BAB I
PENDAHULUAN

I.1 Latar Belakang

Pada zaman yang sudah canggih ini, hampir setiap manusia memiliki perangkat *Personal Computer* (PC) atau laptop yang digunakan untuk sehari-hari. Perangkat PC atau laptop harus memiliki sistem operasi terlebih dahulu untuk dapat dijalankan. Sistem operasi komputer racikan Microsoft, Windows 10, berhasil menjadi sistem operasi PC terpopuler di dunia saat ini, Windows 10 mendominasi pasar sistem operasi PC dengan 39,22 % (Dythia Novianty, 2019). Windows adalah keluarga sistem operasi yang dikembangkan oleh Microsoft yang menggunakan antarmuka berbasis *Graphical User Interface* (GUI) atau tampilan antarmuka bergrafis (Microsoft, 2018).

Dalam penggunaan komputer, dibutuhkan alat pendukung lainnya seperti *Universal Serial Bus* (USB). Perangkat USB kini menjadi jenis perangkat yang paling andal dan paling sering digunakan (Phule, 2015). Salah satu mekanisme yang digunakan oleh banyak orang dengan fungsionalitas *plug and play* yang praktis. Berbagai masalah terkait keamanan telah terjadi karena digunakan secara luas. Namun demikian, sebagian besar USB *flash drive* tidak termasuk mekanisme keamanan, penyerang dapat dengan mudah memperoleh informasi pribadi di USB *flash drive* (Kim, 2016).

Perangkat transien seperti perangkat USB telah lama digunakan sebagai vektor serangan. Berbagai bentuk pelanggaran keamanan dalam beberapa tahun terakhir menggambarkan bahwa musuh menggunakan perangkat semacam itu untuk menyebarkan *malware*, mengendalikan sistem, dan mengekstrak informasi (Kharraz, 2015). Baru-baru ini, para peneliti telah menunjukkan bahwa meskipun ada beberapa peringatan yang menggarisbawahi risiko periferal berbahaya, pengguna masih rentan terhadap serangan USB (Tian, 2015) (Tischer, 2015). Dalam mengatasi masalah ini, perangkat lunak antivirus menjadi semakin terbiasa memindai penyimpanan USB untuk *malware*. Melewati pemeriksaan seperti itu seringkali tidak terlalu sulit karena *firmware* perangkat USB tidak dapat dipindai

oleh *host*. USB *flash drive* dapat mendaftarkan dirinya sebagai perangkat penyimpanan dan *Human Interface Device* (HID) seperti *keyboard*, memungkinkan kemampuan untuk menyuntikkan serangan diam-diam untuk melakukan kejahatan.

Dalam beberapa tahun terakhir, semakin banyak serangan telah memanfaatkan teknik serangan yang mencakup serangan injeksi klik tombol/*mouse*. Serangan-serangan ini biasanya dilakukan oleh perangkat antarmuka manusia non-USB yang menyamar sebagai *keyboard* atau *mouse* yang *firmware*-nya telah dimodifikasi. Alat khusus untuk menerapkan serangan ini menggunakan bahasa skrip sederhana yang dengannya siapa pun dapat membuat muatan yang mampu mengubah pengaturan sistem, membuka *backdoor*, mengambil data, memulai *reverse shell*, menjalankan *malware*, atau aktivitas lain yang dapat dicapai dengan akses fisik yang semuanya dapat diotomatisasi dan dieksekusi dalam hitungan detik.

Program *keylogging*, umumnya dikenal sebagai *keyloggers* adalah jenis *malware* yang melacak *input* pengguna dari *keyboard* dalam upaya untuk mengambil informasi pribadi. Meningkatnya penggunaan komputer untuk kegiatan bisnis dan pribadi yang umum menggunakan internet telah membuat penanganan *keylogging* mendesak menjadi efektif. Selain itu, internet tidak hanya menjadi saluran utama untuk menempatkan dan mendistribusikan program jahat, tetapi juga bantuan dalam infeksi dan eksekusi mereka. Karena itu, potensi Internet yang sangat besar telah menyebabkan peningkatan upaya *keylogging* dengan peningkatan tahunan linear *keylogger* unik.

Serangan *spyware/keylogger* menempati urutan pertama sebagai penyerangan yang sering digunakan kepada masyarakat dunia. Data ini berasal dari penelitian Dimension Data Indonesia, di mana *spyware* mendominasi dengan persentasenya mencapai 26% (Hendra, 2018). *Spyware/keylogger* merupakan serangan membaca seluruh aktivitas yang ada dalam perangkat dan dikirimkan kepada penyerang.

Powershell menawarkan suatu antarmuka berbasis perintah dan bahasa *scripting* untuk mengotomasi serta mengelola tasks. Powershell telah menjadi salah satu tempat yang populer untuk melakukan *cyber criminals* karena Powershell sudah tertanam pada sistem operasi Windows dan karena fleksibilitas 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 (Wueest, 2018). Hal tersebut mengindikasikan bahwa para penyerang masih menggunakan Powershell dalam melakukan serangan.

Pada penelitian ini membahas metode *Keyboard Injection Attack* atau dikenal sebagai *keylogger* dengan menggunakan perangkat *microcontroller* berbasis Arduino Pro Micro yang nantinya akan dijadikan sebagai perangkat *BadUSB* yang bernama USB *Keylogger*. *Script* penyerangan akan dikonfigurasi dengan menggunakan *software* Arduino *Integrated Development Environment* (IDE). Dengan metode tersebut, penelitian ini diharapkan dapat dilakukan penyerangan yaitu merekam aktivitas *keystroke* pengguna komputer. *File* hasil *keylogger* akan dikirimkan ke *email* penyerang. Disini penulis memanfaatkan beberapa alat dan teknologi seperti Arduino, Arduino IDE dan Powershell.

I.2 Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut:

1. Bagaimana cara kerja USB *Keylogger* pada *Operating System* Windows 10?
2. Bagaimana hasil implementasi *Keyboard Injection Attack* menggunakan *Microcontroller* Arduino Pro Micro pada *Operating System* Windows 10?
3. Bagaimana cara meminimalisir terjadinya *Keyboard Injection Attack*?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah pada penelitian ini, tujuan yang ingin dicapai adalah sebagai berikut:

1. Mengetahui cara kerja USB *Keylogger* pada OS Windows 10.
2. Mengetahui hasil implementasi *Keyboard Injection Attack* menggunakan *Microcontroller* Arduino Pro Micro pada *Operating System* Windows 10.
3. Memberikan rekomendasi pencegahan untuk meminimalisir terjadinya *Keyboard Injection Attack*.

I.4 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan beberapa manfaat baik secara teoritis maupun praktis, yaitu :

1. Teoritis.

   Secara teoritis, hasil dari penelitian ini diharapkan menjadi acuan untuk peningkatan keamanan dalam penggunaan komputer menggunakan sistem operasi Windows serta dapat mengedukasi masyarakat mengenai pentingnya *awareness* terhadap berbagai macam serangan pada komputer.

2. Praktis.

   Secara praktis, hasil dari penelitian ini diharapkan menjadi bahan pertimbangan bagi pengembang sistem operasi Windows di masa depan dalam menanggulangi *vulnerability* yang didapatkan pada penelitian ini.

I.5 Batasan Masalah

Adapun batasan masalah pada tugas akhir ini, yaitu:

1. Membahas tentang penyerangan menggunakan USB *Keylogger* terhadap *Operating System* Windows 10.
2. Menggunakan perangkat Arduino Pro Micro.
3. Komputer target hanya menggunakan antivirus Windows Defender.
4. Komputer target dalam keadaan stabil dan tidak sedang dalam penggunaan yang berat.

I.6 Sistematika Penulisan

Sistematika penulisan penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini meliputi latar belakang masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan landasan teori yang berkaitan dengan pembahasan masalah yang akan diteliti.

BAB III METODOLOGI PENELITIAN

Bab ini menguraikan jenis penelitian yang akan dilakukan, sumber data yang digunakan dalam penelitian, bagaimana cara mendapatkannya dan terakhir menganalisis dari permasalahan yang ada pada penelitian.

BAB IV PERANCANGAN SISTEM DAN SKENARIO PENYERANGAN

Bab ini menguraikan detail dari perancangan sistem dan skenario penyerangan yang dilakukan.

BAB V PENGUJIAN SISTEM DAN ANALISIS

Bab ini menguraikan langkah-langkah tahapan pengujuan yang terjadi pada saat penelitian. Hasil dari penelitian, analisis ataupun perancangan dari penelitian tersebut.

BAB VI KESIMPULAN DAN SARAN

Bab ini menguraikan tentang kesimpulan dan saran penulis berdasarkan data yang didapatkan dari hasil penelitian.