Raspberry PI Pen Testing

The aim of this lab is to introduce you to the world of penetration testing with a basic demo. Following this lab sheet, you will learn about SQL injection (As well as some basic SQL) and buffer overflows in a C program. **Beware**, trying any of these techniques on any system without permission is a **crime and you will be caught and prosecuted for it**. With that out of the way, at the end of the cheat sheet is some helpful resources to safely and legally practice pen testing in your own time.

# Task 1: SQL Injection

To begin with, you’ve been asked to test the site of a new and upcoming frozen food shop Rice-On-IceTM. The owner has reported issues where users have been gaining root access on their raspberry pi server setup. It is likely they have neglected to protect against SQL injection attacks (it definitely is). Therefore, you have several tasks to prove that SQL Injection is the cause of these issues.

1. Find the name of the second ‘secret’ table

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Find the name of the file and decode the password

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Task 2: Network Mapper

With the password and the name of the file, it’s time to access it. To do this, use the Network mapper tool to scan and find the webserver to access the file.

1. Find the phrase from the readme found inside of the secret file

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Task 3: Buffer Overflow

Inside of this file there is a C program (myHelper.c). Why this file is here we have no idea, but we figure its likely this is giving users that root access. With some research and help from the cheat sheet, open a terminal with root access to the system.

Once you think you have it, type ‘whoami’ to confirm that you are the root user.

Congratulations! You have gained root access to your first system.