Lab 07 – Metasploit Basics

Include a screenshot for each step along the way while exploiting the system.

# Overview

With data from scanning you can now attempt to exploit a system. You’ll have to decipher the scan output, decide which exploits to use, and then launch them against the system to get a shell.

**Target: 172.17.0.0/24 Local network (Docker Container)
DO NOT EXPLOIT ANY SYSTEM THAT IS NOT ON YOUR LOCAL DOCKER NETWORK**

Command to start docker container:

docker run -it tleemcjr/metasploitable2:latest sh -c "/bin/services.sh && bash"

# Task 1

Start the docker container and rescan it with nmap. Document your results with a screenshot.

# Task 2

Find a suitable exploit for the system under test. Once you have decided on an exploit set the options and launch it. Take a screenshot of the options set and of you running the commands getuid/whoami, pwd, and ifconfig through the newly attained shell from a successful exploit.

# Task 3

Find a **second** suitable exploit for the system under test. Once you have decided on an exploit set the options and launch it. Take a screenshot of the options set and of you running the commands getuid/whoami, pwd, and ifconfig through the newly attained shell from a successful exploit.