

ABSTRAK

IMPLEMENTASI DAN ANALISIS SERANGAN USB PASSWORD STEALER TERHADAP PENGAMBILAN LOGIN DATA PADA GOOGLE CHROME DAN MOZILLA FIREFOX MENGUNAKAN POWERSHELL

Oleh
ABDUL AZIES MUSLIM
1202164284

Seiring dengan berkembangnya sistem operasi Windows, aplikasi *browser* untuk menjelajah internet juga berkembang pesat. *Browser* yang paling banyak digunakan di dunia saat ini antara lain adalah Google Chrome dan Mozilla Firefox. Kedua *browser* ini memiliki fitur penyimpanan *username* dan *password* sehingga memudahkan pengguna saat melakukan *login* pada *website* tertentu yang diinginkan, namun pada kenyataannya menyimpan *username* dan *password* pada *browser* cukup berbahaya karena data-data yang tersimpan dapat diretas menggunakan serangan *brute force* ataupun dibaca melalui suatu program. Salah satu cara untuk mendapatkan *username* dan *password* pada *browser* adalah dengan menggunakan program yang dapat membaca *login data* Google Chrome dan Mozilla Firefox dari penyimpanan internal komputer lalu menampilkan *username* dan *password* yang tersimpan pada kedua *browser* tersebut. Pada penelitian ini akan dilakukan penyerangan dengan mengimplementasikan *Rubber Ducky* menggunakan BadUSB untuk menjalankan program ChromePass dan PasswordFox serta Powershell *script* menggunakan perangkat Arduino Pro Micro Leonardo sebagai USB Password Stealer. Hasil yang didapatkan dari penelitian ini adalah *username* dan *password* pada Google Chrome dan Mozilla Firefox berhasil didapatkan saat USB dihubungkan ke perangkat target, adapun rata-rata waktu berjalannya penyerangan ini adalah 14 detik sebelum kemudian dikirimkan ke *email* penulis.

Kata Kunci: *Rubber Ducky*, Arduino Pro Micro Leonardo, Powershell, ChromePass, PasswordFox.