

ABSTRACT

IMPLEMENTATION AND ANALYSIS OF USB ATTACK USING METASPLOIT FRAMEWORK WITH ARDUINO LEONARDO IN WINDOWS OPERATION SYSTEM

By

Ferryansa

1202162175

The rapid development of the Windows operating system, followed by crimes that can be committed on the operating system. Universal Serial Bus (USB) is one of the mechanisms used by many people with functionality such as plug and play and is very easy to use, also fast data transfer when compared with other hardware. The Windows operating system has many weaknesses, one of which is easy to exploit the system. There are various methods for committing crimes on the Windows operating system only using an USB, one of which is allows perpetrators of the crime planting a backdoor reverse shell to exploit the device just by connecting the USB to the computer without the victim being noticed. This research was conducted in order to produce planting a backdoor reverse shell for exploitation, especially in the webcam and microphone section of the victim's computer only using an USB. From 35 experiments that have been carried out in this study, it was found that about 83% of the reverse shell backdoor planting test to exploit the webcam and microphone on the Windows operating system was successfully carried out.

Keywords: Operating System, Powershell, USB Attack, Arduino, Reverse Shell, Exploitation.