**CS 3132 Cloud Computing Lab Report (2024-25) (Jul-Dec)**

**Student Name: Aryan Vats**

**Registration ID: BT22GCS208**

**Section: C3**

**Email ID: Aryan.vats22@st.niituniversity.in**

**Assignment Date: 05-11-2024**

**Completion Date** *(when you completed the lab assignment)***:** *14-11-2024*

**1. Lab Assignment #6:** Security Analysis and Attack Simulation in Containerized Environments Using Docker

**Objectives**:

1. Perform at least four different types of attacks (such as privilege escalation, DoS, etc.) on Docker containers.
2. Use Docker commands for introspection and analysis of docker objects (container, images)
3. Document the findings, highlighting insights gained from each simulated attack

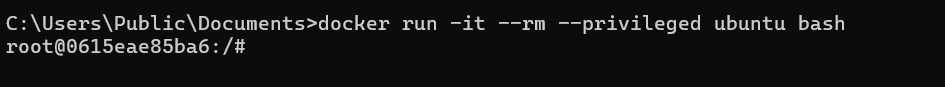
(Useful docker commands for introspection: **ps, images, version, info, management commands, events, history, inspect, logs, save, stats, top** etc.)

**2. Hardware Requirement: PC**

**3. Software Requirement:** *Docker Desktop*

**4. Lab Tasks:**

**1st) We'll attempt to perform privilege escalation in Docker:**

****

**We're using a command to check if the user has administrative privileges. To test this, we'll attempt to create a file in the /etc directory.**

**A screenshot of a computer screen

Description automatically generated**

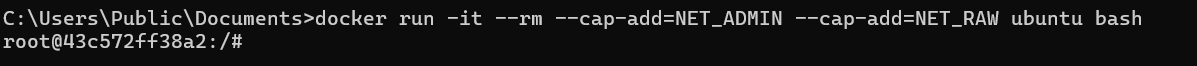
**2nd) we'll attempt a buffer overflow attack within the Docker environment:**

**A screenshot of a computer

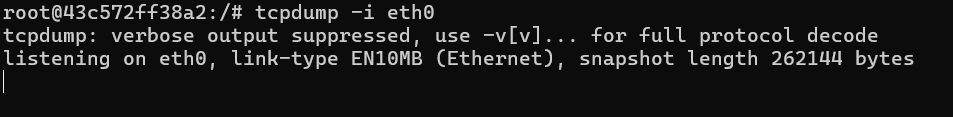
Description automatically generated**

**We reduced the CPU cores to 1 and ran a bash script that continuously creates and deletes files.**

**3rd) We are conducting network analysis:**

****

**We added capabilities that allow the creation of raw network packets and the use of low-level network tools, enabling the execution of network-related administrative tasks.**

****

**We installed tcpdump and attempted to use it, but we couldn't capture any packets, indicating that it's not functioning properly.**

**4th) Reverse shell:**

****

**In this step, we're using a Docker image with pre-configured ncat parameters and have started a listener on the specified IP.**

****

**A black background with white text

Description automatically generated**

**The reverse shell is successfully working.**

**To inspect docker images we can do the following:**

**Docker ps: Lists all running Docker containers.**

**A screenshot of a computer screen

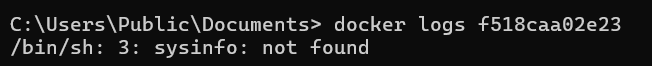
Description automatically generated**

**The docker inspect command is used to retrieve detailed information about a Docker image.**

**A screenshot of a computer

Description automatically generated**

**The docker logs command is used to display the logs of a Docker container.**

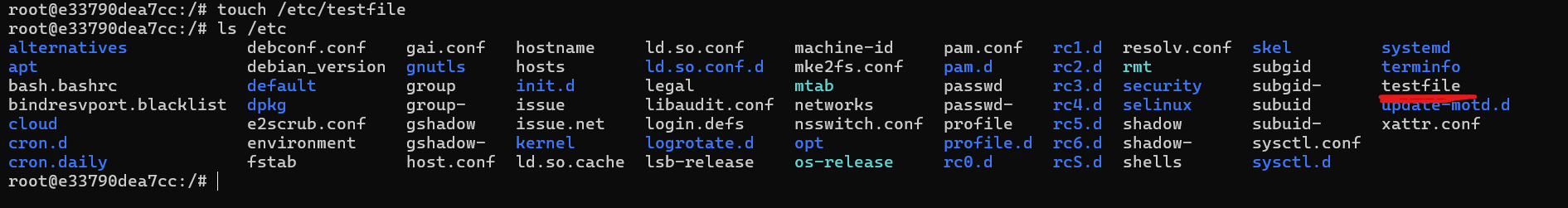
****

**5. Observations:**

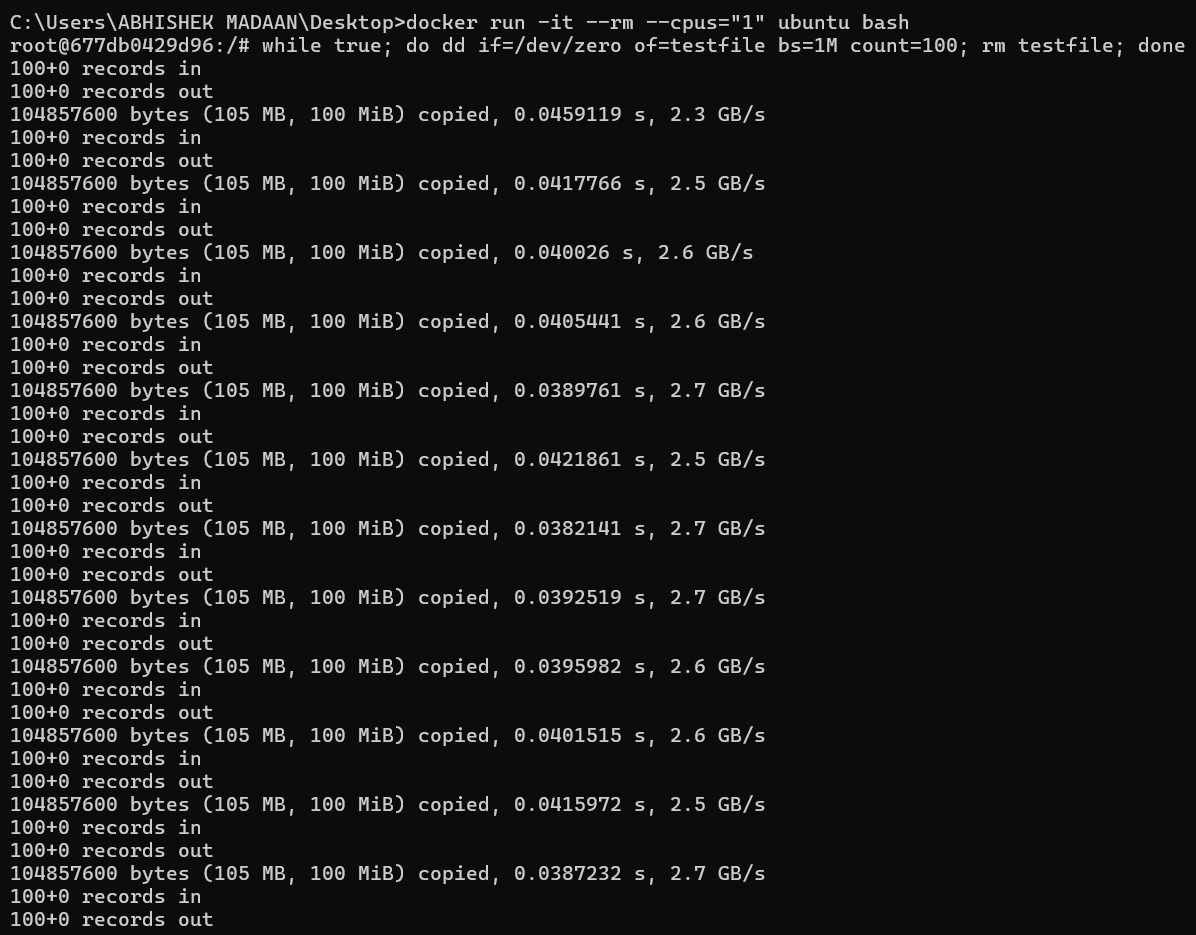
* We observed that the reverse shell, privilege escalation, and DoS attacks are working, but network analysis is not functioning*.*

**6. Results and Analysis:**

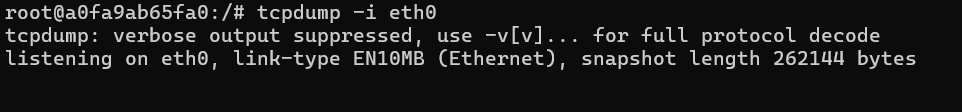
**In 1st attack:**

****

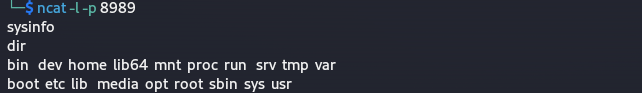
**In 2nd attack:**

****

**In 3rd attack:**

****

**In 4th attack:**

****

**7. Conclusion:**

* Incorrect configuration of the Docker image can result in serious problems*.*

**8. References:**

* [*http://chat.openai.com*](http://chat.openai.com)