IMPLEMENTASI DAN ANALISIS BADUSB EVILDUINO DENGAN MENGGUNAKAN ARDUINO PRO MICRO PADA SISTEM OPERASI WINDOWS

IMPLEMENTATION AND ANALYSIS OF BADUSB EVILDUINO USING ARDUINO PRO MICRO IN WINDOWS OPERATING SYSTEMS

Prima Posma Ryan[1], Avon Budiono[2], Ahmad Almaarif[3]

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

Abstrak

Sistem operasi *Windows* merupakan sistem operasi yang umum digunakan oleh banyak orang. *Universal Serial Bus* (USB) merupakan salah satu mekanisme yang digunakan oleh banyak orang dengan fungsionalitas *plug and play* yang praktis, menjadikan transfer data yang cepat dan mudah dibandingkan dengan perangkat keras lainnya. Pada penggunaannya, *Windows* memiliki kelemahan yaitu dengan mudahnya pengguna mengalami eksploitasi terhadap komputer/laptopnya. Ada metode bernama *Evilduino* yang memungkinkan untuk seseorang melakukan penanaman *backdoor reverse shell* dan eksploitasi *file* hanya dengan menghubungkan USB ke komputer target tanpa diketahui. Pada penelitian ini bertujuan untuk mengimplementasikan dan menganalisis dampak dari penyerangan yang dilakukan *BadUSB Evilduino*. Penelitian dilakukan untuk melihat apakah penanaman *backdoor reverse shell* dan eksploitasi *file* pada komputer target dengan menggunakan *BadUSB Evilduino* dapat dilakukan atau tidak. Hasil yang didapatkan adalah pengujian *backdoor reverse shell* menggunakan *Evilduino* yang dilakukan pada sistem operasi *Windows* 73% berhasil dilakukan.

Kata Kunci: BadUSB, *Universal Serial Bus* (USB), *reverse shell, backdoor,* eksploitasi *file*, Evilduino.

Abstract

The Windows operating system is an operating system commonly used by many people. Universal Serial Bus (USB) is one of the mechanisms used by many people with practical plug and play functionality, making data transfer fast and easy compared to other hardware devices. In this easy time, a method called Evilduino that allows someone to plant a reverse shell backdoor and exploit important files simply by connecting USB to the target computer without being noticed. This study aims to implement and analyze BadUSB Evilduino. The study was conducted to see whether planting a back shell backdoor and exploiting files on the target computer using BadUSB Eviluino can be done or not. Recommendations are also given to prevent attacks based on the results of tests conducted. The results obtained were planting a back shell backdoor and exploiting important files on the target computer using BadUSB Evilduino successfully.

Keywords: BadUSB, *Universal Serial Bus* (USB), *reverse shell, backdoor, file exploitation*, Evilduino.

1. Pendahuluan

Di era perkembangan digital yang sangat pesat ini, pemindahan data dari satu perangkat ke perangkat lainnya dapat dilakukan dengan mudah. Pengguna teknologi dapat melakukannya dengan memanfaatkan perangkat Universal Serial Bus (USB), arsitektur jaringan menggunakan kabel, maupun nirkabel. USB menawarkan fleksibilitas yang telah banyak diperlukan untuk menunjang kegiatan pekerjaan sehari-hari, namun dengan setiap keunggulan ada kekurangannya masing-masing. Kemudahan tersebut menimbulkan celah pengambilan data menggunakan USB yang dapat dilakukan oleh oknum yang tidak bertanggung jawab.

Penyerang yang menggunakan USB sebagai media untuk melakukan penyerangan, dapat melakukan kegiatan yang meliputi kemampuan mengirim, memasang dan menjalankan malware, menanamkan backdoor reverse shell, dan menjalankan program jahat dengan interaksi pengguna terhadap sistem. Penanaman backdoor reverse shell dapat dengan mudah dilakukan pada sistem operasi Windows. Sistem operasi yang telah dipakai banyak orang tersebut masih memiliki celah keamanan yang masih harus dibenahi, celah yang dimanfaatkan pada penelitian ini adalah masih mudahnya akses Windows Registry oleh pengguna yang tidak memiliki otoritas pada komputer yang bukan miliknya. Hanya dengan memiliki akses admin Command Prompt (CMD) pada komputer target, penyerang telah dapat melakukan perubahan value Registry pada komputer target.

Pada perusahaan besar seperti IBM, penggunaan perangkat USB sudah tidak diperbolehkan karena potensinya yang tinggi untuk digunakan sebagai alat Social Engineering Attack, berupa peretasan atau untuk menyebar malware ke dalam internal perusahaan (BBC, 2018). Ada berbagai macam metode yang dapat dilakukan penyerang untuk melancarkan serangannya menggunakan USB pada PC/laptop target diantaranya adalah USBdriveby, USBee Attack,

dan Evilduino (Nissim, Yahalom, & Elovici, 2017), oleh karena itu sudah banyak orang yang diperingatkan untuk tidak menghubungkan perangkat penyimpanan dan/atau perangkat USB lainnya yang bukan miliknya sendiri ke perangkatnya masing-masing.

Pada penelitian ini membahas metode penyerangan menggunakan perangkat Mikrokontroler yang nantinya akan dijadikan sebagai perangkat BadUSB yang bernama Evilduino. Dengan mengetahui metode tersebut, pada penilitian ini juga diharapkan bisa mengetahui dampak dari penyerangan penanaman backdoor reverse shell dan eksploitasi file yang dilakukan. Evilduino merupakan salah satu metode penyerangan yang dikembangkan oleh Rashid Feroz dan metode ini berbasis Mikrokontroler Arduino (Nissim, Yahalom, & Elovici, 2017). Evilduino digunakan untuk mengemulasikan keyboard atau mouse dan dapat mengirim keystroke atau gerakan kursor mouse ke host sesuai dengan baris kode yang telah dimuat. Dengan adanya penelitian ini diharapkan dapat mengetahui dampak dari penyerangan melalui perangkat USB dengan menggunakan metode Evilduino terhadap sistem operasi Microsoft Windows.

2. Dasar Teori

2.1. Evilduino

Evilduino adalah Trojan perangkat keras USB yang dikembangkan oleh Rashid Feroz dan didasarkan pada mikrokontroler Arduino, berbeda dengan serangan Programmable HID USB Keyboard/Mouse Dongle / Universal RF USB Keyboard Emulation Device (PHUKD / URFUKED) yang didasarkan pada mikrokontroler Teensy (Nissim, Yahalom, & Elovici, 2017). Evilduino mengemulasi keyboard/mouse dan dapat mengirim penekanan tombol/gerakan kursor mouse ke host sesuai dengan script yang dimuat sebelumnya. Pada penelitian ini, penulis hanya mengemulasikan keyboard saja untuk melancarkan penyerangan ke komputer target. Evilduino ini cukup untuk menjadi pilihan metode yang tepat untuk pembuatan perangkat BadUSB, karena mekanisme perancangan perangkat tersebut cukup mudah, (Nissim, Yahalom, & Elovici, 2017) dan juga mikrokontroler Arduino dapat dibeli secara online dengan harga yang jauh lebih murah dibandingkan dengan perangkat Rubber Ducky dan Teensy yang jauh lebih mahal.

2.2. Powershell

Powershell adalah environment command line baru bagi Microsoft Windows. Powershell dibangun dengan tujuan untuk menyediakan environment shell scripting yang terbaik untuk Microsoft Windows, bukan hanya itu tetapi untuk menghasilkan environment yang dirancang khusus hanya untuk Windows. [3] Tidak seperti shell pada umumnya, yang hanya menerima dan mengembalikan teks, Powershell dibangun pada runtime bahasa .NET, dan dapat menerima dan mengembalikan objek framework .NET. Perubahan mendasar pada environment ini membawa metode yang sepenuhnya baru dalam melakukan pengelolaan dan konfigurasi pada Windows. [4]

2.3. Sistem Operasi

Menurut Hariyanto Sistem Operasi adalah program yang bekerja sebagai perantara antara *brainware* dan *hardware* komputer. [5] Maksud dari sistem operasi adalah kumpulan perangkat lunak yang menjadi pengelola terhadap sumber daya perangkat keras komputer yang ada pada suatu komputer dan menyediakan layanan umum untuk komputer. Sistem operasi merupakan bagian penting dari sistem dalam komputer. Program aplikasi pada umumnya membutuhkan sistem operasi agar bisa berfungsi. Sistem operasi juga berperan untuk membagi waktu dalam pengeksekusian *task* dan penggunaan sistem yang baik. Untuk fungsi perangkat keras seperti *input, output,* dan alokasi memori, sistem operasi berperan sebagai penghubung antara program dan perangkat keras komputer untuk mengaturnya. Sistem operasi dapat ditemukan di hampir semua perangkat yang berdasar komputer seperti telepon seluler, konsol permainan, superkomputer, dan *web server*.

2.4. *Universal Serial Bus* (USB)

USB adalah standar bus serial untuk perangkat penghubung, biasanya menjadi perangkat penghubung kepada komputer namun juga sering ditemui pada perangkat lainnya seperti konsol permainan, ponsel dan PDA [6]. Desain USB ditujukan untuk memudahkan pengalaman plug-and-play dengan memperbolehkan petukaran data ke sistem tanpa perlu melakukan *reboot* pada komputer. Ketika USB dihubungkan ke komputer, komputer bisa langsung mengenal dan melakukan pemrosesan pada driver yang diperlukan USB untuk dapat digunakan di komputer tersebut. Selain untuk melakukan pertukaran data, USB juga dapa menghubungkan peralatan tambahan komputer seperti *mouse, keyboard,* pemindai gambar, kamera digital, *printer, harddisk,* dan perangkat-perangkat jaringan. Kini USB telah menjadi standar penghubung bagi peralatan seperti pemindai gambar dan kamera digital.

2.5. Netcat

Netcat adalah program jaringan yang dirancang untuk dapat mengakses data di kedua koneksi seperti *Transmission Control Protocol* (TCP) dan *User Datagram Protocol* (UDP) menggunakan TCP / Internet Protocol (IP). Netcat sering disebut sebagai "*Swiss Army Knife of Networking*" karena begitu banyak fitur yang bisa digunakan dari *tools* ini untuk keperluan baik maupun keperluan yang dapat merugikan orang lain. Fitur yang ada pada *Netcat* antara lain seperti; *port scanning* transfer *file, banner grabbing, port listening and redirection,* dan yang digunakan pada penelitian ini adalah *backdoor*. [7] Seperti sudah disinggung sebelumnya bahwa fitur yang digunakan pada penelitian ini adalah fitur *backdoor*. Fitur *backdoor* yang digunakan tidak sepenuhnya menggunakan fitur yang ada pada Netcat. Pada penelitian ini penyerang juga memanfaatkan *Windows Registry* yang ada di dalam sistem operasi

Windows untuk melancarkan serangannya dalam penanaman *backdoor* pada komputer target.

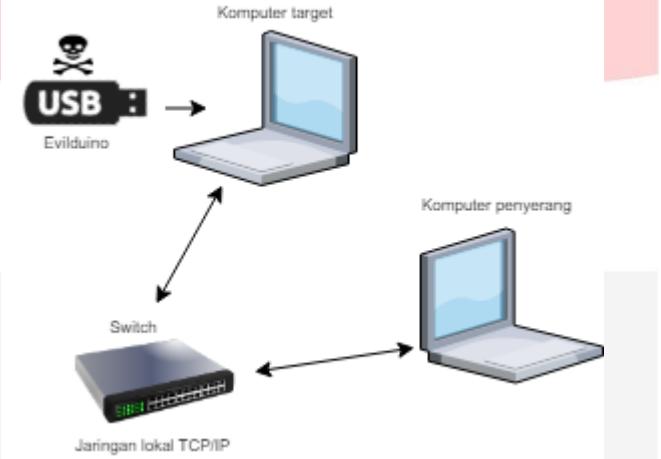
2.6. Windows Registry

Registry adalah sebuah pusat repositori yang berguna untuk sistem operasi Windows dan hampir sebagian besar program yang ada di dalamnya. [8] *Registry* berisikan informasi yang sangat banyak, dapat dikatakan *Registry* berisikan semua informasi dari sistem operasi Windows. Semua informasi yang dikandung dalam *Registry* merupakan bagian dari pengendali program aplikasi yang terpasang di sistem. Saat *Registry* tidak terkonfigurasi dengan baik, maka dapat dikatakan sistem Windows mengalami cacat. Jika hal tersebut terjadi maka akan berpengaruh juga terhadap kinerja sistem operasi Windows.

3. Pembahasan

3.1. Perancangan Sistem

Dalam proses implementasi diperlukan perangkat pendukung untuk melakukannya, seperti perangkat lunak dan perangkat keras. Oleh karena itu dilakukan identifikasi arsitektur perangkat yang diperlukan yang terdiri dari *hardware* dan *software*.



Gambar 1 Perancangan Sistem

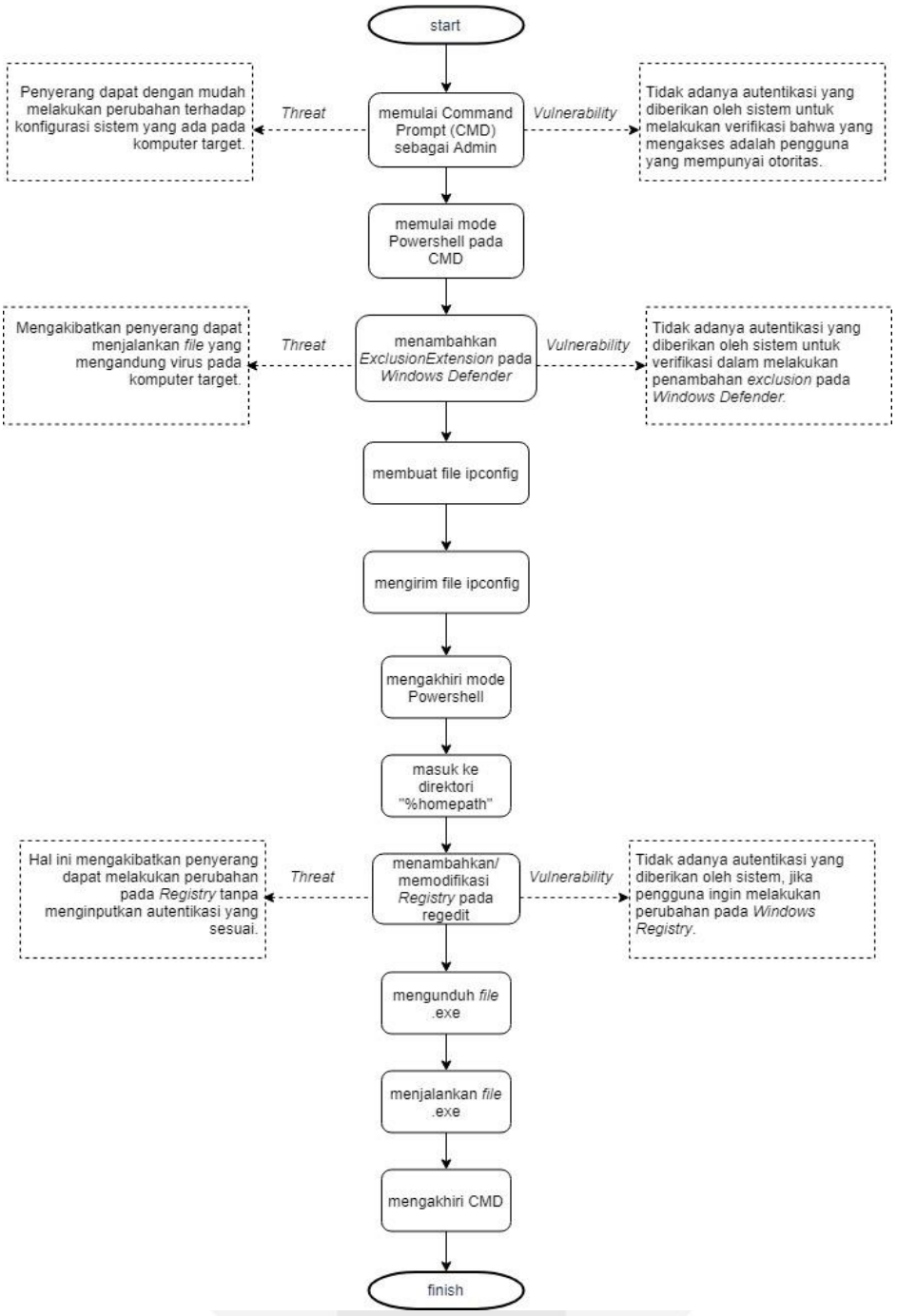
Pada gambar 1 ditampilkan ilustrasi penyerangan yang dapat dilakukan oleh penyerang pada komputer target. Penyerangan diawali dengan menghubungkan Evilduino ke komputer target. Setelah itu Evilduino akan bekerja secara otomatis dengan melakukan emulasi terhadap *keyboard* pada komputer target. Emulasi yang dilakukan adalah berdasarkan baris kode yang disematkan oleh penyerang ke dalam Evilduino. Jika Evilduino telah selesai menjalankan baris kodenya, maka setelah itu penyerang telah dapat melakukan eksploitasi dengan cara menelurkan *Command Prompt* (CMD) komputer target pada komputernya.

3.2. Skenario Penyerangan

1. Membuat *exclusion* pada Windows Defender
   Hal ini dilakukan agar *file* yang dibutuhkan untuk melakukan penyerangan dapat berjalan pada komputer target.
2. Menambahkan registry pada komputer target
   Add registry yang dilakukan bertujuan untuk menanamkan *backdoor Reverse Shell*, menonaktifkan *User Account Control* (UAC), dan menonaktifkan *Password Portected Sharing* pada komputer target.
3. Mengunduh *file* .exe
   Mengunduh *file* .exe dari internet yang nantinya akan dijalankan pada komputer target.
4. Menjalankan *file* .exe
   Mengeksekusi *file* .exe yang berguna untuk menambahkan *registry* baru pada *registry editor* komputer target.
5. Eksploitasi sistem melalui *Command Prompt* (CMD)
   Melakukan eksploitasi sistem pada komputer target.

4. Pengembangan Sistem

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



Gambar 2 Mekanisme penyerangan

4.1. Membuat *Exclusion* pada *Windows Defender*

Agar dapat melakukan penyerangan pada target, penyerang terlebih dahulu harus membuat pengecualian *file extension* pada Windows Defender di komputer target. Hal tersebut perlu dilakukan agar *file* yang nantinya dibutuhkan untuk melakukan penyerangan tetap dapat digunakan dan tidak dideteksi oleh Windows Defender. Ekstensi yang dijadikan pengecualian pada *windows defender* adalah ekstensi *file* .exe.

4.2. Mengirimkan Informasi Jaringan

Pada bagian ini dijelaskan bagiamana cara agar dapat mengetahui informasi jaringan yang ada pada komputer target, informasi yang dibutuhkan adalah IP *address*. Penyerang melakukan hal tersebut dengan cara menginputkan hasil dari perintah "ipconfig" dari Command Prompt (CMD) yang berisikan konfigurasi jaringan yang terpasang pada komputer target ke dalam *file* baru yang bernama ipconfig.txt.

4.3. Menambahkan Registry Pada Komputer Target

Pada tahap ini, dilakukan penambahan *registry* baru dan modifikasi pada *registry editor* komputer target. Hal tersebut dilakukan dengan tujuan untuk menanamkan *backdoor reverse shell*, dan menonaktifkan *User Account Control* (UAC) serta *restrictanonymous* pada komputer target. Dua hal tersebut bertujuan untuk memungkinkan penyerang melakukan serangan.

4.4. Mengunduh File .exe

Pada penelitian ini dibutuhkan *file* berekstensi .exe yang digunakan untuk melakukan penyerangan awal pada komputer target. *File* .exe yang digunakan pada penelitian ini dibuat menggunakan aplikasi WinRAR. Tujuan pembuatan *file* tersebut adalah untuk membangun penyerangan pada tahap awal saat Evilduino dihubungkan pada komputer target. *File* .exe yang digunakan harus diunduh terlebih dahulu menggunakan jaringan internet yang ada pada komputer target, *file* .exe tersebut sebelumnya telah diunggah oleh penulis ke sebuah layanan *file hosting* yang bernama *Mediafire.* Pada penelitian ini pengunduhan dilakukan melalui *command line* yang ada pada komputer target yaitu Command Prompt (CMD).

4.5. Menjalankan File .exe

Pada tahap ini, dilakukan eksekusi pada *file* .exe yang telah diunduh sebelumnya. File tersebut berguna untuk mengekstrak *file* nc.exe ke folder ”%homepath%” dan juga untuk melakukan penyerangan awal dengan mengeksekusi baris kode “nc.exe -vv -d -L -p 4444 -e cmd.exe”.

4.6. Eksploitasi Sistem Melalui Command Prompt (CMD)

Pada bagian ini, penyerang akan menghubungkan Command Prompt (CMD) miliknya ke CMD milik target. Jika hal tersebut telah berhasil dilakukan maka penyerang dapat melakukan eksploitasi seperti mengakses *file* yang ada pada komputer target tanpa terdeteksi. Serangan lain yang dapat dilakukan cukup beragam diantaranya seperti; *read/write file* atau folder, pencarian dokumen penting, melakukan format drive, mengubah pengaturan partisi, dan memodifikasi *Registry Editor*.

5. Analisis

5.1. Analisis Pengujian Backdoor Pada Saat Evilduino Tehubung

Reverse Shell merupakan sebuah mekanisme penyerangan pada penelitian ini yang berguna untuk mendapatkan *shell*/CMD komputer target dan menggunakannya pada komputer penyerang. Dari hasil pengujian yang telah dijalankan, penanaman *backdoor reverse shell* berhasil dilakukan setelah menghubungkan Evilduino pada komputer target. Selama Evilduino tetap terhubung pada komputer target, penyerang tetap bisa melakukan penyerangan *reverse shell* ke komputer target.

5.2. Analisis Pengujian Backdoor Saat Evilduino Sudah Tidak Terhubung

Penanaman *backdoor reverse shell* yang sudah dilakukan bertujuan untuk memungkinkan penyerang dapat kembali mengakses *shell*/CMD setelah Evilduino sudah tidak terhubung pada komputer target, ataupun setelah komputer target melakukan *restart* atau menyalakan kembali.

5.3. Rekomendasi Untuk Meminimalisir Terjadinya Serangan

Berdasarkan hasil penelitian eksploitasi komputer target dengan menggunakan reverse shell, peneliti mendapatkan hasil bahwa penyerang dapat mengakses file yang ada pada komputer target dengan mudah.

Rekomendasi untuk mencegah terjadinya serangan seperti itu terbagi menjadi dua aspek, yaitu:

1. Pengguna:
   - Mencegah perangkat USB yang mencurigakan untuk terhubung ke komputer pengguna.
   - Jangan meninggalkan komputer pada keadaan stand-by desktop.
2. Sistem:
   - Menggunakan anti-virus yang terbukti mumpuni untuk mengatasi penyerangan seperti penanaman backdoor pada komputer.
   - Menonaktifkan port USB pada komputer/laptop.

- Menonaktifkan port TCP 4444 agar tidak dapat diakses oleh penyerang.
- Memberikan verifikasi autentikasi untuk mengakses Windows Defender, dan Registry Editor.
- Mengaktifkan autentikasi untuk memulai sesi CMD ataupun Powershell.

6. Kesimpulan

Berdasarkan penelitian yang telah dilakukan dapat ditarik kesimpulan sebagagi berikut:

1. Pengimplementasian Evilduino pada *Arduino Pro Micro* berhasil dilakukan menggunakan *tools Arduino* IDE dengan menanamkan baris kode yang bertujuan untuk melakukan penanaman *backdoor reverse shell*.

2. Cara kerja penyerangan Evilduino dilakukan dengan memanfaatkan *keyboard* yang digunakan pada komputer target. *Keyboard* tersebut dilakukan emulasi oleh Evilduino agar menjalankan perintah sesuai dengan tujuan penyerang.

3. Dari pengujian pada penelitian ini dapat diketahui bahwa ada beberapa dampak dari penyerangan yang dilakukan pada sistem operasi *Windows*, yaitu:
   - Komputer target dapat mengalami cacat sistem, dikarenakan penyerang melakukan beberapa perubahan yang permanen pada *Windows Registry*.
   - *File* yang ada pada komputer target dapat dengan mudah diakses oleh penyerang dengan memanfaatkan fitur *Public Folder sharing*.
   - Penyerang dapat dengan mudah menyusupkan atau mengunduh langsung *file* berbahaya ke dalam komputer target.
   - Berhasil melakukan pengambilan data pribadi tanpa melakukan autentikasi.
   - Rekomendasi (control) yang diberikan pada bagian V.4 dan V.1.7.3 dapat dijadikan sebagai bahan acuan untuk melakukan pencegahan terhadap potensi serangan yang dapat dilakukan oleh Evilduino.

7. Saran

Untuk penelitian lebih lanjut, hasil pengujian maupun analisis yang telah dibuat pada penelitian ini dapat digunakan sebagai data acuan untuk melakukan penelitian yang berfokus pada dampak penyerangan yang lebih dalam lagi atau pada pengembangan penyerangan yang ingin dilakukan. Eksploitasi pada sistem operasi *Windows* dengan menggunakan BadUSB dapat diperluas dengan menggunakan mekanisme penyerangan seperti *Remote Access Trojan* (RAT), *Man in The Middle* (MiTM), dan *USB Thief.*

Daftar Pustaka:

[1] BBC, "IBM workers banned from using USB sticks - BBC News," 10 May 2018. [Online]. Available: https://www.bbc.com/news/technology-44069488.

[2] N. Nissim, R. Yahalom and Y. Elovici, *USB-Based Attacks.*, 2017.

[3] B. Payette, Windows Powershell in Action, Shelter Island: Manning Publications Co., 2011.

[4] J. Aiello, D. Coulter, J. P. Jofre and 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.

[5] D. B. Hariyanto, Sistem Operasi, Bandung: Informatika Bandung, 2009.

[6] J. Axelson, USB Complete: The Developer's Guide 5th Edition., Lakeview Research, 2015.

[7] Syngress, "Introduction to Netcat," 2013.

[8] J. Kennedy and M. Satran, "Structure of the Registry - Windows applications | Microsoft Docs," 31 5 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/desktop/sysinfo/structure-of-the-registry.