ABSTRACT

The Windows Operating System is one of the most popular operating systems in use today. The rapid development of the Windows operating system, followed by the development of browsers, namely Microsoft Edge. In Microsoft Edge, which is related to other users who do not have usable authority, users and passwords originating from Microsoft Edge use methods in Powershell. Powershell is a popular place to do cyber criminals on the Windows operating system. BadUSB is a USB device that is manipulated by attackers. It is a USB attack platform called P4wnP1. The use of P4wnp1 makes it possible to attack via Powershell and retrieve a saved username and password. To conduct research using P4wnP1, a Rubber Ducky method is needed to create Custom Drive Letters and run Powershell scripts. The result of this research is that the Rubber Ducky process runs with a total time of 8.5 seconds with the fastest delay of 0.5 seconds and the longest delay is 3detic. USB attacks by retrieving user name data and passwords stored on Microsoft Edge and Internet Explorer browsers by performing various types of attacks can be 100% successful and an assessment is used to minimize the attack.

Keywords : USB Attack, Powershell, Raspberry, P4wnP1, Rubber Ducky.