ABSTRAK

IMPLEMENTASI DAN ANALISIS USB *ATTACK* MENGGUNAKAN METASPLOIT *FRAMEWORK* DENGAN ARDUINO LEONARDO PADA SISTEM OPERASI WINDOWS

Oleh

Ferryansa

1202162175

Pesatnya perkembangan sistem operasi Windows, diikuti pula dengan kejahatan yang dapat dilakukan pada sistem operasi tersebut. *Universal Serial Bus* (USB) merupakan salah satu mekanisme yang digunakan oleh banyak kalangan masyarakat dengan fungsionalitasnya seperti *plug and play* dan sangat mudah untuk digunakan, serta *transfer data* yang cepat jika dibandingkan dengan perangkat keras lainnya. Sistem operasi Windows memiliki banyak kelemahan, salah satunya mudah mengalami eksplotasi pada sistemnya. Ada berbagai metode untuk melakukan kejahatan pada sistem operasi Windows hanya dengan menggunakan sebuah USB saja, salah satu yang memungkinkan adalah pelaku kejahatan melakukan penanaman *backdoor reverse shell* untuk mengeksploitasi perangkat hanya dengan menghubungkan USB ke komputer tanpa diketahui oleh korbannya. Penelitian ini dilakukan supaya menghasilkan penanaman *backdoor reverse shell* untuk melakukan eksploitasi, khususnya dibagian *webcam* dan *microphone* pada komputer korban hanya dengan menggunakan USB. Dari 35 percobaan yang telah dilakukan pada penelitian ini, didapatkan bahwa sekitar 83% pengujian penanaman *backdoor reverse shell* untuk melakukan eksploitasi terhadap *webcam* dan *microphone* pada sistem operasi Windows berhasil dilakukan.

Kata Kunci: Sistem Operasi, *Powershell*, USB *Attack*, Arduino, *Reverse Shell*, Eksploitasi.