ABSTRAK

Sistem operasi *Windows* merupakan salah satu sistem operasi yang populer digunakan saat ini. Pesatnya perkembangan sistem operasi *Windows*, diikuti pula dengan pesatnya perkembangan *browser* yaitu *Microsoft Edge* yang merupakan *browser* bawaan dari sistem operasi *Windows* terbaru yaitu *Windows 10*. Pada *Microsoft Edge* terdapat celah dimana pengguna lain yang tidak memiliki otoritas dapat mengakses *username* dan *password* yang tersimpan dari *Microsoft Edge* menggunakan *method* pada *Powershell. Powershell* menjadi tempat yang populer untuk melakukan *cyber criminals* pada sistem operasi *Windows. BadUSB* merupakan perangkat USB yang dimanipulasi oleh penyerang. Terdapat suatu platform serangan USB yang dinamakan P4wnP1. Penggunaan P4wnp1 memungkinkan untuk melakukan penyerangan melalui *Powershell* dan melakukan pengambilan *username* dan *password* yang tersimpan. Untuk melakukan penelitian menggunakan P4wnP1, dibutuhkan metode *Rubber Ducky* untuk melakukan pembuatan *Custom Drive Letter* dan menjalankan *Powershell script.* Hasil dari penelitian ini adalah proses *Rubber Ducky* berjalan dengan total waktu 8.5detik dengan *delay* tercepat yaitu 0.5 detik dan *delay* terpanjang yaitu 3detik. USB *attack* dengan melakukan pengambilan data *username* dan *password* yang tersimpan pada *browser Microsoft Edge* dan *Internet Explorer* dengan melakukan beberapa macam skenario penyerangan dapat 100% berhasil dilakukan dan didapatkan rekomendasi yang digunakan untuk meminimalisir terjadinya serangan.

Kata Kunci : *USB Attack, Powershell, Raspberry, P4wnP1, Rubber Ducky.*