yaitu 0.5 detik dan *delay* terpanjang yaitu 3 detik. USB *attack* dengan melakukan pengambilan data *username* dan *password* yang tersimpan pada *browser Microsoft Edge* dan *Internet Explorer* dengan melakukan beberapa macam skenario penyerangan dapat 100% berhasil dilakukan dan didapatkan rekomendasi yang digunakan untuk meminimalisir terjadinya serangan.

Kata kunci : ***USB attack, powershell, raspberry, P4wnP1, rubber ducky.***

Abstract

The Windows Operating System is one of the most popular operating systems in use today. The rapid development of the Windows operating system, followed by the development of browsers, namely Microsoft Edge. In Microsoft Edge, which is related to other users who do not have usable authority, users and passwords originating from Microsoft Edge use methods in Powershell. Powershell is a popular place to do cyber criminals on the Windows operating system. BadUSB is a USB device that is manipulated by attackers. It is a USB attack platform called P4wnP1. The use of P4wnp1 makes it possible to attack via Powershell and retrieve a saved username and password. To conduct research using P4wnP1, a Rubber Ducky method is needed to create Custom Drive Letters and run Powershell scripts. The result of this research is that the Rubber Ducky process runs with a total time of 8.5 seconds with the fastest delay of 0.5 seconds and the longest delay is 3detic. USB attacks by retrieving user name data and passwords stored on Microsoft Edge and Internet Explorer browsers by performing various types of attacks can be 100% successful and an assessment is used to minimize the attack..

Keywords: ***USB attack, powershell, raspberry, P4wnP1, rubber ducky.***

1. Pendahuluan

Sistem operasi *Windows* menempati posisi tertinggi dalam penggunaan sistem operasi terbanyak digunakan pada oktober 2018 yaitu sebanyak 78.04% [1]. Sistem operasi *windows* terdapat suatu kerangka atau *framework* berbasis .NET yang bernama *Powershell*. *Powershell* menawarkan suatu antarmuka berbasis perintah dan bahasa *scripting* untuk mengotomasi serta mengelola *tasks*. *Powershell* menyediakan akses penuh terhadap fungsi sistem seperti *Windows Management Instrumentation* (WMI) dan *Component Object Model* (COM) [2].

Pesatnya perkembangan sistem operasi, diikuti pula dengan pesatnya perkembangan peramban internet atau *browser* yaitu *Microsoft Edge* yang merupakan peramban internet bawaan dari sistem operasi *Windows*

terbaru yaitu *Windows* 10. Microsoft Edge menyumbangkan 8 persen dari 1,2 miliar kunjungan ke situs pemerintahan di Amerika Serikat dan jumlahnya terus meningkat pada 3 bulan pertama tahun 2018 [3]. Pengguna browser Microsoft edge dapat melakukan penyimpanan *username* dan *password* menggunakan fitur penyimpanan yang terdapat pada *browser Microsoft edge*, namun pengguna lain yang tidak memiliki otoritas pada satu komputer dapat mengakses *username* dan *password* yang tersimpan dari Microsoft Edge dengan menggunakan *method* yang dimiliki oleh *Powershell* [4]. *Powershell* yang menjadikannya pilihan ideal untuk beragam tujuan. Dilaporkan bahwa terjadi peningkatan sebesar 661 persen serangan berbasis *Powershell* pada paruh kedua tahun 2017 hingga paruh pertama tahun 2018 [5].

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 berbasis USB yang lebih berbahaya muncul dan dikenal sebagai keluarga *BadUSB* yang dapat dimodifikasi sesuai dengan kebutuhan yang bernama P4wnP1 [6]. . Penggunaan P4wnp1 memungkinkan untuk melakukan penyerangan melalui *Powershell*. Dengan kemudahan yang disediakan oleh P4wnP1, penyerang dimungkinkan untuk melakukan pengambilan data username dan password yang tersimpan. *File* yang memuat informasi mengenai *email* dan kata sandi pengguna tersebut akan tersimpan pada USB *Flash Drive* dan langsung dikirimkan melalui *email*.

2. Dasar Teori

2.1. Raspberry Pi Zero W

Raspberry Pi merupakan *Single Board Computer* (SBC) berukuran kartu kredit dengan biaya rendah yang dikembangkan oleh Yayasan Raspberry Pi di Inggris [7]. *Raspberry Pi Zero W* sangat berguna karena dapat dipasangkan dengan perangkat keras dan perangkat lunak dengan biaya rendah sehingga dapat digunakan dalam berbagai macam proyek *Do-It-Yourself* [8]. *Raspberry Pi Zero W* dapat berguna untuk berbagai macam penggunaan sehari-hari, salah satu contoh yaitu dapat digunakan dalam hal penyerangan untuk mencari celah yang terdapat pada suatu sistem [9].

2.2. Powershell

Windows Powershell merupakan suatu kerangka kerja atau *framework* yag dibangun di atas *.NET Framework Common Language Runtime* (CLR) dan *accept and return .Net Framework* [10]. *Windows* menyediakan wadah untuk menulis dan menguju skrip yang sedang dikerjakan yang disebut *Powershell Integrated Scripting Environtment* (ISE) dan akan menghasilkan *file* skrip *Powershell*. Ekstensi dari *file* skrip *Powershell* tersebut adalah .ps1 [2].

2.3. Sistem Operasi

Menurut *American National Standart Institute* (ANSI) Sistem operasi merupakan s*oftware* yang mengelola program-program komputer, yaitu mengatur waktu kerja, pengecekan kesalahan, mengelola *input* dan *output*, penyimpanan, komplikasi serta pengolahan data. Secara umum, dapat disimpulkan bahwa sistem operasi merupakan *software* lapisan pertama pada memori komputer pada saat komputer dinyalakan atau *booting*, yang bertugas mengelola sumber daya *hardware* komputer, dan menyediakan layanan untuk aplikasi *software* lainnya [11].

2.4. USB

Universal Serial Bus (USB) merupakan antarmuka plug and play yang memungkinkan komputer untuk berkomunikasi dengan perangkat periferal dan lainnya [12]. Saat ini USB menjadi standar industri yang dikembangkan untuk koneksi periferal elektronik seperti keyboard, modem, *flash drive* dan lainnya. 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* [13].

2.5. Credential Manager

Credential manager merupakan digital locker sebagai tempat Windows menyimpan log-in credentials seperti username dan password. Informasi tersebut disimpan oleh Windows dan dapat digunakan di komputer lokal, di komputer lain dengan jaringan yang sama, atau situs web. Data ini dapat digunakan oleh Windows sendiri atau oleh aplikasi dan program seperti File Explorer, Microsoft Office dan Skype.

2.6. P4wnP1

P4wnP1 merupakan platform serangan USB yang dapat disesuaikan dengan kebutuhan penyerangan yang

disematkan kedalam *microcontroller* Raspberry Pi Zero atau Raspberry Pi Zero W [14]. P4wnP1 dijadikan pilihan karena mekanisme perancangan penyerangan dapat disesuaikan dengan kebutuhan dan karena kemampuannya dalam menjalankan perintah *Rubber Ducky* yang berfungsi untuk mengakses powershell script [14].

2.7. USB Rubber Ducky

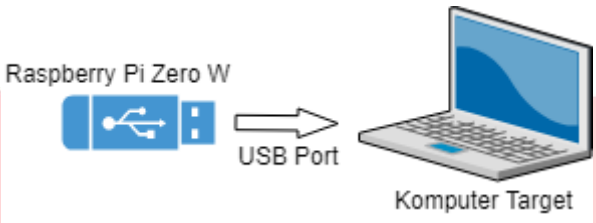
USB *Rubber Ducky* merupakan perangkat untuk melakukan pengujian penetrasi atau penyerangan. Saat perangkat ini dihubungkan ke komputer, perangkat akan mendaftarkan dirinya sebagai keyboard USB pada sistem dan memungkinkan untuk menyuntikan *script* berbahaya [15].

Ducky script merupakan bahasa pemrograman high-level. Script dapat dilakukan dari editor teks ascii yang sudah umum digunakan seperti Notepad, vi, nano, dll. Perintah pada Ducky script ditulis dengan huruf kapital. Sebagian besar perintah digunakan untuk melakukan panggilan ketikan kombinasi. Sementara beberapa perintah lain yaitu untuk penundaan atau jeda.

3. Pembahasan

3.1. 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 Perancangan sistem

Pada Gambar 1 ditampilkan ilustrasi penyerangan yang dilakukan untuk melakukan pengambilan data pada komputer target. Penyerangan diawali dengan menghubungkan *Raspberry Pi Zero W* yang sudah modifikasi menyerupai USB *Flashdisk* ke komputer target melalui *port* USB. Setelah itu P4wnP1 akan bekerja secara otomatis menjadikan *Raspberry Pi Zero W* sebagai USB *Mass Storage* dan menjalankan USB *Rubber Ducky* yang menjalankan baris kode yang disematkan oleh penyerang ke dalam P4wnP1. Hasil dari penyerangan ini akan didapatkan *username* dan *password* yang tersimpan pada *browser Microsoft Edge* dan *Internet Explorer.*

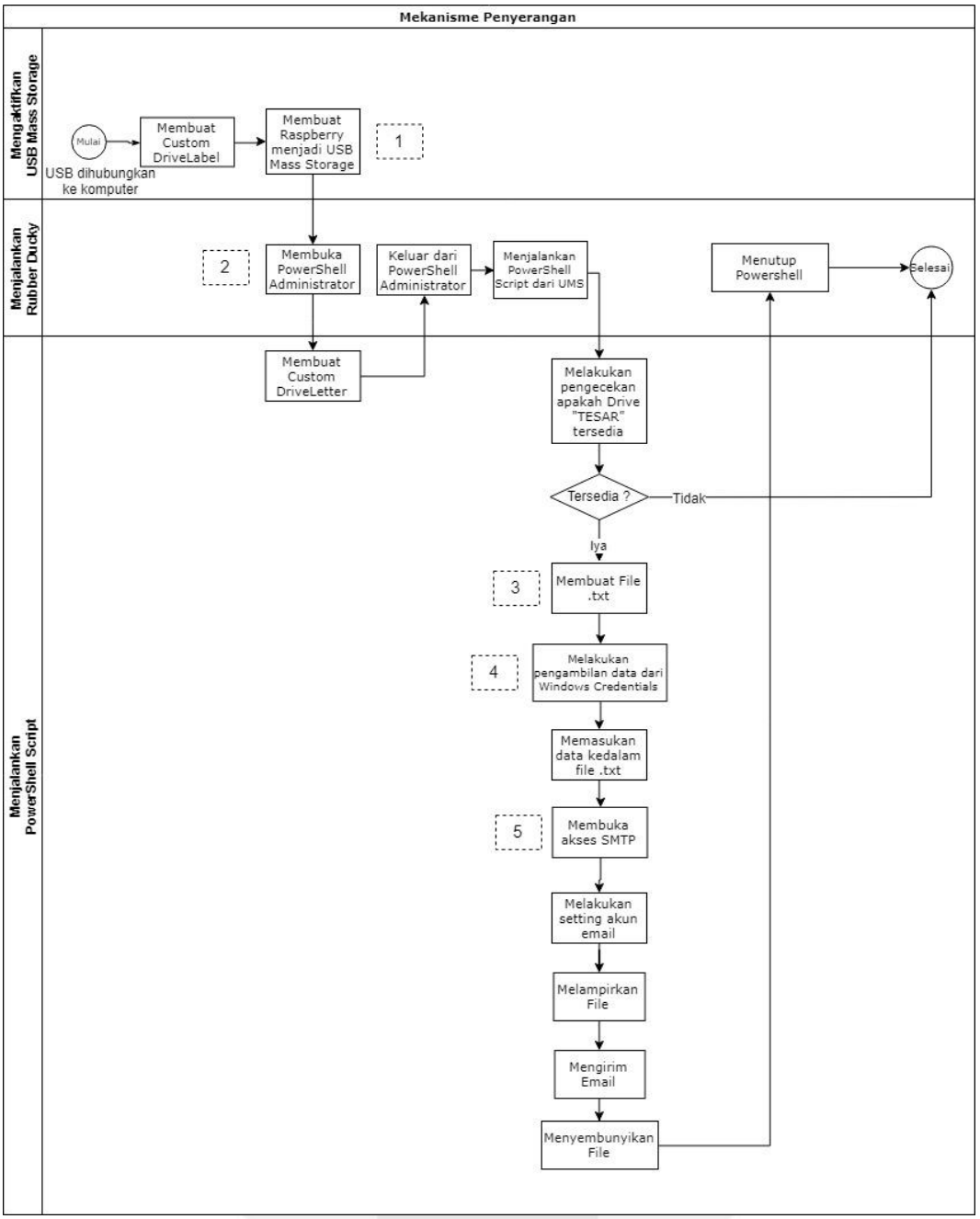
3.2. Mekanisme Penyerangan

Pada penelitian ini terbagi menjadi 3 proses utama, yaitu :

1. Mengaktifkan *USB Mass Storage*
   Menjadikan *Raspberry Pi Zero W* sebagai USB *Mass Storage* atau yang dikenal sebagai flashdisk.
2. Menjalankan *Ducky script*
   Menjalankan *Rubber Ducky* dari file *Ducky script* yang sudah dikonfigurasi untuk menjalankan fungsi *custom drive letter* dan menjalankan *Powershell script.*
3. Menjalankan *Powershell script*
   Menjalankan *Powershell script* yang tersimpan untuk menjalankan fungsi pengambilan data yang tersimpan dan pengiriman hasil data yang didapatkan.

Gambar 2 mekanisme penyerangan

Pada Gambar 2 ditampilkan mengenai mekanisme penyerangan yang digunakan.



Gambar 3 Flowchart mekanisme penyerangan

Pada Gambar 3 ditampilkan mengenai *flowchart* mekanisme yang digunakan dalam penyerangan.

4. Pengembangan Sistem

4.1. Mengaktifkan USB Mass Storage

Sebelum dapat melakukan penyerangan, agar perangkat ini tidak terlihat mencurigakan bagi target, maka perangkat ini dijadikan USB *Mass Storage* atau yang dikenal dengan USB *Flashdisk*. Baris program untuk mengaktifkan USB *Mass Storage* dengan label ”TESAR" terdapat pada *file payload.txt* pada direktori *P4wnP1*.

File image.bin yang tersimpan pada P4wnP1 diubah menjadi tempat penyimpanan atau *Mass Storage.* USB *Mass Storage* ini memiliki format *file system FAT16* yang berbeda dengan USB *Mass Storage* pada umumnya. FAT16 digunakan karena saat ini sudah sedikit penggunaannya, sehingga menjadi keuntungan tersendiri untuk melakukan *custom drive letter*.

4.2. Menjalankan *Rubber Ducky script*

Baris perintah untuk menjalankan *Rubber Ducky script* terdapat pada *file* dengan nama *startps.duck* yang tersimpan pada direktori *P4wnp1*. Baris perintah *Rubber Ducky script startps.duck* berfungsi untuk melakukan

emulasi pada keyboard yang akan berjalan secara otomatis untuk melakukan aksi kombinasi keyboard tertentu yang sebelumnya sudah dilakukan konfigurasi.

Pada proses *Rubber Ducky* terdapat baris program yang berfungsi untuk membuat *custom drive letter* pada USB *Mass Storage*. Tujuan dilakukan *custom drive letter untuk* memudahkan dalam menjalankan *Powershell script* yang tersimpan dalam USB *Mass Storage. Drive Letter* yang sudah didapatkan pada komputer target, diubah menjadi ”M” untuk menghindari bentrok dalam menjalankan *Powershell script*.

Tahap akhir proses *Rubber Ducky*, dilakukan perintah untuk menjalankan Powershell script yang bernama code.ps1. Powershell script code.ps1 berfungsi untuk melakukan pengambilan data password dan username yang tersimpan. File code.ps1 sudah dilakukan konfigurasi terlebih dahulu dan tersimpan pada USB Mass Storage. Powershell script code.ps1 akan berjalan pada background atau tidak terlihat pada layar komputer target karena dijalankan dengan perintah “-windowstyle hidden”.

4.3. Menjalankan *Powershell script*

Pada bagian ini, dijalankan *Powershell script* dengan nama *code.ps1* yang sudah dikonfigurasi dan tersimpan pada USB *Mass Storage*. Mekanisme kerja dari dari *Powershell script* yang dijalankan adalah pada awalnya akan membaca apakah terdapat USB *Mass Storage* dengan label ”TESAR”. Setelah ditemukan maka dibuat *variable* $dl yang berisi lokasi direktori dari ”TESAR” yang digunakan untuk lokasi penyimpanan *file* teks. Proses selanjutnya yaitu pembuatan variable $*filename* yang berisi *variable* $dl dan nama *file* teks dengan format nama *file* ”*computername*” + ”*username*” .txt

Setelah file berhasil terbentuk maka dilanjutkan dengan pengambilan data *password* dan *username* dari *Microsoft Edge* dan *Internet Explorer* dengan menggunakan *method RetrieveAll()* untuk melakukan pengambilan data yang tersimpan secara menyeluruh. Data yang berhasil didapatkan selanjutnya disimpan pada *file* teks yang sebelumnya sudah dibuat pada variable $*filename*.

Setelah keseluruhan proses diatas telah selesai, maka masuk ke proses pengiriman langsung melalui *email* yaitu dengan membuka akses *port* SMTP. Setelah itu mendaftarkan *email* dan *password* dari pengirim dan mendaftarkan *email* penerima, *subject*, *body* dan melampirkan *file* yang tersimpan pada *variable* $*filename*. Setelah semua proses pengiriman file melalui email telah selesai, maka file tersebut selanjutnya akan langsung disembunyikan / hidden sehingga tidak terlihat oleh user.

Pengujian ini akan dilakukan dengan 6 skenario yang berbeda, yaitu pengambilan data tanpa ada username dan password yang tersimpan, dengan kondisi terdapat password yang tersimpan dengan jumlah 5 huruf, dengan kondisi terdapat password dengan jumlah 10 karakter, dengan kondisi password dalam jumlah 15 karakter dengan kombinasi huruf, angka dan simbol, dengan kondisi terdapat 10 *username* dan *password* yang tersimpan dengan kombinasi yang beragam, dan dengan kondisi komputer target tidak terhubung dengan jaringan internet.

5. Analisis

5.1. Analisis Rubber Ducky

Dari hasil pengujian, *Rubber Ducky* berhasil berjalan sesuai dengan perintah yang ditentukan. Tetapi *Rubber Ducky* memiliki hambatan dalam melakukan penyerangan yaitu *Rubber Ducky* menggunakan *delay* yang menjadi jarak waktu antara perintah satu dengan perintah selanjutnya. Pada pengujian ini, disimulasikan penyerangan terhadap komputer laptop DELL Inspiron 3476. Proses *Rubber Ducky* berjalan dengan baik dan membutuhkan total waktu *delay* sebanyak 8.5 detik dengan *delay* tercepat yaitu 0.5 detik dan *delay* terpanjang yaitu 3 detik.

Pada pengujian dengan skenario kedua dilakukan proses *Rubber Ducky* dengan kondisi komputer terdapat aktifitas yang sedang dilakukan oleh pengguna. Aktifitas tersebut dapat berupa penggunaan komputer dengan melakukan perintah terhadap perangkat *keyboard* atau *mouse.*

Hasil dari pengujian dengan skenario kedua, didapatkan bahwa proses *Rubber Ducky* akan terganggu dan berpeluang tidak berhasil dilakukan karena adanya konflik antara perintah *Rubber Ducky* yang sudah dikonfigurasi dengan perintah yang dilakukan oleh pengguna.

Dari pengujian yang sudah dilakukan dengan dua skenario, didapatkan hasil bahwa penerapan *Rubber Ducky* terdapat kekurangan yang memiliki risiko *Rubber Ducky* tidak berhasil dilakukan yaitu penggunaan *delay* yang harus disesuaikan dengan komputer target dan apabila komputer sedang dalam kondisi digunakan, perintah *Rubber Ducky* akan mengalami konflik dengan perintah yang dijalankan oleh pengguna yang mengakibatkan perintah yang sudah dikonfigurasi menjadi terganggu.

5.2. Analisis *USB Mass Storage*

Pada pengujian ini *Raspberry Pi Zero W* menjadi perangkat penyimpanan data yang diciptakan untuk membuat target penyerangan tidak curiga saat penyerangan dilakukan. USB *Mass Storage* yang diaktifkan berasal dari *file image.bin* yang tersimpan pada direktori P4wnp1. USB *Mass Storage* memiliki format *file system* FAT16 dan memiliki kapasitas 128 MB. Kapasitas tersebut untuk saat ini belum bisa desuaikan dengan

keinginan kita, dikarenakan repositori untuk *file image.bin* masih dikunci oleh pengembang nya yaitu Mame82. Hal tersebut yang menjadi kekurangan dalam penerapan USB *Mass Storage* pada penelitian kali ini.

5.3. Analisis Pengambilan Data

Pengambilan data *password* dan *username* yang tersimpan dilakukan melalui Powershell. Powershell memungkinkan akses langsung terhadap *Credential Manager* dengan menggunakan *Method* yang dimiliki *API Credential Locker* yaitu *PasswordVault.RetrieveAll()* yang memungkinkan untuk melakukan pengambilan data yang tersimpan secara keseluruhan.

Dari hasil pengujian dengan enam skenario dapat disimpulkan bahwa penyerangan menggunakan *Powershell dengan method PasswordVault.RetrieveAll()* berhasil bekerja dengan baik dengan kondisi terdapat kombinasi yang beragam dan data *username* dan *password* yang tersimpan tidak dalam kondisi yang terenkripsi. Hal tersebut dikarenakan *method PasswordVault.RetrieveAll()* melakukan pengambilan seluruh *username* dan *password* yang tersimpan pada *browser Microsoft Edge* dan *Internet Explorer.*

5.4. Analisis Custom Drive Letter

Custom drive letter merupakan solusi dari masalah yang terjadi, dengan digunakan nya *custom drive letter*, maka kita dapat menyesuaikan *Drive letter* untuk USB *Mass Storage* dengan perintah yang digunakan untuk menjalankan *Powershell script*. Sehingga lokasi file *Powershell script code.ps1* tidak berubah dan perintah untuk menjalankan *Powershell script* dapat bekerja dengan baik.

Custom drive letter yang dilakukan akan mengubah *drive letter* yang didapatkan dari komputer target, menjadi *drive letter* "M". Alasan dipilihnya *drive letter* "M" karena kemungkinan jumlah partisi dan perangkat penyimpanan yang terdapat pada komputer target tidak melebihi dari 10 buah, dan *drive letter* partisi *default* dari *Windows* akan mulai dari *drive letter* "C". Kekurangan yang dimiliki saat ini adalah jika proses *Rubber Ducky* tidak berjalan dengan seharusnya yang menyebabkan *custom drive letter* tidak berhasil dilakukan.

5.5. Rekomendasi Untuk Meminimalisir Terjadinya Pengambilan Data Oleh Penyerang

Dari hasil penelitian dengan melakukan penyerangan pengambilan data *username* dan *password* yang tersimpan pada *browser Microsoft Edge* dan *Internet Explorer*. Didapatkan hasil dimana *username* dan *password* yang tersimpan dapat terambil secara menyeluruh.

Rekomendasi untuk meminimalisir terjadinya serangan dapat dilihat dari dua aspek yang berbeda. yaitu seperti berikut :

A. *Users*
- Menghindari perangkat komputer dihubungkan terhadap perangkat USB yang mencurigakan.
- Segera melepas perangkat USB yang terhubung apabila terdapat kapasitas USB *Mass Storage* yang tidak wajar dan apabila terdapat program yang berjalan secara otomatis tanpa dijalankan oleh pengguna.

B. *Systems*
- Melakukan *disable USB Drives & Mass Storage Devices* menggunakan *Windows Registry.*
- Melakukan *Uninstall USB Mass Storage Drivers.*

6. Kesimpulan

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

1. *Platform* penyerangan *P4wnP1* terpasang pada perangkat *Raspberry Pi Zero W* yang disimulasikan dengan bentuk yang menyerupai perangkat USB *Flash Drive*. Saat *Raspberry Pi Zero W* terpasang pada komputer target, akan terdeteksi sebagai perangkat USB *Mass Storage* dan akan menjalankan perintah *Rubber Ducky*. Penelitian ini menggunakan fungsi *Rubber Ducky* yang digunakan untuk membuat *Custom Drive letter*, dan menjalankan *Powershell script*.
2. Penggunaan *Powershell dengan method PasswordVault.RetrieveAll()* digunakan untuk melakukan pengambilan data *username* dan *password* secara menyeluruh yang terdapat pada *Credential Locker*. Pengujian pengambilan data *username* dan *password* yang tersimpan dilaksanakan dengan 6 skenario yang memiliki beragam kombinasi *username* dan *password* dapat 100% berhasil dilakukan.
3. Rekomendasi untuk meminimalisir terjadinya serangan dapat dilihat dari dua aspek yang berbeda. yaitu seperti berikut :
   a. *Users*
      - Menghindari perangkat komputer dihubungkan terhadap perangkat USB yang mencurigakan.
      - Segera melepas perangkat USB yang terhubung apabila terdapat kapasitas USB *Mass Storage* yang tidak wajar dan apabila terdapat program yang berjalan secara otomatis tanpa dijalankan oleh pengguna.

b. Systems

- Melakukan *disable USB Drives & Mass Storage Devices* menggunakan *Windows Registry*.
- Melakukan *Uninstall USB Mass Storage Drivers.*

7. Saran

Untuk penelitian lebih lanjut, terdapat saran-saran yang dapat membantu untuk pengembangan penelitian selanjutnya yaitu :

1. Melanjutkan pengujian USB *Mass Storage* dengan melakukan komunikasi dengan pengembang dari *P4wnP1* agar mendapatkan akses terhadap repositori sehingga bisa mengatur kapasitas dari USB *Mass Storage.*
2. Menggabungkan penyerangan pengambilan data *username* dan *password* yang tersimpan pada *browser* dengan fitur *Windows Lockpicker* yang terdapat pada P4wnP1.

Daftar Pustaka:

[1] Statcounter, "Desktop Operating System Market Share Worldwide - October 2018," November 2018. [Online]. Available: http://gs.statcounter.com/os-market-share/desktop/worldwide. [Diakses 18 November 2018].

[2] Symantec, The Increased Use Of Powershell In Attacks, 2016.

[3] E. Bott, "ZDNet," 25 April 2018. [Online]. Available: https://www.zdnet.com/article/in-the-new-browser-war-microsoft-edge-is-losing-internet-explorer/.

[4] Windows, "Windows Dev Center," 02 06 2019. [Online]. Available: https://docs.microsoft.com/en-us/uwp/api/windows.security.credentials.passwordvault.retrieveall#Windows_Security_Credentials_PasswordVault_RetrieveAll.

[5] C. Wueest, "PowerShell Threats Grow Further and Operate in Plain Sight," 16 July 2018. [Online]. Available: https://www.symantec.com/blogs/threat-intelligence/powershell-threats-grow-further-and-operate-plain-sight.

[6] Mame82, "P4wnp1," Februari 2017. [Online]. Available: Https://Github.Com/Mame82/P4wnp1. [Diakses 25 September 2018].

[7] RaspberryPi, "About Us," 20 April 2019. [Online]. Available: https://www.raspberrypi.org/about/.

[8] R. Grimmett, Getting Started with Raspberry Pi Zero, Packt, 2016.

[9] R. Murray, *A Raspberry Pi Attacking Guide,* 2017.

[10] J. Aiello , D. Coulter, J. P. Jofre dan S. , "Getting Started with Windows PowerShell," 05 Juni 2017. [Online]. Available: https://docs.microsoft.com/en-us/powershell/scripting/getting-started/getting-started-with-windows-powershell?view=powershell-6.

[11] R. R. Fadhilah, "Definisi Sistem Operasi," 2017.

[12] C. Hope, "USB," 5 April 2019. [Online]. Available: https://www.computerhope.com/jargon/u/usb.htm.

[13] J. Susanto, I. dan T. Rismawan , "Jurnal Coding, Sistem Komputer Untan Volume 04, No.2," *Aplikasi Enkripsi Dan Dekripsi Untuk Keamanan Dokumen Menggunakan Triple Des Dengan Memanfaatkan Usb Flash Drive,* 2016.

[14] Mame82, "P4wnp1," 2017. [Online]. Available: Https://Github.Com/Mame82/P4wnp1. [Diakses 25 September 2018].

[15] B. Cannols dan A. Ghafarian , "Systemics, Cybernetics And Informatics Volume 15," *Hacking Experiment by Using USB Rubber Ducky Scripting,* 2007.