

ABSTRACT

IMPLEMENTATION AND ANALYSIS USB ATTACK OF PASSWORD RETRIEVAL FOR LOG IN TO A PERSONAL COMPUTER USING WINDOWS LOCKPICKER

By

NICO ALMANSYA ELLSADAAI

1202152181

USB has the convenience of connecting to various types of operating systems that some people use as loopholes to create applications with special methods that can be used for attacks, for example Windows as the most widely used operating system these days. This operating system has weaknesses, such as the ease of retrieving user password hashes stored on Windows SAM. The USB attack method called Windows Lockpicker on the P4wnP1 platform aims to allow attackers to enter as computer users in a locked position without needing to know the user's password first, by retrieving the stored hash and then hacking the password to log in. This research resulted in the possibility of 60% success in completing passwords from 32 scenarios that had been successfully extracted and also recommendations that could be given by the author to minimize the occurrence of attacks.

Keywords: USB, operation system, Windows Lockpicker, P4wnP1, Password Cracking