ABSTRACT

IMPLEMENTATION AND ANALYSIS OF KEYBOARD INJECTION ATTACK USING USB DEVICES IN WINDOWS OPERATING SYSTEM

By

ANNISA DWIAYU RAMADHANTY

1202164121

Windows is one of the popular operating systems in use today. Whereas Universal Serial Bus (USB) is one of the mechanisms used by many people with practical plug and play functionality. USB has long been used as a vector of attacks on computers. One method of attack is Keylogger. Keylogger can take advantage of existing vulnerabilities in the Windows 10 operating system to carry out attacks in the form of recorded computer keystroke activity without the user knowing. Keylogger utilizes a platform that is used to carry out USB attacks, Arduino. Arduino can be used to carry out attacks through the Powershell Administrator. This research was conducted to be able to find out how the USB Keylogger works, to know the results of the implementation of Keyboard Injection Attack on Arduino Pro Micro and to provide prevention recommendations to minimize the occurrence of attacks. The results obtained on the USB Keylogger test using Arduino Pro Micro were successfully carried out on a computer that was not carrying out certain activities on the keyboard or mouse as well as on computers with conditions connected to the internet. Attackers will get the results of the keylogger via email.

Keywords: Windows, USB, Keylogger, Arduino, Powershell.