ABSTRACT

IMPLEMENTATION AND ANALYSIS OF USB PASSWORD STEALER ATTACK ON TAKING DATA LOGIN FROM GOOGLE CHROME AND MOZILLA FIREFOX USING POWERSHELL

By
ABDUL AZIES MUSLIM
1202164284

Along with the development of the Windows operating system, browser applications to surf the internet are also growing rapidly. The most widely used browsers in the today is Google Chrome and Mozilla Firefox. Both browsers have a username and password management feature that makes users log in to a website easily, but in fact saving usernames and passwords in the browser is quite dangerous because the stored data can be hacked using brute force attacks or read through a program. One way to get a username and password in the browser is to use a program that can read Google Chrome and Mozilla Firefox login data from the computer's internal storage and then show those data. In this study an attack will be carried out by implementing Rubber Ducky using BadUSB to run the ChromePass and PasswordFox program and the Powershell script using the Arduino Pro Micro Leonardo device as an USB Password Stealer. The results obtained from this study are the username and password on Google Chrome and Mozilla Firefox successfully obtained when the USB is connected to the target device, the average time of the attack is 14 seconds then sending it to the author's email.

Keyword: Rubber Ducky, Arduino Pro Micro Leonardo, Powershell, ChromePass, PasswordFox.