IMPLEMENTASI DAN ANALISIS *USB ATTACK* PENGAMBILAN PASSWORD UNTUK *LOGIN* PADA *PERSONAL COMPUTER* MENGGUNAKAN *WINDOWS LOCKPICKER*

IMPLEMENTATION AND ANALYSIS USB ATTACK OF PASSWORD RETRIEVAL FOR LOG IN TO A PERSONAL COMPUTER USING WINDOWS LOCKPICKER

Nico Almansya Ellsadaai[1], Avon Budiono[2], Ahmad Almaarif[3]

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

Abstrak

USB memiliki kemudahan untuk terhubung pada berbagai jenis sistem operasi yang dimanfaatkan beberapa orang sebagai celah dengan dibuatnya sebuah aplikasi dengan metode khusus dapat digunakan untuk penyerangan, salah satunya *Windows* sebagai sistem operasi yang paling banyak digunakan saat ini. Sistem operasi ini memiliki kelemahan, misalnya kemudahan dalam pengambilan *hash user password* yang tersimpan pada *Windows SAM*. Sebuah metode penyerangan melalui USB bernama *Windows Lockpicker* yang berada dalam *platform P4wnP1* bertujuan bagi penyerang untuk dapat masuk sebagai *user* komputer pada posisi *locked* tanpa perlu mengetahui *password* pengguna terlebih dahulu, dengan mengambil hash yang tersimpan dan kemudian dilakukan *password cracking* untuk *login*. Penelitian ini menghasilkan kemungkinan keberhasilan 60% pemecahan *password* dari 32 skenario yang berhasil diambil *hash*nya dan juga rekomendasi yang bisa penulis berikan untuk meminimalisir terjadinya serangan.

Kata kunci : ***USB, sistem operasi, P4wnP1, Windows Lockpicker, Password Cracking***

Abstract

USB has the convenience of connecting to various types of operating systems that some people use as loopholes to create applications with special methods that can be used for attacks, for example Windows as the most widely used operating system these days. This operating system has weaknesses, such as the ease of retrieving user password hashes stored on Windows SAM. The USB attack method called Windows Lockpicker on the P4wnP1 platform aims to allow attackers to enter as computer users in a locked position without needing to know the user's password first, by retrieving the stored hash and then hacking the password to log in. This research resulted in the possibility of 60% success in completing passwords from 32 scenarios that had been successfully extracted and also recommendations that could be given by the author to minimize the occurrence of attacks.

Keywords: ***USB, operation system, P4wnP1, Windows Lockpicker, Password Cracking***

1. Pendahuluan

Dalam penggunaan komputer yang maksimal dibutuhkan alat pendukung lain yang dapat membantu dalam penggunaannya misalnya seperti USB. USB hadir untuk membuat sistem pengkabelan pada komputer menjadi lebih sederhana. Hampir setiap komputer saat ini sudah dilengkapi dengan *USB port* dengan fungsi untuk menghubungkan *hardware* berbentuk USB yang bisa digunakan pengguna misalnya untuk pemindahan maupun penyalinan data. Hal tersebut mungkin terlihat sangat sederhana, tapi terdapat adanya kemungkinan yang bisa merugikan jika perangkat USB yang kita sambungkan berisi software berbahaya [1].

Ancaman serangan dengan menggunakan USB semakin beragam saat ini. Serangan ini didasarkan pada perangkat *firmware* yang sudah dimodifikasi agar dapat memasukkan *command* berbahaya untuk menginfeksi komputer yang ditargetkan. *Command* yang digunakan tersebut dapat mengunduh *malware* dari internet atau memang sudah tertanam secara langsung pada perangkat USB. Sebagian besar *antivirus* kurang efektif dalam pencegahan serangan yang masuk melalui metode ini [2].

Sebuah *platform* baru yang bernama P4wnP1 muncul pada Februari 2017, *platform* ini berbasis serangan melalui USB dan sangat mudah untuk disesuaikan dengan kebutuhan yang diinginkan melalui sebuah *microcontroller* berupa *Raspberry Pi Zero W* [3], *platform* ini lebih terfokus untuk melakukan penyerangan pada sistem operasi *Windows*, sebab sebagai salah satu sistem operasi yang banyak digunakan pada saat ini, maka memiliki peluang yang paling besar juga sebagai target sasaran penyerangan.

Metode penyerangan *P4wnP1* memiliki jenis fungsi yang berbeda-beda, salah satunya *Windows LockPicker*, metode ini dapat efektif bekerja untuk *PC user* yang meninggalkan perangkatnya dalam kondisi *locked* atau *sleep*, sebab masih tersimpannya *cache* password yang sebelumnya digunakan oleh pemiliknya untuk melakukan *login.*

Hanya dengan menghubungkan *Raspberry Pi Zero W* pada *PC* target maka *password cracking* dapat mulai diaktifkan.

Pada penelitian ini akan membahas mengenai rincian penerapan *platform P4wnP1* dengan menfaatkan teknologi yang tertanam dalam *Raspberry Pi Zero W* dengan salah satu metodenya yaitu *Windows Lockpicker*. Metode ini digunakan oleh penyerang untuk dapat masuk sebagai pengguna tanpa perlu mengetahui *password* terlebih dahulu karena tidak diperlukannya untuk memasukkan *password* pengguna dengan sistem operasi *Windows* sebagai tujuan utamanya.

2. Dasar Teori

2.1. *Universal Serial Bus* (USB)

Universal Serial Bus merupakan salah fitur bawaan dari sebagian besar *PC*. USB diciptakan untuk menggantikan banyaknya kabel yang berada di belakang PC hanya dengan satu kabel saja. USB dikembangkan oleh industri pembuat PC diantaranya *Compaq, DEC, IBM, Intel, Microsoft, NEC, dan Northern Telecom*. USB digunakan untuk menyambungkan *hardware* misalnya *keyboard*, *mouse*, *CD-ROM*, *printer*, dan lainnya [4].

2.2. *Raspberry Pi Zero W*

Raspberry Pi Zero W merupakan sebuah *microcontroller* yang identik seperti komputer namun memiliki ukuran yang kecil dan yang terkecil dari semua jenis *Raspberry Pi*. *Raspberry Pi Zero W* sudah dilengkapi dengan *RAM*, prosesor, dan *port* pendukung untuk membantu proses *input* atau *output*nya. *Raspberry Pi Zero W* membutuhkan sistem operasi berupa *Raspbian Linux* untuk dapat menjalankan *software* dalam penggunaannya, dan juga dapat digunakannya sistem operasi lain, seperti *Windows* atau *MacOS* [5]. Jenis bahasa pemrograman yang umum dipakai pada *Raspberry Pi Zero W* adalah *Phyton*.

2.3. Sistem Operasi

Sistem operasi merupakan penghubung antara *user* dengan perangkat keras yang digunakan pada sebuah *PC* yang berfungsi sebagai *interface*. Sistem operasi bertugas untuk melakukan kontrol dan manajemen perangkat keras komputer, serta operasi dasar sistem dan menjalankan program aplikasi seperti pengolah kata, desain, musik, dan *browser*. Sistem operasi bertujuan untuk membuat komputer lebih mudah digunakan, mengefisienkan penggunaan sumber daya, dan memungkinkan untuk melakukan penerapan-penerapan baru tanpa mengganggu layanan yang sudah ada sebelumnya [6].

2.4. *P4wnP1*

P4wnP1 adalah sebuah *platform* serangan dengan menggunakan fitur *USB*. *Platform* ini pertama kali muncul pada Februari tahun 2017 dengan menargetkan tujuan utama kepada pengguna sistem operasi *Windows*. Penggunaan *platform* ini dapat mengubah sebuah *Raspberry Pi Zero W* menjadi sebuah alat *hacking* secara fisik yang bersifat sederhana [3].

2.5. *Windows LockPicker*

Windows LockPicker merupakan salah satu metode dari P4wnP1 yang berfungsi untuk dapat melakukan user login secara otomatis tanpa perlu diketahui oleh pemiliknya. Metode ini merupakan sebuah pengembangan dari penelitian *snagging creds from locked machines* oleh Rob "Mubix" Fuller dan *PoisonTap* oleh Samy Kamkar [7]. *Windows LockPicker* hanya efektif bekerja pada *PC* yang berada posisi *locked* atau *sleep*, sebab masih tersimpannya *cache password* dari sesi *login* sebelumnya yang dilakukan oleh pemiliknya.

Windows LockPicker melakukan penyerangan terhadap *Windows Credential Manager* sebagai penyimpan *cache password* pengguna yang kemudian diambil dalam bentuk *hash NetNTMLv2*. Metode ini menggunakan aplikasi pendukung lain dalam proses pengambilan dan pemecahan *password*.

2.6. *John The Ripper*

John The Ripper adalah sebuah aplikasi pemecah kata sandi yang pada saat ini tersedia untuk beberapa sistem operasi diantaranya *Windows*, *MacOS*, *Unix*, *DOS*, *BeOS*, dan *OpenVMS*. Tujuan utama dari aplikasi ini awalnya untuk mendeteksi kata sandi yang lemah yang sistem operasi *Unix*, namun saat ini pada versi "*jumbo*" mampu mendeteksi banyak jenis hash lainnya [8].

Terdapat 3 metode penyerangan yang digunakan ada aplikasi ini, yaitu *single*, *wordlist*, dan *incremental*. Pada metode *single* dan *wordlist* terjadi proses penghitungan dan pencocokan terhadap hash dengan kata sandi yang sudah tersedia atau bersifat *library*, sementara pada metode *incremental* menggunakan cara *brute force attack* [9].

2.7. Brute Force Attack

Brute force attack adalah sebuah cara atau upaya untuk memecahkan kata sandi atau menemukan kunci pada pesan yang terenkripsi. Metode ini dilakukan secara *trial* dan *error* yang kemudian dapat menebak kata sandi atau kunci dengan benar. Lama pemecahan bergantung dari tingkat kompleksitas kata sandi yang digunakan. Metode ini merupakan salah satu metode lama, tetapi dinilai masih sangat efektif untuk digunakan [10].

2.8. Hash

Hash adalah sebuah metode algoritma yang digunakan untuk mengubah data informasi berupa huruf, angka, dan karakter lainnya menjadi karakter terenkripsi. *Hash* memiliki fungsi yang dapat menerima *string* dengan jumlah karakternya bebas lalu diubah menjadi sebuah string berukuran tetap, hal ini bisa berguna untuk menyamakan besar ukuran berbagai macam *password* yang akan disimpan (Susanto, 2015).

2.9. Windows Credential Manager

Windows Credential Manager merupakan tempat dimana *user* dapat menyimpan *Credentials* berupa *username* dan *password* untuk situs web, aplikasi, maupun server yang mendukung fitur ini. *Credentials* disimpan dalam *Windows Vault* dan memungkin *user* untuk mengaksesnya dengan cepat dan mudah. Hal ini bermanfaat bagi *user* yang memiliki masalah untuk *login* dan penulisan *password.* Pengelolaan dan peyimpanan *password* yang baik sangat diperlukan agar mengurangi kemungkinan kebocoran data *password*. *Windows Credentials Manager* dapat diakses dan dikelola melalui *Control Panel* [11].

3. Pembahasan

3.1. Perancangan Sistem

Perangkat lunak dan perangkat keras dibutuhkan dalam proses implementasi penelitian ini, maka telah dilakukan identifikasi spesifikasi perangkat keras dan lunak yang sesuai dengan yang dibutuhkan.

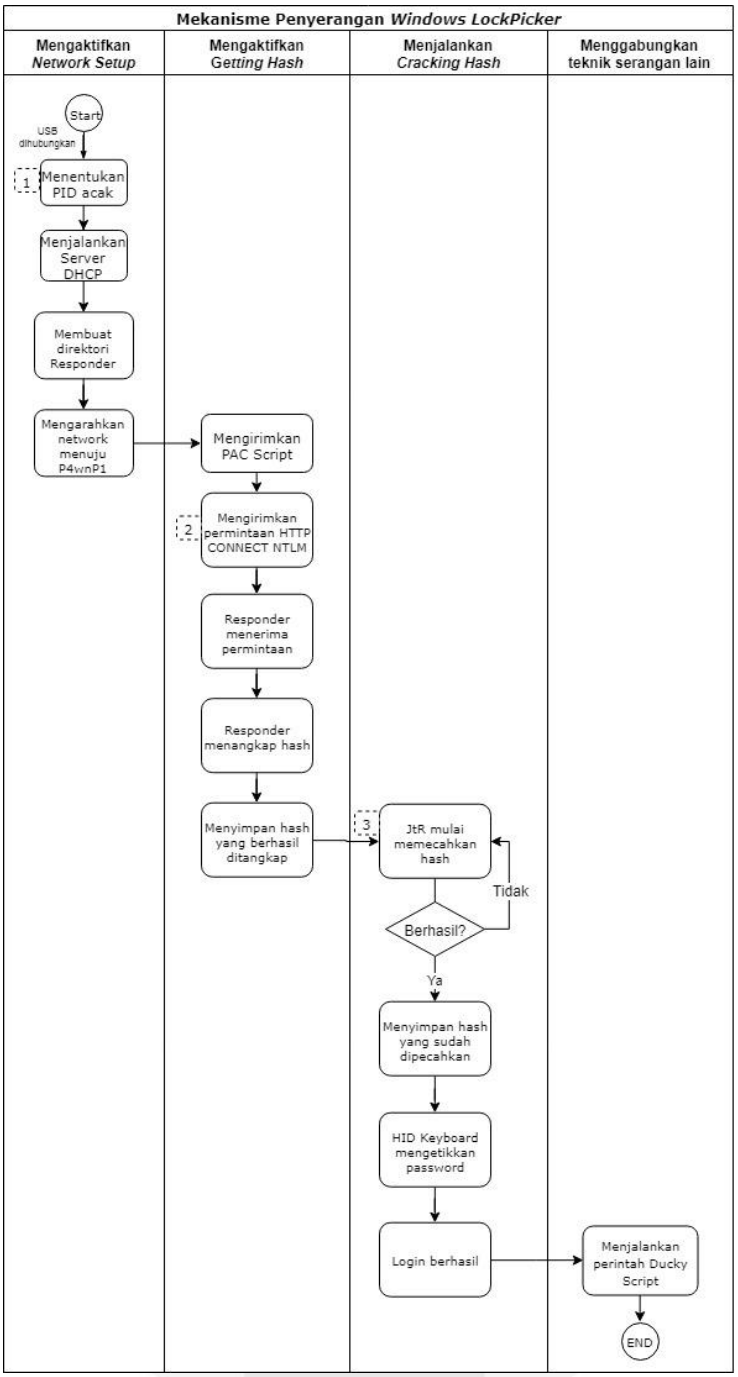
Gambar 1 Perancangan sistem

Berdasarkan Gambar 1 yang menunjukkan ilustrasi dari penyerangan, penyerangan dimulai pada saat *Raspberry Pi Zero W* yang sudah berisi baris kode *Windows LockPicker* dihubungkan pada *PC* Target melalui USB Port yang tersedia. Ketika sudah dihubungkan maka *P4wnP1* akan secara otomatis melakukan penyerangan *password cracking* terhadap *User* yang berada pada posisi *Locked*. Apabila *password cracking* berhasil dilakukan, maka akan dilanjutkan dengan menjalankan *USB Rubber Ducky* hingga selesai dan diakhiri dengan mengembalikan kembali posisi *User* pada posisi *Locked*.

3.2. Mekanisme Penyerangan

Mekanisme penyerangan pada penelitian ini terdiri dari 4 proses utama seperti pada Gambar 2 , yaitu:

1. Mengaktifkan *Network Setup*
   Mengaktifkan *Raspberry Pi Zero W* yang berisi *P4wnP1* menjadi sebuah *network* berbentuk *ethernet* agar bisa menyusupi *password* yang tersimpan pada jaringan lokal *PC* yang sedang berada pada posisi *locked* atau *sleep*.
2. Mengaktifkan *Getting Hash*
   Mengaktifkan fungsi *responder* untuk menangkap *password* yang tersimpan dalam bentuk *hash* yang didapat dari *request* yang dimasukkan. Setelah *hash* berhasil ditangkap maka *hash* akan disimpan pada direktori tersendiri.
3. Menjalankan *Cracking Hash*
   Menjalankan fungsi *John The Ripper* dalam melakukan *password cracking* terhadap *hash* yang berhasil disimpan. Jika *password cracking* berhasil maka *password* akan disimpan dalam bentuk teks pada direktori tersendiri dan kemudian *HID Keyboard* akan mengetikannya pada kolom *password*
4. Menggabungkan Teknik Serangan Lain
   Menjalankan teknik serangan lain setelah berhasil melakukan *user login* melalui *Ducky Script* yang berfungsi sebagai *virtual keyboard*. Tahap ini *Ducky Script* akan disusun untuk menjalankan aplikasi sederhana yang tersimpan *USB Mass Storage* dari *Raspberry Pi Zero W.*



Gambar 2 *Flowchart* alur penyerangan

4. Pengembangan Sistem

4.1. Mengaktifkan *Network Setup*

Penyerangan dimulai saat PC Target disambungkan dengan *Raspberry Pi Zero W* yang telah berisi *Windows LockPicker* di dalamnya, ketika sudah terhubung tugas awal dari *Windows LockPicker* adalah untuk menentukan USB VID dan PID secara acak yang berfungsi untuk membuat *Windows* percaya sedang terhubung dengan perangkat *USB Ethernet* yang selalu berbeda, sebab penyerangan terhadap target yang sama dengan menggunakan perangkat USB yang sama berakhir dengan hasil fungsi yang kurang baik dan memperlambat proses.

Dalam *Windows LockPicker terdapat* baris perintah yang berisi fungsi-fungsi dari *P4wnP1* diantaranya, RNDIS pada P4wnP1 berfungsi untuk menjalankan *network* sebagai *ethernet* untuk pengambilan *hash*, HID berfungsi sebagai *virtual keyboard* yang dapat memasukkan *password* pada kolom *password*, UMS berfungsi untuk mengaktifkan fungsi penyimpanan pada USB, CRACK berfungsi untuk menjalankan fungsi *password cracking* apabila *hash* berhasil ditangkap, LOGIN berfungsi untuk menjalankan fungsi percobaan *Login* pada *PC*, dan ROUTE_SPOOF berfungsi untuk mengarahkan semua IP pada *PC* Target mengarah ke P4wnP1.Lang

merupakan fungsi untuk mencocokkan bahasa *password* yang berguna untuk mempercepat proses. Terdapat juga baris perintah untuk menentukan IP dari P4wnP1, *Subnet Mask*-nya, dan jangkauan IP DHCP yang dapat digunakan.

4.2. Mengaktifkan *Getting Hash*

Tahap ini dimulai dengan memasukkan Protokol WPAD untuk mengatur DHCP pada P4wnP1 yang bertujuan untuk mengambil *NTLMv2 hash*. Terdapat baris perintah untuk mengaktifkan fungsi WPAD_ENTRY yang berisi *PAC Script* untuk melakukan *request HTTP Connect NTLM* untuk mendapatkan *NTLM Credential* berupa *hash*.

Fungsi *Responder* dituliskan dengan baris perintah WPAD_ENTRY untuk membuat *file* dan mengaktifkan *database responder* pada direktori *Responder* yang memiliki fungsi untuk penyimpanan bersifat sementara untuk *hash* yang berhasil ditangkap. Fungsi get_hash() berguna menangkap hash dan menyimpan pada direktori *Responder* dalam bentuk *database*. Fungsi kill_responder() berguna untuk menghentikan fungsi *responder* dalam menangkap *hash*. Fungsi onNetworkUp() berisi baris perintah pada saat lampu *led* berkedip satu kali maka sedang terjadi pengaturan *ip tables* untuk mengarahkan ulang *TCP* dan *UDP* menuju ke *P4wnP1* dan memulai untuk menyalakan *responder*. Saat *responder* sudah siap dan mulai menjalankan fungsi untuk menangkap *hash* maka lampu *led* akan berkedip 2 kali.

4.3. Menjalankan *Cracking Hash*

Tahap ini terjadi pemecahan *password* untuk dicocokan dengan *hash* yang sudah ditangkap oleh *responder* dengan bantuan aplikasi *JohnTheRipper*. Terdapat fungsi extract_password() untuk mengaktifkan fungsi *JohnTheRipper* dalam memecahkan *password.* Fungsi onTargetGotIP() berguna untuk melakukan penyimpanan *hash* yang telah diterima pada direktori "collected" yang berisi nama_user dan nama_host. Kemudian lampu *led* akan berkedip 3 kali yang menunjukkan bahwa *JohnTheRipper* sedang bekerja. Jika *password* berhasil dipecahkan maka lampu *led* akan menyala dan akan disimpan pada direktori "collected" dengan akhiran nama file ".cracked".

Terakhir fungsi onKeyboardUp() berisi baris perintah *HID Keyboard* CTRL+ALT+DEL untuk memastikan sudah siap berada layar *password input*. Kemudian lampu *led* akan mulai kembali menyala lagi dan *HID Keyboard* memulai fungsinya dalam mengetikkan *password* yang sebelumnya sudah berhasil didapatkan dilanjutkan memasukkan ENTER. Setelah semua selesai dan berhasil *login* dapat dilanjutkan ke *USB Rubber Ducky Attack*.

4.4 Menggabungkan Teknik Serangan lain

Pada proses ini terjadi penggabungan teknik serangan lain yang dapat dilakukan saat sudah berhasil *login* dengan digunakannya *Rubber Ducky Attack*. Perintah *Rubber Ducky Attack* bisa disesuaikan fungsinya dengan yang dibutuhkan melalui *script*. Pada penelitian ini *script* hanya digunakan untuk menjalankan aplikasi sederhana yang tersimpan pada *USB Mass Strorage* dari *Raspberry Pi Zero W*.

Ducky Script yang dibuat berisi baris perintah dimulai dengan membuka *powershell* sebagai *administrator* yang berfungsi untuk bisa memperoleh akses untuk melakukan perubahan pada *PC Target*. Baris perintah berikutnya berfungsi untuk melakukan *custom drive letter* terhadap *USB Mass Storage* dari *Raspberry Pi Zero W* dan menutup *powershell*. Baris perintah berikutnya berfungsi untuk *command prompt* dan mulai menjalankan aplikasi yang tersimpan pada *USB Mass Storage*. Setelah semua selesai diakhiri dengan menutup *command prompt* dan mengembalikan kembali *PC* target pada posisi *locked*. Pada posisi ini *Raspberry Pi Zero W* sudah bisa dilepas dari *PC* target dengan kondisi aplikasi yang sebelumnya dijalankan masih berproses di *PC* target.

5. Analisis

5.1. Analisis *Network Setup*

Fungsi tambahan *USB Mass Storage* diaktifkan agar *USB* yang terdeteksi tidak terlihat mencurigakan hanya muncul sebagai *USB Ethernet* dan juga bisa dimanfaatkan sebagai penyimpanan untuk membantu proses *USB Rubber Ducky Attack*. Analisis *Getting Hash*

Berdasarkan pengujian yang sudah dilakukan semua fungsi dasar dari rancangan baris kode yang ada pada *Windows Lockpicker* berjalan dengan baik pada tahap ini tidak ada terjadinya kesalahan ataupun *error*. Lama proses yang terjadi pada tahap ini berlangsung sekitar 30 detik.

5.2. Analisis *Getting Hash*

Fungsi *responder* untuk menangkap dan menyimpan *NTLMv2 hash* tahap ini berjalan dengan baik. *NTLMv2 hash* yang berada di *Windows SAM* yang merupakan bagian dari *Windows Credentials* dapat ditangkap karena *PAC Script* menjalankan fungsinya untuk melakukan *request HTTP Connect NTLM*.

Fungsi tambahan lampu *led* sangat membantu dalam mengetahui proses sudah berjalan sampai ke titik mana. Lama proses yang terjadi pada tahap ini berlangsung sekitar 17 detik.

5.3. Analisis *Cracking Hash*

Pada tahap ini dilakukan beberapa percobaan skenario untuk mengetahui tingkat keberhasilan dari *John The*

Ripper dalam melakukan *password cracking*, yaitu:

1. Kategori huruf
    a. Jumlah karakter berdasarkan kata dalam kamus
    Dari 8 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan metode *library*, memiliki peningkatan waktu setiap adanya penambahan satu huruf dan baru efektif bekerja untuk dengan maksimal jumlah karakter sebanyak tujuh huruf.
    b. Jumlah karakter berdasarkan kata tidak ada dalam kamus
    Dari 7 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan metode *brute force*, memiliki peningkatan waktu setiap adanya penambahan satu huruf dan baru efektif bekerja untuk dengan maksimal jumlah karakter sebanyak tujuh huruf.
2. Kategori angka
    a. Jumlah karakter berdasarkan angka urut
    Dari 4 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan metode *library*, memiliki peningkatan waktu setiap adanya penambahan satu angka dan baru efektif bekerja untuk dengan maksimal jumlah karakter sebanyak tiga angka.
    b. Jumlah karakter berdasarkan angka acak
    Dari 3 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan metode *brute force*, memiliki peningkatan waktu setiap adanya penambahan satu angka dan baru efektif bekerja untuk dengan maksimal jumlah karakter sebanyak tiga angka.
3. Kategori tanda baca
    Dari 7 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan penggunaaan tanda baca berdasarkan peletakannya dengan metode *brute force*, hanya berhasil dipecahkan pada *password* yang menggunakan tanda baca diakhir kata.
4. Kategori kombinasi
    Dari 3 skenario pengujian, fungsi *John The Ripper* terhadap *hash password* dengan penggunaaan kombinasi huruf, angka, atau tanda baca dengan metode *brute force* belum berhasil dipecahkan.

John The Ripper baru mampu untuk melakukan *password cracking* secara cepat pada *password* yang memiliki jumlah karakter dibawah tujuh dan tanpa kombinasi angka atau tanda baca, *password* ini biasa dianggap sebagai *password* bersifat lemah. Pada *password* yang menggunakan kombinasi angka atau tanda baca, pemecahan membutuhkan waktu yang lebih lama. Di semua skenario pengujian, *hash* tetap berhasil ditangkap dan disimpan walaupun tingkat kesulitan *password* tersebut cukup sulit. Hasil *hash* yang sudah disimpan dari *password* dengan tingkat kesulitan tinggi, pemecahan *password* dapat dilakukan secara manual dengan bantuan komputer lain.

5.4. Analisis Penggabungan Teknik Serangan Lain

Rubber Ducky Attack sebagai *virtual keyboard* pada pengujian ini hanya sebagai fitur tambahan untuk membuktikan bahwa teknik serangan ini bisa dikombinasikan dengan *Windows LockPicker*. Teknik serangan ini berhasil diimplementasikan ketika komputer sudah berhasil melakukan *user login*. Pengembangan teknik serangan ini terdapat banyak jenisnya dan dapat disesuaikan kebutuhan yang diharapkan.

5.5. *Vulnerability, Threat, Risk*, dan *Control* Skenario Penyerangan

Bagian ini akan menjelaskan *Vulnerability*, *Threat*, *Risk*, dan *Control* (VTRC) dari skenario penyerangan. Berikut penjelasan VTRC yang ada pada penelitian ini:

- *Vulnerability*: celah yang dapat digunakan untuk melakukan penyerangan berupa pengambilan *hash user password* yang tersimpan pada jaringan lokal *PC*.
- *Threat*: penyerang dapat menfaatkan celah yang ada untuk melakukan pemecahan *password* dari *hash* yang berhasil diambil.
- *Risk*: risiko yang mungkin timbul dari celah tersebut adalah dapat diaksesnya *PC* target secara penuh oleh penyerang apabila *password* yang digunakan bersifat lemah.
- *Control*: mematikan fitur USB *Driver* dan USB *Mass Storage* pada sistem operasi *Windows*.

5.6. Rekomendasi Untuk Meminimalisir Terjadinya Serangan

Berdasarkan hasil penelitian yang sudah dilakukan dengan melakukan penyerangan *Windows LockPicker* didapatkan hasil bahwa penyerangan dapat terjadi dengan mudah dan cepat pada *password* yang bersifat lemah. Rekomendasi untuk meminimalisir terjadinya serangan seperti ini dilihat dari 2 aspek berbeda sebagai berikut:

1. User
    - Jangan menggunakan password yang bersifat lemah, gunakan kombinasi angka acak atau jumlah karakter diatas delapan pada user password untuk memperkecil kemungkinan serangan.
    - Jangan membiarkan PC lepas dari pantauan pemiliknya dalam kondisi locked atau sleep.
    - Membiasakan untuk selalu Sign Out User Account jika memang diperlukan.

- Hindari menghubungkan PC dengan perangkat USB yang mencurigakan atau tidak dikenal.

2. Sistem
   - Mematikan fitur USB Driver dan USB Mass Storage melalui Windows Registry.
   -

6. Kesimpulan

Berdasarkan hasil penelitian yang sudah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Penerapan metode *WindowsLockPicker* dengan *platform P4wnP1* dapat berhasil dilakukan pada *microcontroller Raspberry Pi Zero W* dengan bantuan *Software PuTTY* untuk penerapannya. Metode ini membuat *Raspberry Pi Zero W* terdeteksi sebagai *USB Ethernet* dan *USB Mass Storage*.
2. Metode *Windows LockPicker* dapat digunakan untuk melakukan penyerangan terhadap sistem operasi dengan *Windows Credentials Manager* selain *Windows 10*, yaitu *Windows 8.1*.
3. *Hash* yang tersimpan pada *cache Windows SAM* akan dengan mudah ditangkap bila *PC* berada dalam kondisi *locked* atau *sleep* karena semua proses dari pengguna sebelumnya masih bekerja secara *background*.
4. Berdasarkan tiga puluh dua skenario pengujian, aplikasi *John The Ripper* sebagai pemecah *password* pada metode ini dirasa masih kurang efektif pada *password* yang memiliki tingkat kesulitan tinggi dengan tingkat keberhasilan 60% dari semua total *hash* yang diambil.Penggunaan kombinasi angka acak lebih efektif dalam mempersulit kemungkinan serangan dibandingkan dengan penggunaan huruf kapital dan tanda baca pada *password*.
5. Penggunaan kombinasi angka dan tanda baca secara acak sangat efektif dalam mempersulit kemungkinan serangan dibandingkan dengan hanya penggunaan huruf saja.
6. Penggabungan teknik serangan lain seperti *Rubber Ducky Attack* dapat dikombinasikan dengan *Windows LockPicker* dan diatur untuk mulai berjalan ketika sudah berhasil melakukan *user login*.

7. Saran

Untuk penelitian lebih lanjut, berdasarkan hasil pengujian yang telah dibuat pada penelitian ini dapat dijadikan sebagai acuan untuk pengembangan yang mendalam lagi. Terdapat saran-saran yang dapat membantu yaitu:

1. Melanjutkan pengembangan pada aplikasi pemecah password untuk menggantikan *JohnTheRipper* dengan aplikasi atau *tool* yang lebih efektif untuk *password cracking* dengan tingkat kesulitan tinggi.
2. Melanjutkan pengembangan *USB Rubber Ducky Attack* agar bisa lebih bervariasi lagi teknik serangan yang dapat dilakukan setelah berhasil melakukan *login*.

Daftar Pustaka:

[1] P. Walters, “The Risks of Using Portable,” 2012.

[2] F. Griscioli, M. Pizzoni dan M. Sacchetti, *USBCheckIn: Preventing BadUSB Attacks by*, 2016.

[3] MaMe82, 2017. [Online]. Available: https://p4wnp1.readthedocs.io/en/latest/. [Diakses 1 Oktober 2018].

[4] C. Tweed dan G. Quigley, “The design and technological feasibility of home systems for the elderly,” The Queen’s University of Belfast, Belfast, 2000.

[5] L. Ada, *Introducing the Raspberry Pi Zero,* 2018.

[6] E. V. Haryanto, Sistem Operasi Konsep dan Teori, Yogyakarta: CV Andi Offset, 2012.

[7] MaMe82, “Windows 10 Lockpicker,” 2017. [Online]. Available: https://github.com/mame82/P4wnP1-Wiki/wiki/Windows-10-Lockpicker. [Diakses 6 Oktober 2018].

[8] Openwall, “John the Ripper password cracker,” Mei 2019. [Online]. Available: https://www.openwall.com/john/.

[9] T. Lubeck, “Distributed Password Cracking with John the Ripper,” 2013.

[10] Kaspersky, “What's a Brute Force Attack?,” 2018. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/brute-force-attack. [Diakses 9 Oktober 2018].

[11] E. Susanto, “Mengenal Hash,” Agustus 2015. [Online]. Available: https://www.kompasiana.com/edysusanto74/55bf219ad17e61430507df3c/mengenal-hash. [Diakses Juni 2019].

[12] J. Orchilles, Microsoft Windows 7 Administrator's Reference, Syngress, 2010.

[13] I. D. Cahyani, “Sistem Keamanan Enkripsi Secure Shell (SSH) Untuk Keamanan Data,” 2010.

[14] S. Carroll, “USB Malware Attacks On the Rise,” November 2010. [Online]. Available:

https://www.pcmag.com/article2/0,2817,2372152,00.asp. [Diakses 9 Oktober 2018].

[15] T. R. Dythia Novianty, "Windows 10 Sistem Operasi Paling Terpopuler di PC, Tapi...," Januari 2019. [Online]. Available: https://www.suara.com/tekno/2019/01/07/060033/windows-10-sistem-operasi-paling-terpopuler-di-pc-tapi. [Diakses Mei 2019].