Overview

This week's goal was to work on transferring our work from writeup 2 (calling card) into Ducky Script, so we can soon actually deploy with Rubber Duckies! This writeup covers some basics of Ducky Script, as well as the commands I used.

Ducky Script

Ducky Script is the scripting language used to deploy payloads in technology created by Hak5. It was originally introduced with the USB Rubber Ducky in 2010, hence the name - though it is now used in many other payload platforms provided by Hak5. The idea is to provide as many abilities to these tools as possible while keeping them easy to use.

Ducky Script uses Bash for logic and conditional operations, so some of its features may seem familiar to Linux users. Its commands are relatively close to plain English and there are command references out there (including one by Hak5 themselves, linked below), so it isn't difficult to pick up. It can also, conveniently, be written on any ASCII text editor.

The capabilities provided by Ducky Script depend on the tool used. The ones available to Rubber Duckies mainly include keystroke injection and delays to allow the computer to catch up - which makes sense, given the Rubber Ducky's purpose is to act as a keyboard. It also provides other ways to interact with the computer, some of which depend on the operating system involved, so it is important to consider your target before scripting.

Another thing to remember is that the Ducky Script needs to be encoded before it can be deployed on a Rubber Ducky. This uses Java functionality to create a bin file that it can process. This encoding can be done one of two ways: either with the JavaScript Ducky Encoder, which is a single HTML file that can be locally run in a modern browser, or the command line tool, which uses the Java runtime environment and a few arguments.

The JavaScript Ducky Encoder can be found on https://downloads.hak5.org/, and the command line tool can be downloaded from https://usbrubberducky.com. For the latter, usage is: `java -jar duckencoder.jar -i input.txt -o output.bin`.

Commands Used

As I was attempting to emulate my Bash/Batch scripts, which involved creating a file and going to a web server, I needed to use Ducky Script to do the same thing. The most convenient way to do this is to have the Rubber Ducky open a command interface itself and input commands there.

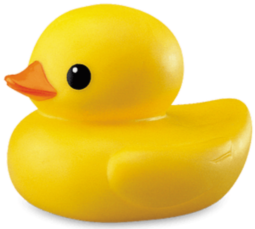
In Linux, the command to open the terminal is `ALT F2`. In Windows, `GUI r` is the equivalent of Windows + R, which opens the Run command. .

A `DELAY` (followed by a number between 1 and 10000, in milliseconds) is needed each time a program is opened before giving new commands.

The `STRING` command gives the Rubber Ducky something to type. The `ENTER` command tells it to use the enter key, in effect running the command.

The `CTRL` key is similar to `ENTER` and `ALT` in that it just represents using keys that exist on the keyboard. These commands are important, as they are often used in automated operations on computers.

Last but not least, the command to comment is the same as on Batch - `REM`, followed by the comment.



Citations

Ducky Script Command Reference

https://docs.hak5.org/hc/en-us/articles/360049449314-Ducky-Script-Command-Reference

Hak5's Beginner Guide

https://docs.hak5.org/hc/en-us/articles/360010471234-Writing-your-first-USB-Rubber-Ducky-Payload

Hak5 Download Center

https://downloads.hak5.org/

About Ducky Script

https://docs.hak5.org/hc/en-us/articles/360010555153-Ducky-Script-the-USB-Rubber-Ducky-language