Lab 10 – Linux Privilege Escalation

# Overview

This lab will consist of you attempting to escalate to the root account on a Linux system. There are multiple vulnerabilities created on the system for you to discover.

# Scenario

You have just popped a shell on your first system on the network and only have low level privileges. Your job is to find as many ways to escalate to root as possible. There are at least 4 different ways to escalate. None of the possible escalation techniques include kernel or service exploits, they will all be based on internal reconnaissance and misconfigurations. Use of open source scripts is allowed but you must document what you use and what it produced.

To simulate getting your first shell on the network you have SSH credentials to the docker container. They are **user/Password1!**.

# Running the Container

Run the container on your Kali host similar to the previous, if there are errors running this command check that the double quotes are correct if you copy pasted the command:

docker run -it tjflaagan/test sh -c "/bin/services.sh && bash"

# Deliverable

From this you should produce a document showing the various techniques that you used to find the methods to escalate to root. Include screenshots showing the technique itself and running the command whoami in the same screenshot.

**NOTE: User native docker functionality to drop into a root shell is not in scope for this exercise.**