ABSTRAK

IMPLEMENTASI DAN ANALISIS *KEYBOARD INJECTION ATTACK* DENGAN MENGGUNAKAN PERANGKAT USB PADA *OPERATING SYSTEM* WINDOWS

Oleh

ANNISA DWIAYU RAMADHANTY

1202164121

Windows merupakan salah satu sistem operasi yang populer digunakan saat ini. Sedangkan *Universal Serial Bus* (USB) merupakan salah satu mekanisme yang digunakan oleh banyak orang dengan fungsionalitas *plug and play* yang praktis. USB telah lama digunakan sebagai vektor serangan pada komputer. Salah satu metode penyerangannya yaitu *Keylogger*. *Keylogger* dapat memanfaatkan kerentanan yang ada pada sistem operasi Windows 10 untuk melakukan penyerangan berupa rekaman aktivitas *keystroke* komputer tanpa diketahui oleh pengguna. *Keylogger* memanfaatkan suatu *platform* yang digunakan untuk melakukan serangan USB yaitu Arduino. Arduino dapat digunakan untuk melakukan penyerangan melalui Powershell Administrator. Penelitian ini dilakukan untuk dapat mengetahui cara kerja USB *Keylogger*, mengetahui hasil implementasi *Keyboard Injection Attack* pada Arduino Pro Micro serta dapat memberikan rekomendasi pencegahan untuk meminimalisir terjadinya penyerangan. Hasil yang didapatkan pada pengujian USB *Keylogger* menggunakan Arduino Pro Micro yaitu berhasil dilakukan pada komputer yang sedang tidak melakukan aktivitas tertentu pada *keyboard* maupun *mouse* serta pada komputer dengan keaadan terkoneksi dengan internet. Penyerang akan mendapatkan hasil *keylogger* tersebut melalui *email*.

Kata Kunci: Windows, USB, Keylogger, Arduino, Powershell.