# **Basic Penetration Testing Report**

### **Cover Page**

**Title:** Basic Penetration Testing on Target Machine 10.0.2.2  
 **Name:** Adithya Pramod Menon  
 **Date:** 03/06/25

## **1. Summary**

This report documents the penetration testing conducted on the target IP address 10.0.2.2. The objective was to identify vulnerabilities and attempt exploitation using various tools such as Netdiscover, Nmap, Enum4linux, Nikto, and Metasploit. The findings, including successes and failures, are discussed along with lessons learned and defense recommendations.

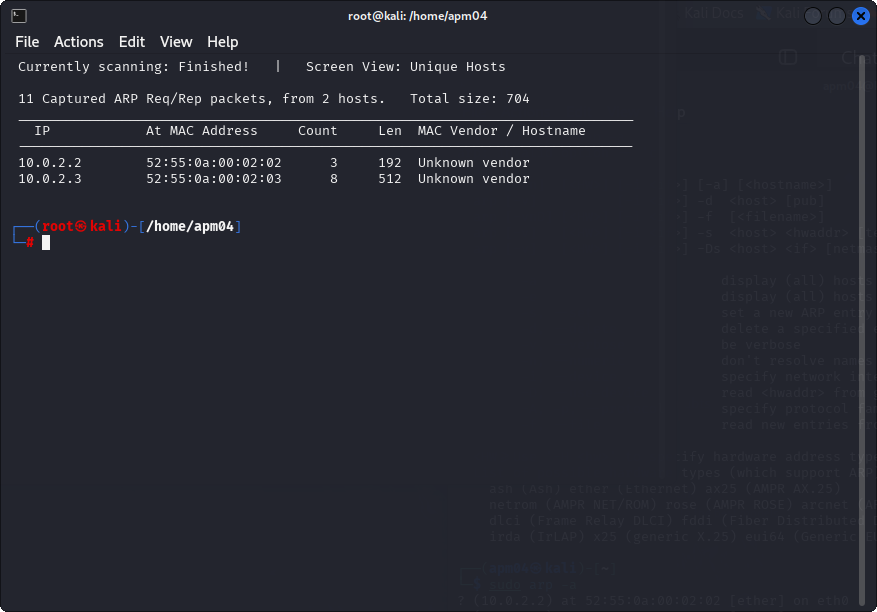
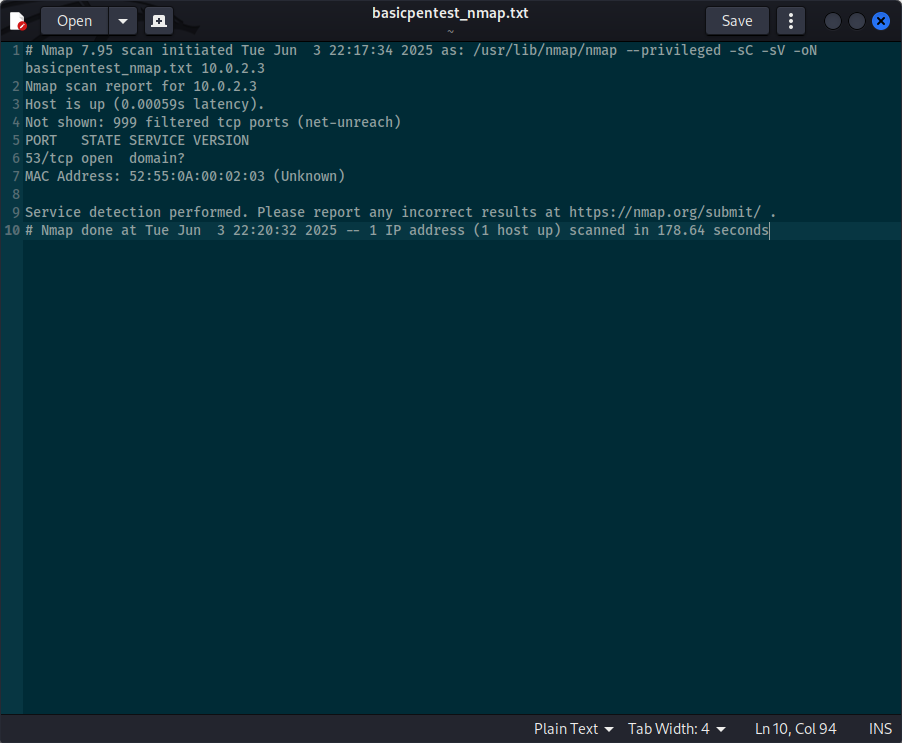
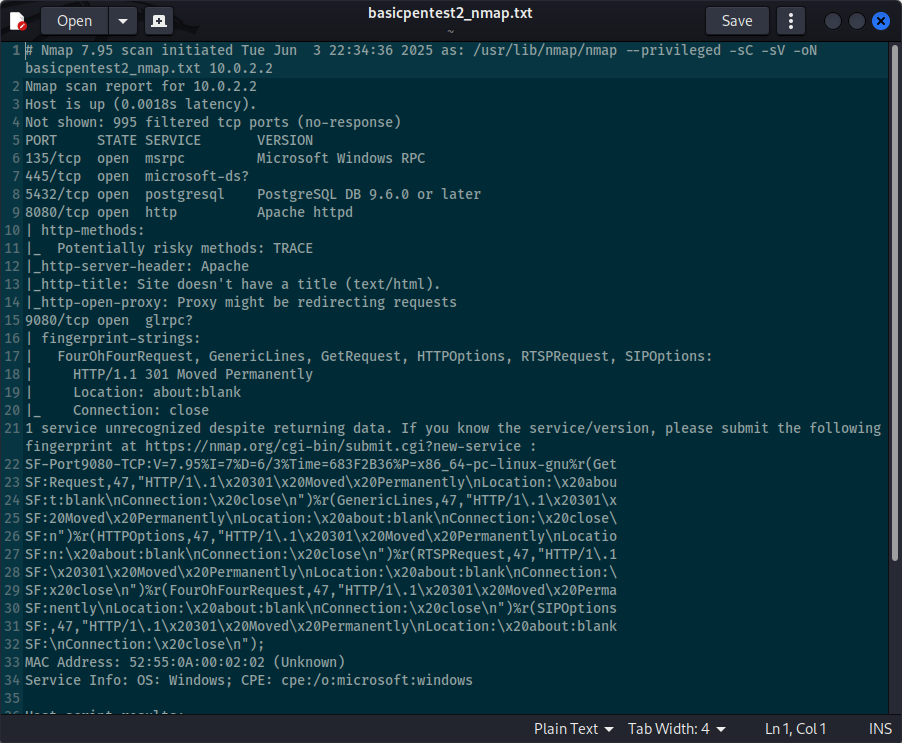
## **2. Reconnaissance & Scanning**

**Tools Used:**

* netdiscover
* nmap

**Findings:**

* Discovered live hosts at IPs 10.0.2.2 and 10.0.2.3
* Open ports on 10.0.2.2 include:  
  + 135 (msrpc)
  + 445 (microsoft-ds)
  + 5432 (PostgreSQL)
  + 8080 (Apache HTTP)
  + 9080 (HTTP)
* 10.0.2.3 only had port 53 (DNS) open.

**Screenshots:** **

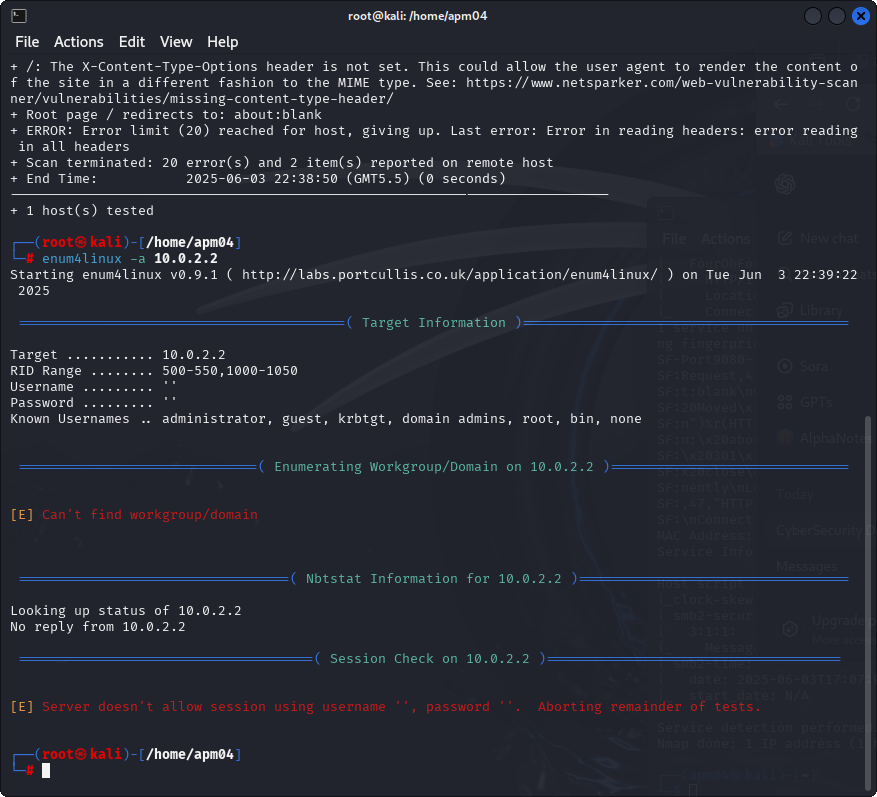
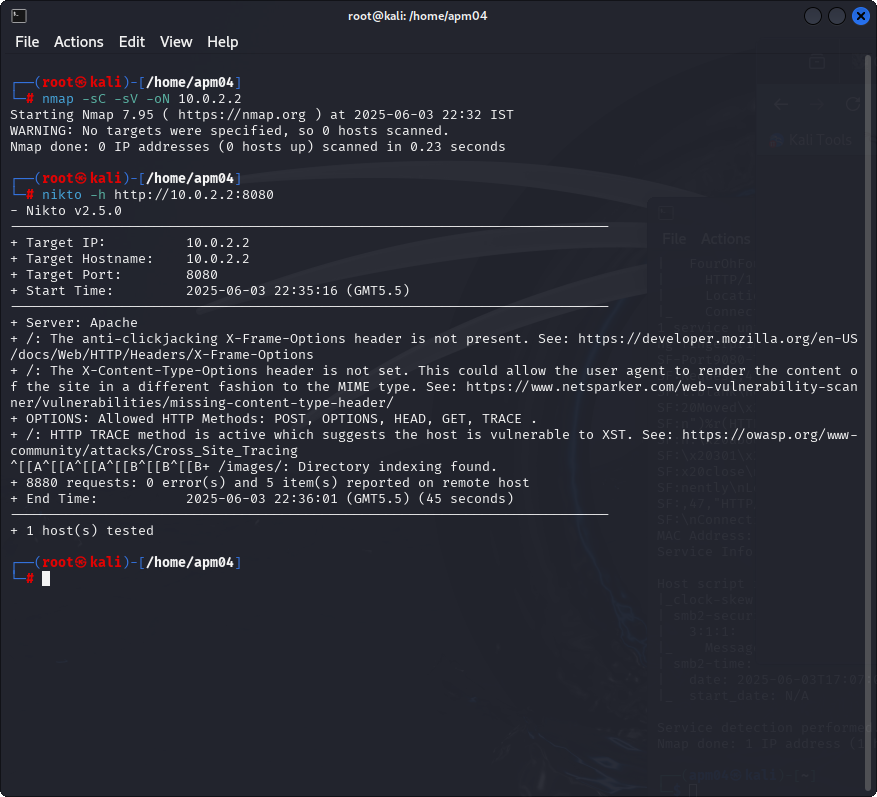
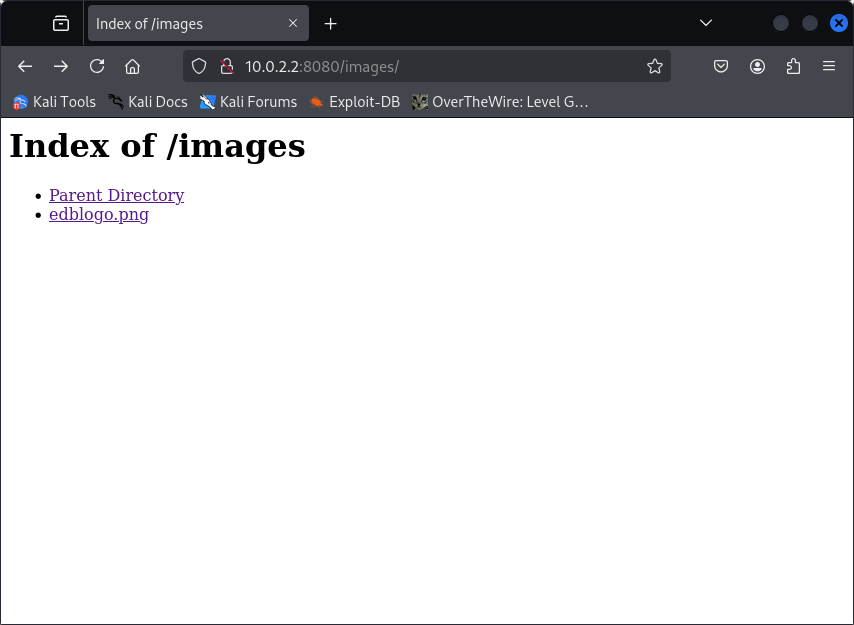
## **3. Enumeration**

**Tools Used:**

* enum4linux (for SMB enumeration)
* nikto (for web vulnerability scanning)

**Findings:**

* enum4linux revealed SMB information (see screenshot).
* nikto scan on port 8080 revealed accessible directories including /images.
* nikto scan on port 9080 returned HTTP 301 redirect to about:blank, indicating a blank page.

**Screenshots:** ** **

## **4. Exploitation**

**Metasploit Module Used:**

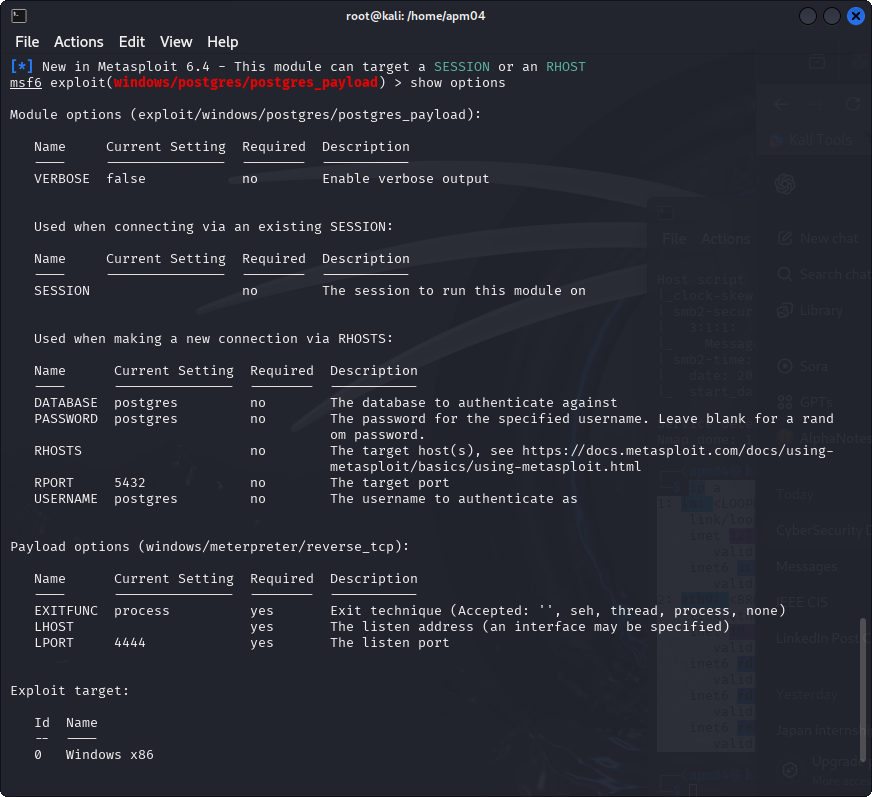
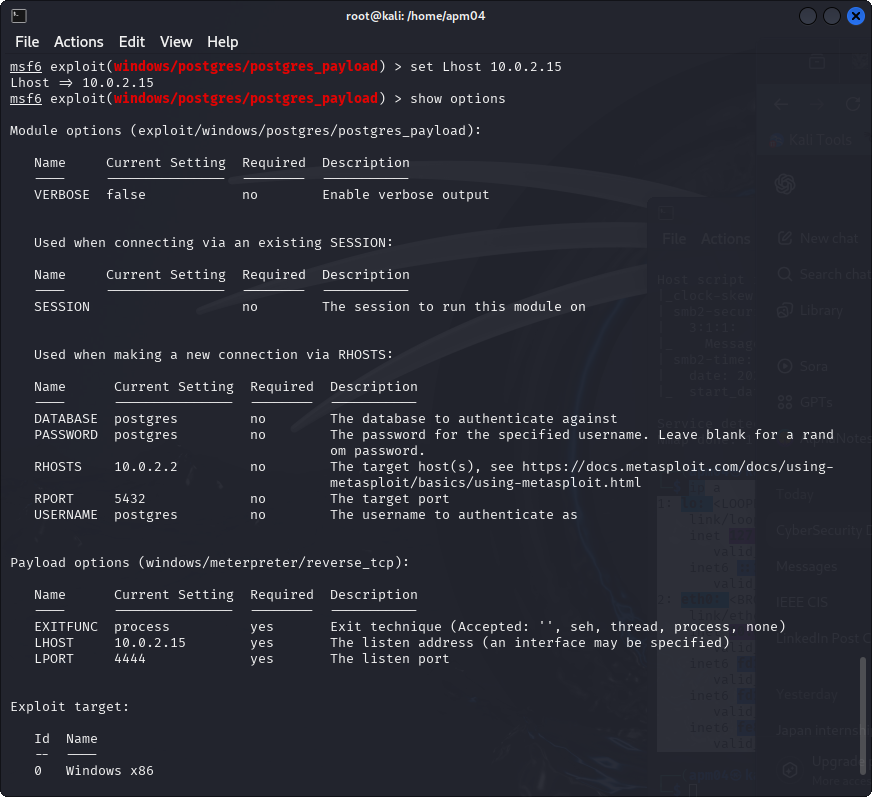
* exploit/multi/postgres/postgres\_copy\_from\_program\_cmd\_exec

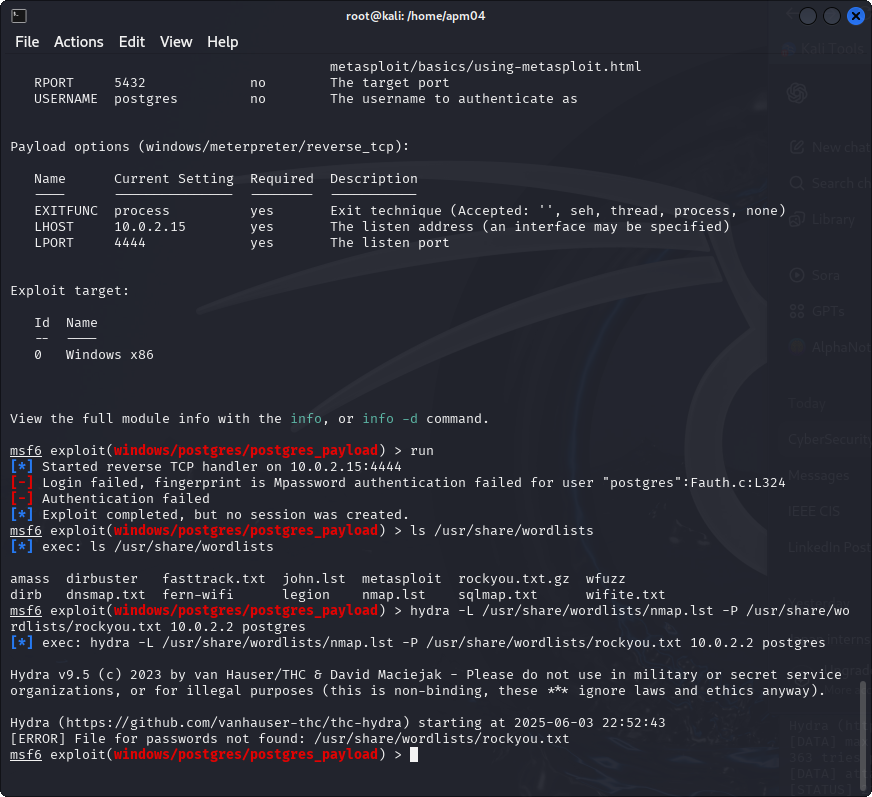
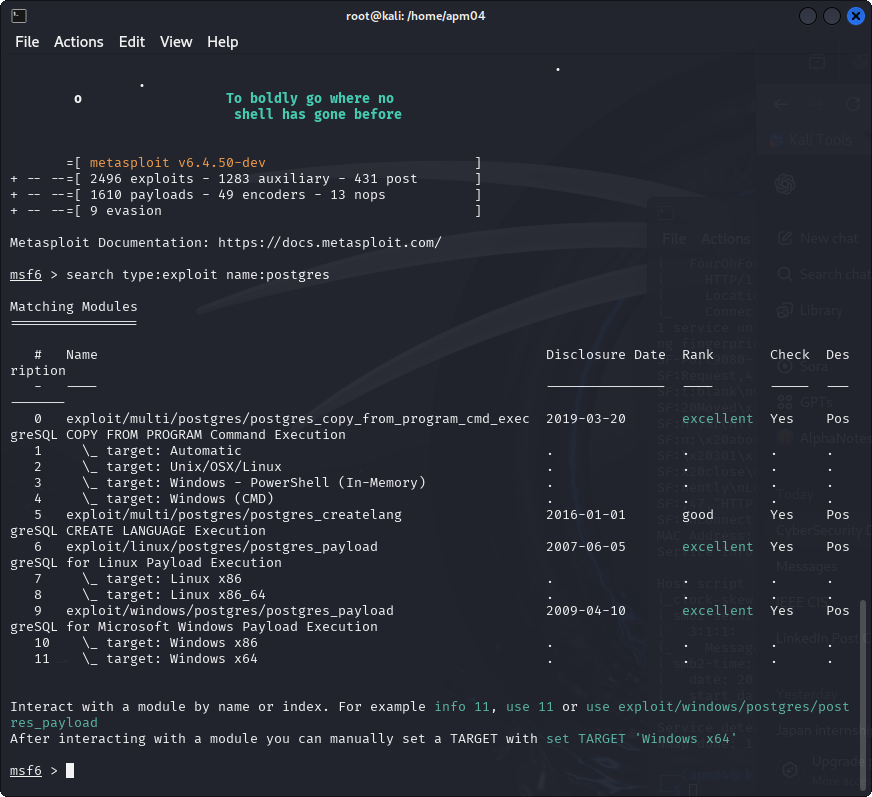
**Steps Taken:**

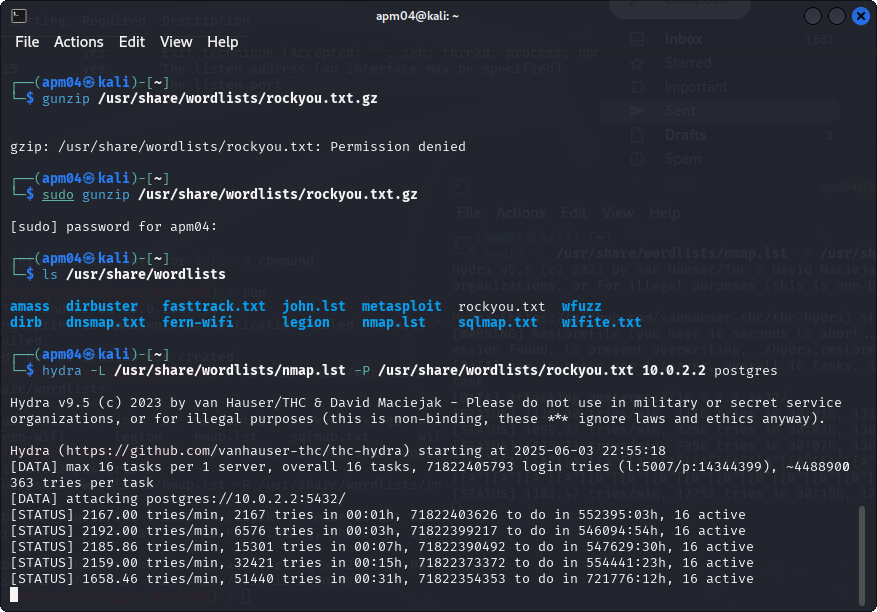
* Set RHOSTS to 10.0.2.2
* Set RPORT to 5432
* Set LHOST to attacking machine IP
* Executed exploit

**Outcome:**

* Exploit failed to provide shell access.

**Screenshots:******





## **5. Post Exploitation**

* Since shell access was not obtained, no post-exploitation commands were executed.
* No flags were captured.

## **6. Lessons Learned**

* Brute forcing PostgreSQL passwords is ineffective without strong wordlists or default credentials.
* Enumeration tools such as enum4linux and nikto provide valuable insights into accessible services and potential attack vectors.
* Exploitation may fail but still offers important information for further analysis.

## **7. Suggestions for Defense**

* Disable or restrict access to unnecessary services like SMB and PostgreSQL.
* Enforce strong passwords and limit network access for database services.
* Harden HTTP servers by disabling directory listing and restricting sensitive directories like /images.
* Monitor network logs for suspicious activity and unauthorized access attempts.