Duck Toolkit project

The initial aim of the Duck Toolkit project was to create a website that would allow users to easily create payloads for the Hak5 USB Rubber Ducky that can be used within a penetration testing environment.

One of the most important features of this toolkit is not the mixing of scripts but the reporting of information collected from the target computer. Reconnaissance reports are generated which contain information about the target computer based on the user script selections.

The information within these reports can range from installed software to network information, but is all designed to be useful in a penetration testing context.

At this time all scripts are written in PowerShell and therefore will only work against target machines with PowerShell installed (Windows 7/8, Windows Server 2008). Administrative access is also required to ensure scripts work correctly.

More information

https://ducktoolkit.com/