BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Password alfanumerik telah digunakan secara tradisional untuk memastikan keaslian pengguna. Walau saat ini teknik identifikasi lain seperti *smartcard* dan *biometric* tersedia, sistem *password* kemungkinan besar akan dominan mengingat masalah keamanan, kemudahan pengguna, privasi dan keandalan pendekatan lain.

Akan tetapi upaya yang diperlukan untuk mengingat kata sandi merupakan kelemahan dari pendekatan ini. Studi yang baru-baru ini dilakukan menggambarkan kapasitas manusia untuk mengingat sejumlah kata sandi terbatas (Khodadadi, Islam, Baharun, & Komaki, 2016). Masalah lain dari penggunaan *password* adalah kualitas dan kuantitas *password* dengan contoh sebarapa mudah (atau sulit) *password* dapat ditebak oleh penyerang yang menginginkan akses yang dimiliki korban dengan berpura-pura menjadi korban (Hu, 2017). Survey dari 63 responden menyatakan bahwa sekitar 80% pengguna memiliki panjang *password* kurang dari sepuluh digit, dan 51% responden tidak pernah mengganti *password* (Charoen, 2014).

Di zaman modern, orang lebih terlibat dalam aktivitas *online*. Untuk melakukannya, pengguna harus membuat dan mengatur banyak akun dalam berbagai sistem. *Password manager* merupakan program yang digunakan untuk membuat, mengenkripsi, dan menyimpan *passwords* untuk sisi *client side*. Akan

tetapi, dengan melakukan *password stealing attack* penyerang banyak mengambil data personal seperti password yang di-*hash*, nama, email, nomor telepon, dan tanggal lahir korban (Billa, Shakil, Nawar, & Das, 2019). Mengingat semakin meningkatnya pencurian data elektronik dan dampak finansial yang signifikan dari kejahatan siber, para peneliti mulai mengeksplorasi dan menemukan pasar data curian online tempat para penjahat siber membeli dan menjual infromasi yang diperoleh (Holt, Chua , & Smirnova, 2013).

Mozilla Firefox merupakan browser populer kedua terbanyak yang digunakan oleh masyarakat Indonesia dengan *platform* desktop yaitu 16.11% pada Desember 2019 (Desktop Browser Market Share Indonesia, 2020). Mozilla Firefox menawarkan fitur *Autofill logins* yang dapat diatur melalui *Firefox Lockwise password manager* (Wyman, Draniu, & Joni, 2019) yang menyimpan *website address, username,* dan *password* tanpa memerlukan *master password* secara *default*. *Credential* dapat dilihat dalam bentuk plaintext sehingga memungkinkan penyerang mengambil *credential* yang tersimpan dengan melakukan *password stealing program attack* menggunakan *malicious software* (malware).

Malware adalah program komputer yang didesain untuk membuat efek berbahaya dan tidak diinginkan. Malware dianggap sebagai salah satu dari banyak ancaman berbahaya bagi pengguna internet (Mohd Faizal Ab Razak, 2016). Banyak ahli *cybersecurity* percaya bahwa malware adalah senjata utama untuk melakukan niat jahat pada dunia maya. Serangan siber ini sangat berkembang karena penyerang hanya membutuhkan beberapa pengeluaran dan koneksi

internet. Penyerang tidak dibatasi oleh geografi dan jarak. Penyerang sulit untuk diidentifikasi dan dituntut karena sifat anonim internet (Nepal & Jang-Jaccard, 2014). Di samping itu, terdapat juga malware yang dapat diimplementasikan dengan bantuan microcontroller Universal Serial Bus (USB).

Microcontroller USB merupakan suatu teknologi yang memiliki interface USB dengan fungsi untuk melakukan komunikasi machine to machine terhadap komputer maupun server (Raj, Rahman, & Anand, 2016). Salah satu microcontroller Universal Serial Bus adalah Digispark. Digispark merupakan arduino *boards* terkecil yang pernah dibuat. Walaupun berbentuk kecil, Digispark memiliki peforma yang cukup baik. Digispark mirip dengan arduino dalam pemrograman, tetapi lebih murah, lebih kecil dan memiliki USB connector (Introduction to DigiSpark - A Smaller, Cheaper and Powerful Arduino board - Electronics-Lab, 2018). Digispark dapat dimanfaatkan sebagai human interface device (HID). USB interface umumnya merupakan sektor berbahaya untuk diserang. Firmware perangkat USB tidak bisa dipindai oleh mesin *host*. Penyerangan ini memungkinkan perangkat untuk mengambil tindakan rahasia pada mesin host. Sebagai contoh, USB *flashdrive* dapat mendaftarkan dirinya sebagai perangkat atau *keyboard*. Hal tersebut memungkinkan kemampuan untuk menjalankan *script* berbahaya. Perangkat lunak antivirus tidak dapat mendeteksi atau melindungi terhadap serangan ini (Cannols & Ghafarian, 2017).

Penelitian mengenai *password stealing program attack* pernah dilakukan oleh Harianto & Gunawan (2019). Penelitian tersebut menganalisis password *Wi-Fi*, khususnya *password Wi-Fi* personal, menggunakan microcontroller USB

Rubber Ducky. Berdasarkan hasil penelitian tersebut, masih terdapat *guessable password* sebesar 87.88% dan tingkat kesamaan penggunaan *password* sebesar 81.82%. Di samping itu, menurut hasil *Data Breach Investigations Report* (DBIR) 2019 oleh Verizon, dari 52% *data breach* yang terjadi, sebanyak 33% disebabkan oleh *social attacks* dan 28% disebabkan oleh malware. Disimpulkan dari 41686 *security incidents* dan 2013 kasus *data breach* yang terjadi, sebanyak 94% malware dikirim melalui email (Verizon, 2019). Berdasarkan permasalahan di atas, dilakukan *password stealing program attack* terhadap *saved password* pada *Mozilla Firefox*.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah sebagai berikut.

1. Bagaimana cara mengimplementasikan *password stealing program attack* terhadap *saved password* pada Mozilla Firefox?
2. Berapa tingkat keberhasilan password stealing program attack dalam mendapatkan seluruh daftar *user password* yang tersimpan pada browser Mozilla Firefox dari sebuah komputer?
3. Berapa tingkat kekuatan seluruh *stolen password* yang diukur dengan menggunakan zxcvbn *password strength estimation*?
4. Berapa persentase *stolen password* yang ada pada *data breach* database menggunakan haveibeenpwned?

1.3 Batasan Masalah

Batasan masalah dari penelitian ini adalah sebagai berikut.

1. Platform sistem operasi yang digunakan adalah sistem operasi Windows 7 dan Windows 10.
2. Komputer yang diserang harus memiliki koneksi internet.
3. Komputer yang diserang harus menggunakan akun *administrator*.
4. Microcontroller USB yang digunakan adalah Digispark.

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut.

1. Mengimplementasikan *password stealing program attack* terhadap *saved password* pada Mozilla Firefox.
2. Mengukur tingkat keberhasilan *password stealing program attack* terhadap *saved password* pada Mozilla Firefox.
3. Mengukur tingkat kekuatan password menggunakan *zxcvbn password strength estimation*.
4. Mengukur persentase *stolen password* yang ada pada *data breach* database menggunakan *haveibeenpwned*.

1.5 Manfaat Penelitian

Manfaat dilakukannya penelitian ini adalah memberikan security awareness kepada masyarakat mengenai bahaya dari malware.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi terdiri dari lima bab, yaitu sebagai berikut.

1. BAB I PENDAHULUAN

   Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

2. BAB II LANDASAN TEORI

   Bab ini menjelaskan landasan teori dari penelitian yang dilaksanakan seperti infrastruktur Digispark, bahasa yang digunakan Digispark, Firefox Lockwise *Password Manager*, *password stealing attack*, Zxcvbn *password strength estimation*, Haveibeenpwned dan *system hacking.*

3. BAB III METODOLOGI DAN PERANCANGAN PROGRAM

   Bab ini berisi tentang metode penelitian yang digunakan dan perancangan program yang dipresentasikan dengan perancangan *flowchart,* model aplikasi, proses pembuatan program, dan proses *system hacking*.

4. BAB IV IMPLEMENTASI DAN UJICOBA

   Bab ini berisi tentang implementasi dan uji coba aplikasi yang dibangun

5. BAB V KESIMPULAN DAN SARAN

   Bab ini berisi simpulan dari hasil pengujian aplikasi dan saran untuk pengembangan aplikasi selanjutnya.