PASSWORD DESIGN & CRACKING

**Lesson Description:** This lesson introduces students to the way that password are actually attacked and how to defend against password attacks by creating strong passwords. Students will experiment with dictionary and brute force attacks against passwords to learn which attack types are faster and how they work.

**Prerequisite Knowledge:** Students are ideally familiar with basic use of a Linux command line interface

**Length of Completion**: 1.5 hours

**Level of Instruction:** Beginning high school or advanced/motivated middle school students

**Applicable First Principles &/or Concepts:**

**GenCyber First Principles**

Domain Separation Abstraction

Process Isolation Data Hiding

Resource Encapsulation Layering

Modularity Simplicity

Least Privilege Minimization

**GenCyber Cybersecurity Concepts**

Defense in Depth Availability

Confidentiality **Think Like an Adversary**

**Integrity** Keep it Simple

**Resources that are Needed:** Linux computers (Raspberry Pis are used in this lesson but virtual machines running Linux could be used instead with appropriate modification to the lesson)

**Accommodations Needed:** n/a (general accessibility components of the operating system may be required for some students)

# learning outcomes

LEsson learning oUTCOMES

* Explain and demonstrate the two primary ways of attacking passwords
* Test various passwords against the John The Ripper password cracking utility to determine relative strength
* Design an example of a good password and explain what goes into creating a strong password and why

# Lesson Details

**Interconnection:** In addition to covering the above principles/concepts this lesson is designed to reinforce previous lessons on exploring the Linux command line and the Raspberry Pi systems generally. Some of the concepts introduced in this lesson (hashing) can be further built upon as related to encryption.

**Assessment:** In the GenCyber camp this activity was assessed informally by walking around and watching participants as well as questions checking for understanding orally at various points of the lesson. In a school setting additional assessment could be used such as turning in a written lab report with conclusions and examples of secure passwords.

**Extension Activities:** Writing a simple Python based application that stores passwords as salted hashes in a simple database and then prompts users for passwords which are checked against the database to determine if the user has valid access to the system.

**Differentiated Learning Opportunities:** Additional learning around various password hashing algorithms, proper creation of salts for password hashes, PBKDF algorithms, etc. are possible for more advanced students.

# lesson

**Warm Up:** Show students a short presentation on the laws surrounding illegal hacking activities.

**Lesson:**

Hak5 is a well-known company that specializes in creating tools and technologies for ethical hacking and penetration testing. They offer a wide range of innovative tools that assist security professionals in identifying vulnerabilities and testing the robustness of systems. One of their popular products is the Wi-Fi Pineapple, a powerful wireless network auditing tool. The Wi-Fi Pineapple allows security testers to conduct various attacks on Wi-Fi networks, such as capturing network traffic, creating rogue access points, and performing man-in-the-middle attacks. It provides valuable insights into the security of wireless networks and helps organizations identify and address potential weaknesses.

In addition to their digital tools, Hak5 also focuses on physical pentesting, which involves assessing the security of physical infrastructure and facilities. Physical pentesting is crucial for evaluating the effectiveness of access controls, surveillance systems, and overall physical security measures. Hak5 offers tools like the Rubber Ducky, a versatile USB device that can be used to simulate keyboard input and execute predefined commands. This tool can be used during physical assessments to bypass login screens, escalate privileges, or perform other automated actions. By combining their digital tools with physical pentesting techniques, Hak5 provides security professionals with a comprehensive approach to evaluating the overall security posture of organizations and helping them identify vulnerabilities that could be exploited by malicious actors.

Most of the tools they sell use a programming language termed Duckyscript:

**MANUAL METHOD:**

1. What is Duckyscript?
   * Duckyscript is a scripting language used with the Rubber Ducky USB device.
   * The Rubber Ducky looks like a regular USB drive but can type commands quickly as if someone is typing on a keyboard.
   * Duckyscript provides a way to automate tasks on a computer by simulating keyboard inputs.
2. Understanding Duckyscript Commands:
   * Duckyscript commands are written in plain text and each command is written on a new line.
   * The key to writing these scripts is to include EVERY keystroke that you need to press to accomplish something. For example, to open the Windows menu and type “word” only using the keyboard requires using the Windows Key, then typing the sting of letters W O R & D.
   * The most common commands include:
     + DELAY: Pauses for a specific amount of time (in milliseconds).
     + STRING: Types a specific string of characters.
     + GUI: Simulates pressing a modifier key (e.g., Windows key) along with another key.
     + ENTER: Simulates pressing the Enter/Return key.
3. Writing a Simple Ducky Script:
   * Let's write a simple Duckyscript to open Notepad.exe on a computer:
     + Start with "DELAY 1000" to wait for one second.
     + Next, write "GUI r" to press the Windows key and the letter "r" together.
     + After that, add "DELAY 500" to wait for half a second.
     + Now, type "notepad.exe" using the "STRING" command.
     + Finally, add "ENTER" to simulate pressing the Enter/Return key.

*DELAY 1000*

*GUI r*

*DELAY 500*

*STRING notepad.exe*

*ENTER*

*DELAY 500*

*STRING Hello GenCyber*

1. Testing the Ducky Script (will be done with a counselor to not violate any laws):
   * Insert the Rubber Ducky USB device into a computer's USB port.
   * The computer will detect it as a regular USB keyboard.
   * Open a text editor or any document where you can type.
   * Run the Ducky Script by copying and pasting the script into the document.
   * Save the file with a .txt extension, and make sure it has a .txt extension rather than .txt.txt.
   * Double-click the script file to open it and watch as Notepad.exe is automatically opened.

**ALTERNATE METHOD:**

There are a few resources online now that store DuckyScripts that can be used as is, or as examples/frameworks for scripts.

Hak5’s Official Github Repo for BashBunny:

[hak5/bashbunny-payloads: The Official Bash Bunny Payload Repository (github.com)](https://github.com/hak5/bashbunny-payloads)

Prank scripts: [bashbunny-payloads/payloads/library/prank at master · hak5/bashbunny-payloads · GitHub](https://github.com/hak5/bashbunny-payloads/tree/master/payloads/library/prank)

Payload designer:

<https://ducktoolkit.com/payload/windows>

**CHALLENGE:**

Using either of the above methods, come up with two scripts to test on a Bash Bunny that will do the following items:

**Open Notepad and type “We will win today’s team challenge” ten times.**

**Shutdown a Windows computer in 10 seconds with a simple message.**

**Brain storm 5 ways that these devices could be used to gain unlawful access to a device.**