DC-3 CTF Machine

▶ DC-3 CTF Machine Walkthrough:-

Recently, I completed the DC-3 CTF machine, which was a great exercise to sharpen my penetration testing and privilege escalation skills.

🔎 Challenge Overview:-

1Difficulty: Intermediate
2)Objective: Gain root access and capture the flag.
3)Skills Tested: Web enumeration, SQL injection, privilege escalation, Linux enumeration.

Step 1:-

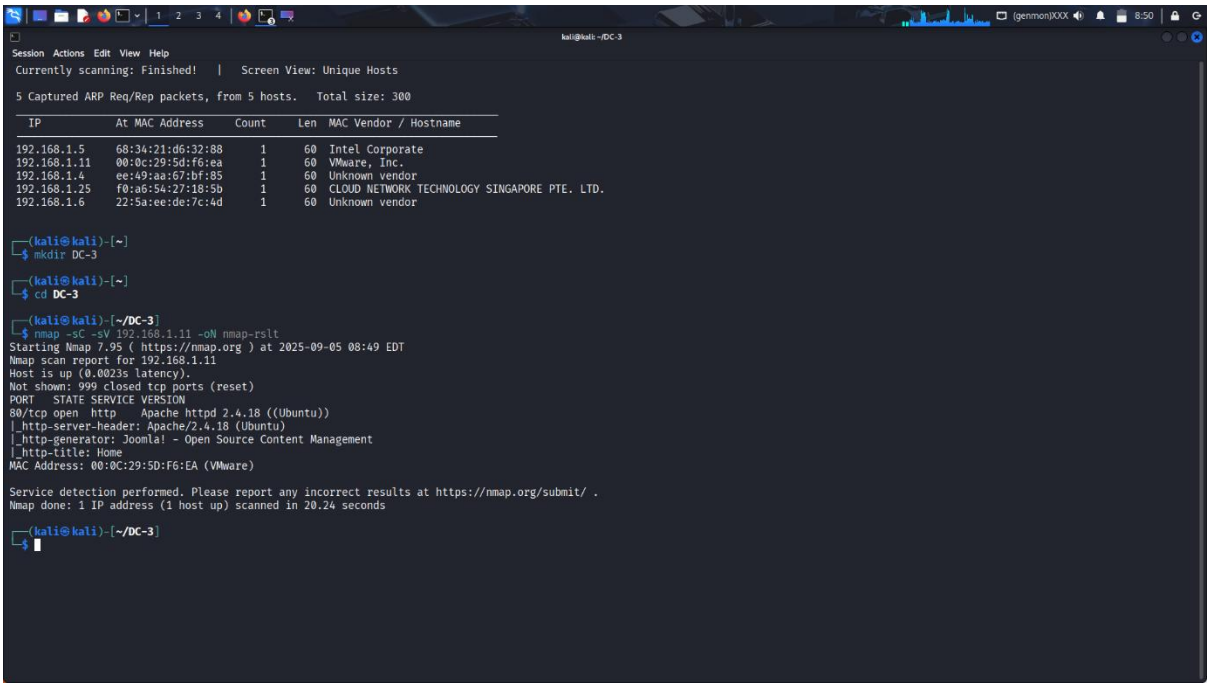
A lightweight network reconnaissance tool commonly used to identify active hosts in a network.

It's Netdiscover is a simple tool, particularly useful in Local Area Networks (LANs). It works by sending

ARP (Address Resolution Protocol) requests and listens for ARP replies to map live systems in a subnet.

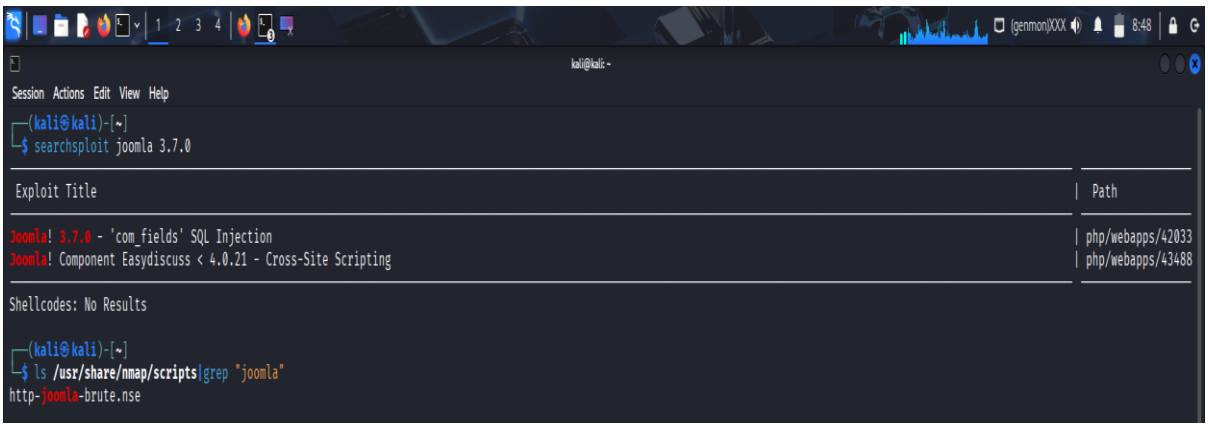
Step-2:-

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities.



Step-3:-

- **SearchSploit** is a command-line tool that comes with **Exploit Database (EDB)** package.
- It allows penetration testers and security researchers to **search through Exploit-DB locally** without needing internet access.
- Exploit-DB contains thousands of public exploits, PoCs (Proof of Concepts), and security tools



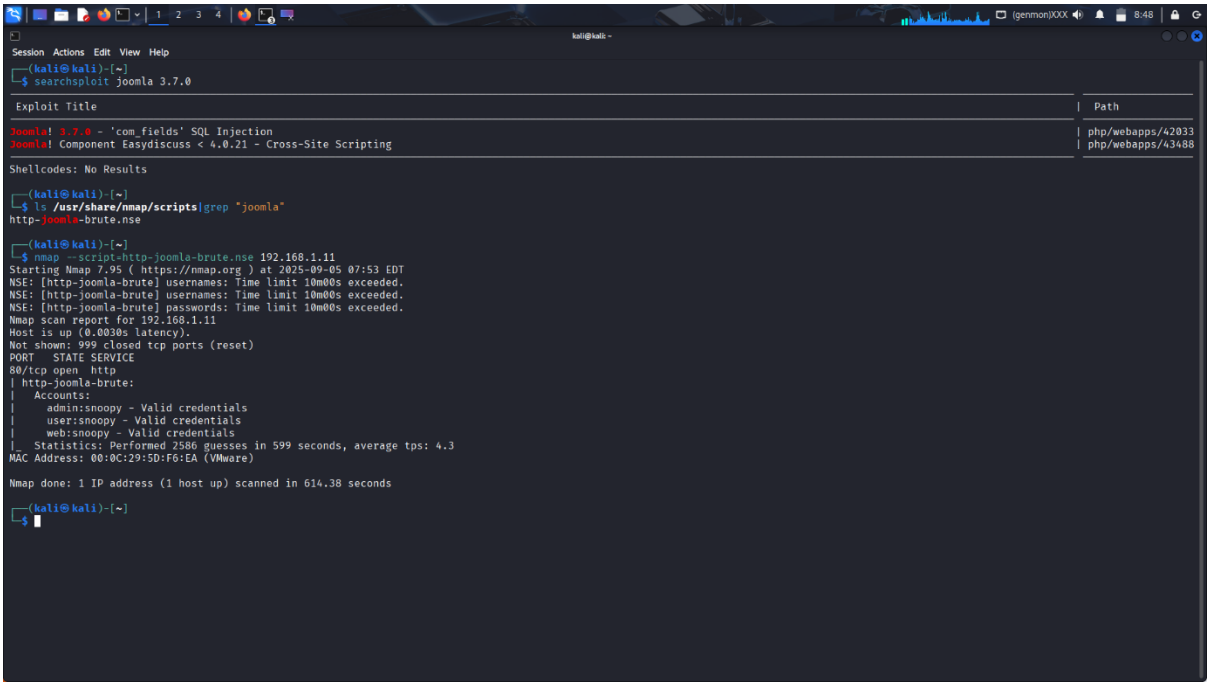
Step-4:-

nmap --script=http-enum.nse <target>

nmap → The network scanning tool.

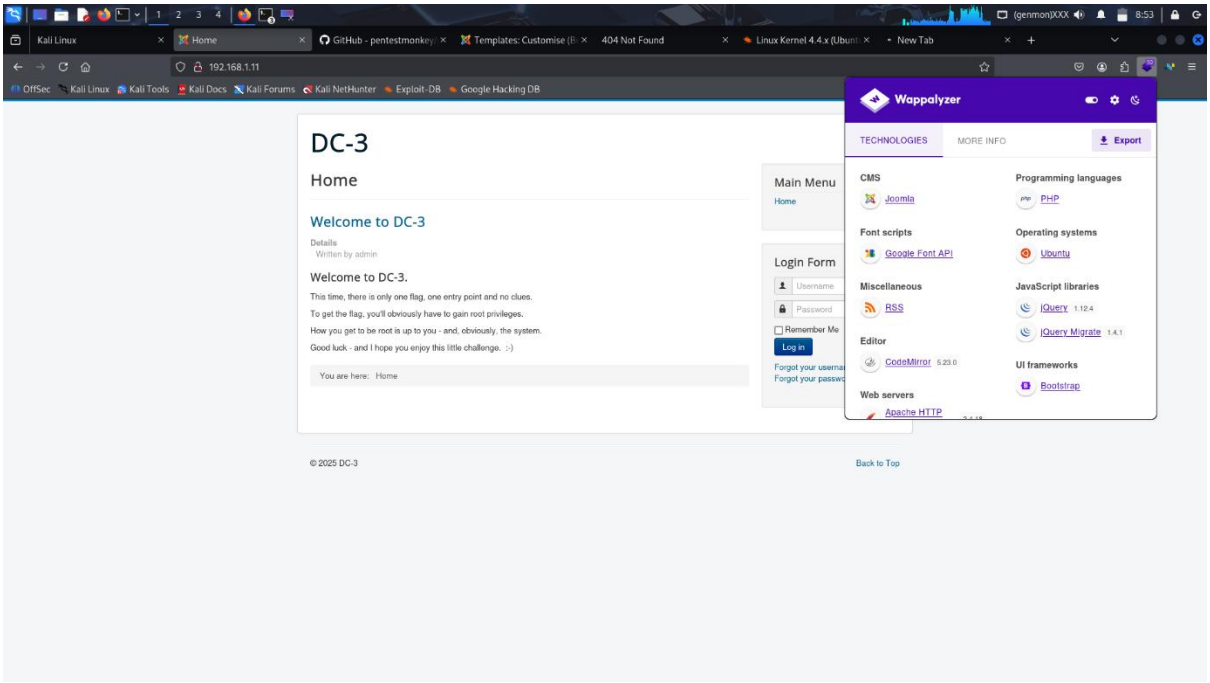
--script=http-enum.nse → Runs the Nmap Scripting Engine (NSE) script named http-enum.nse.

<target> → The IP address, domain, or hostname of the system you're scanning.



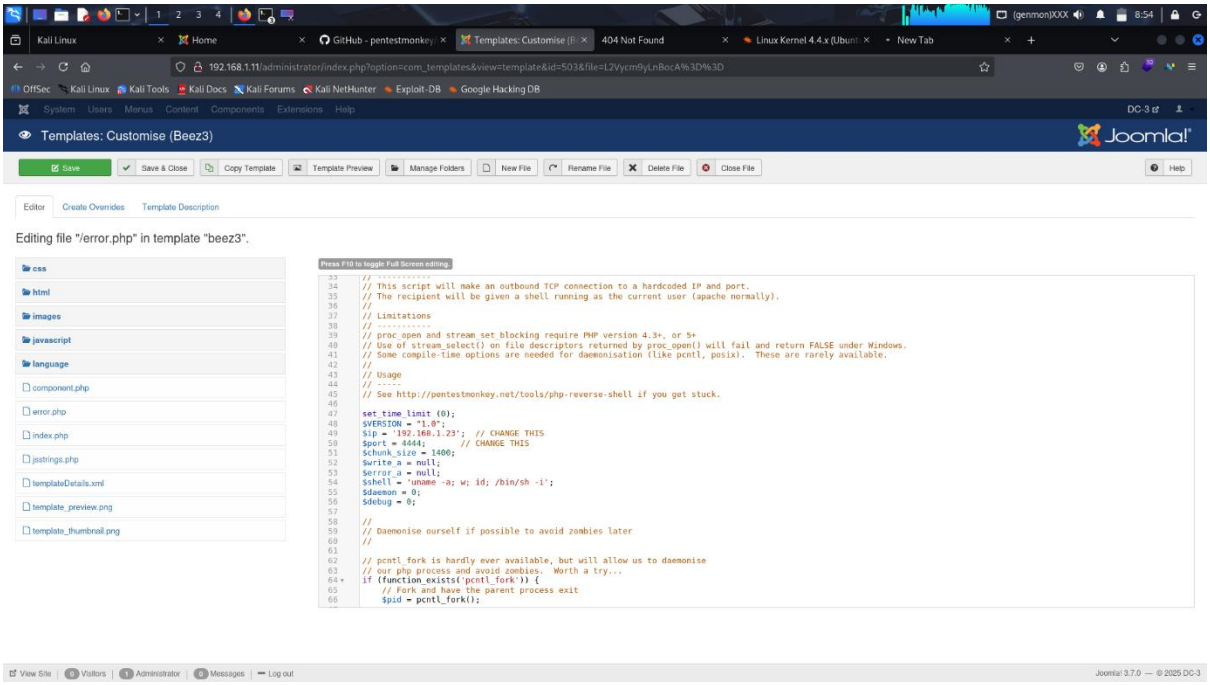
Step-5:-

DC-3 Login Home page



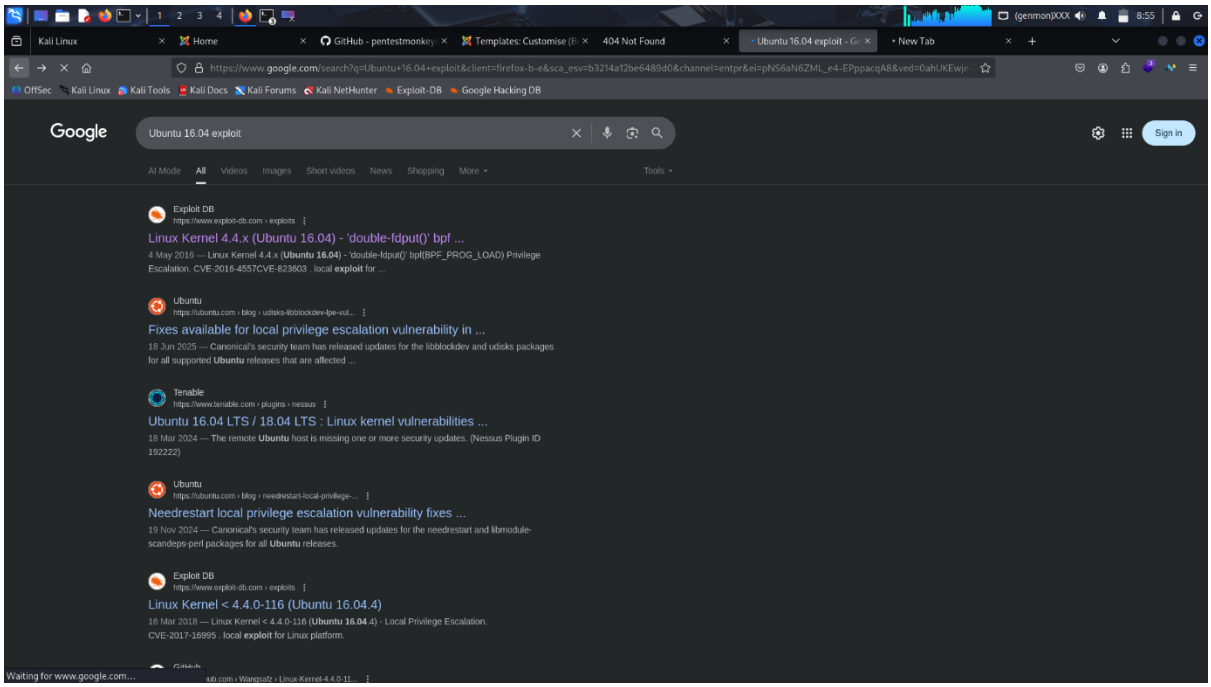
Step-6:-

192.168.1.11/administrator/index.php in these step we can change the template to beez3



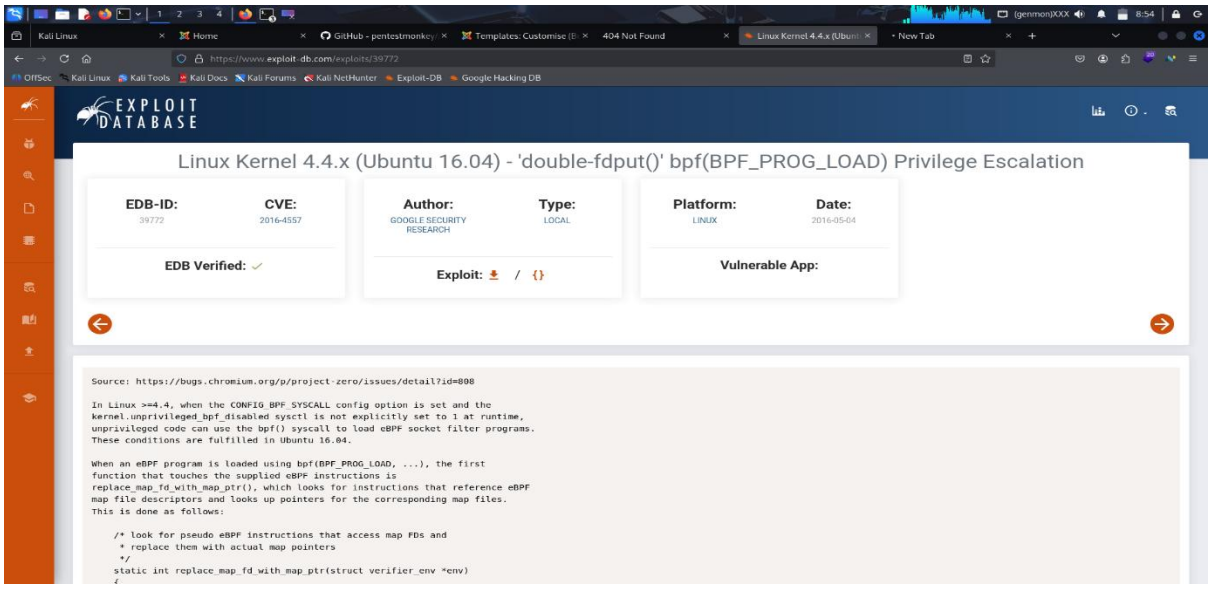
Step-7:-

First of all, we can search for an Ubuntu 16.04 exploit

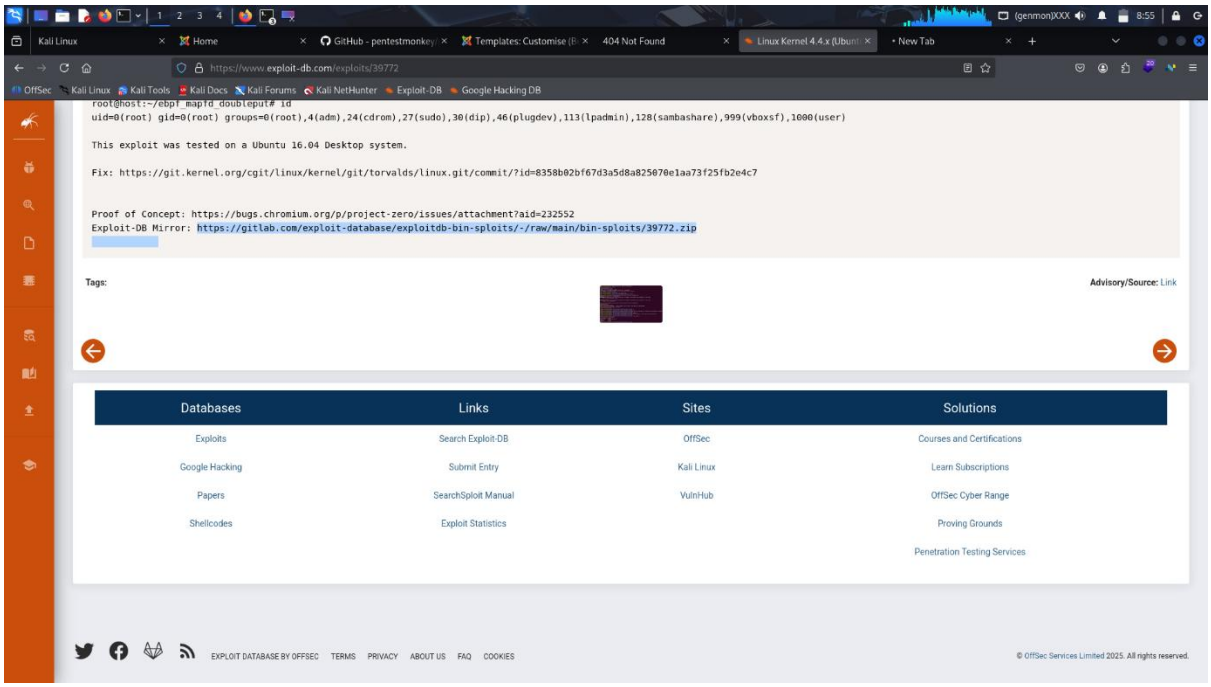


Step-8:-

In these step, we can exploit-db.com/exploit/39772

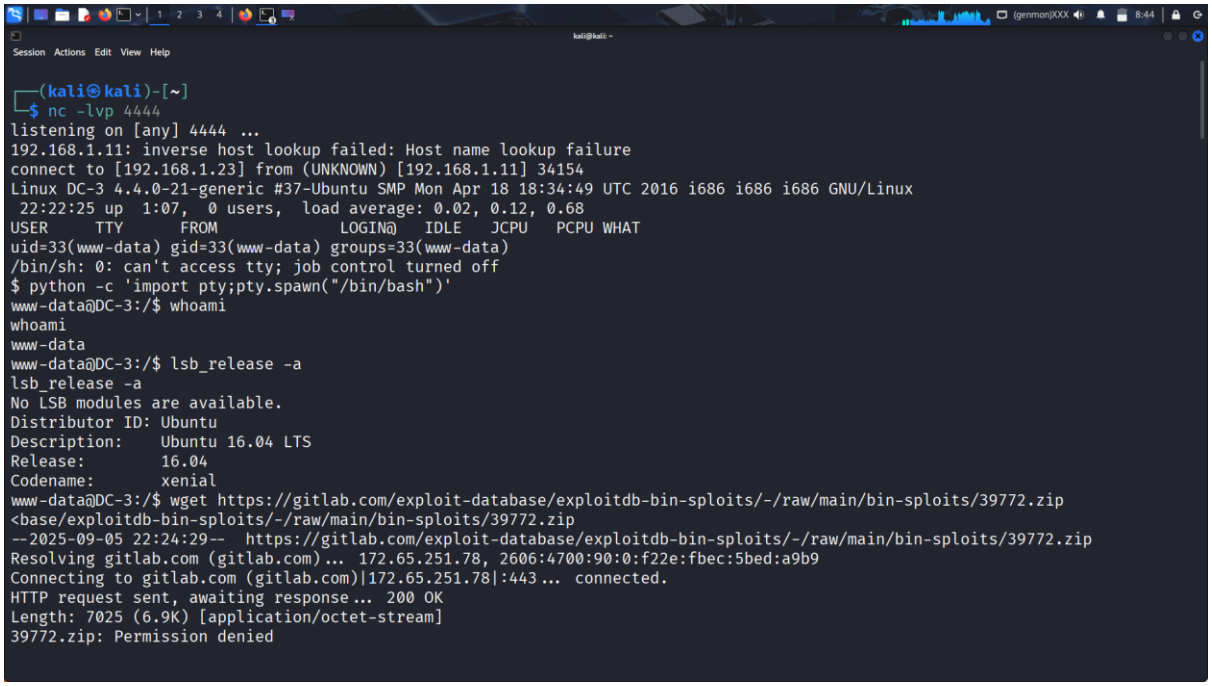


& then we get exploit

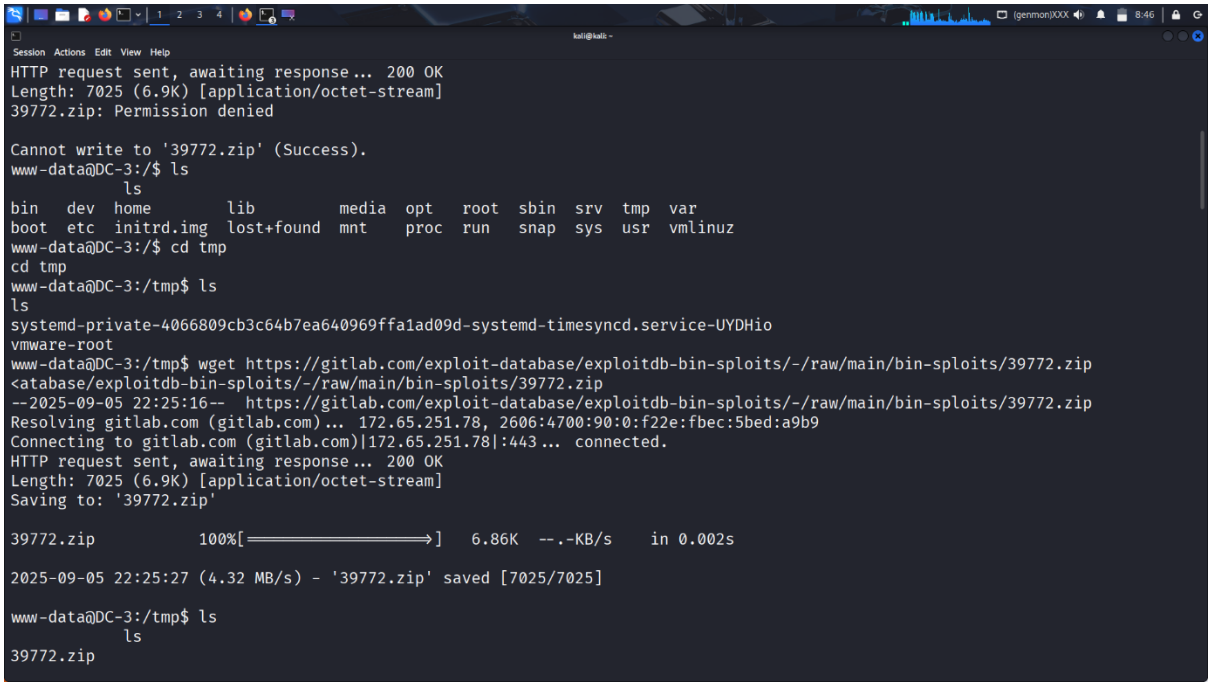


Step-9:-

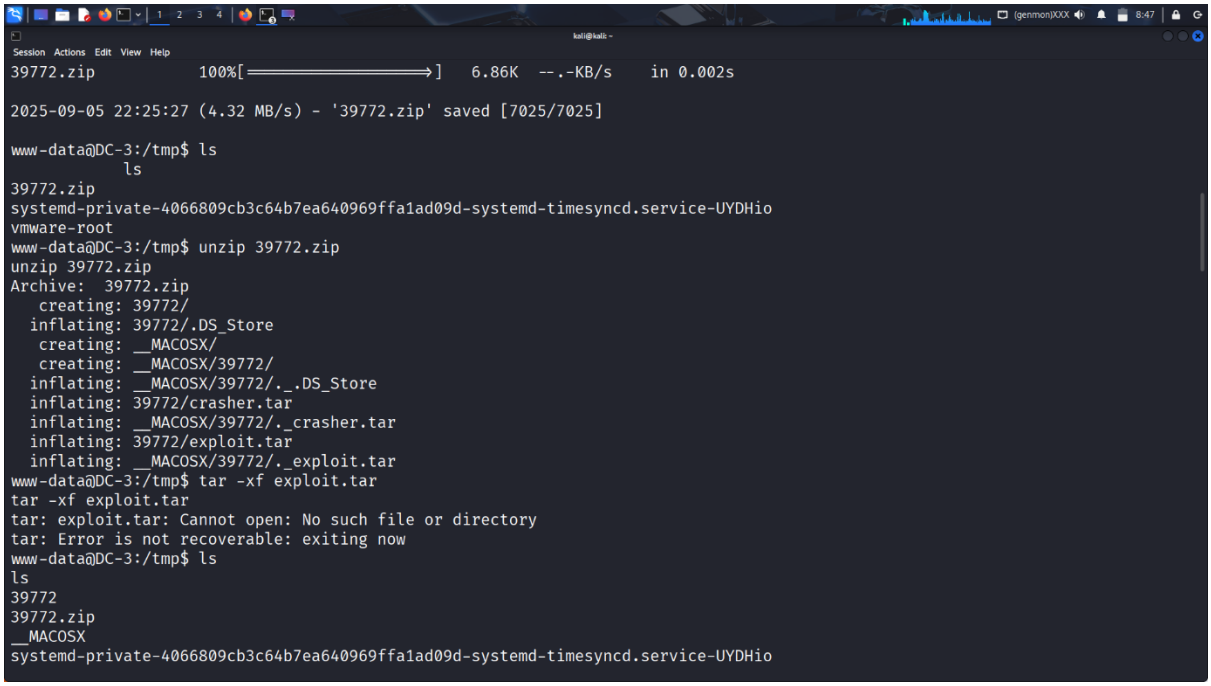
1. **`nc`**
   Stands for **Netcat**, a networking utility for reading and writing data across network connections using TCP or UDP.
2. **`-l` (listen mode)**
   - Puts Netcat in **listening mode**.
   - Instead of connecting to another host, it waits for incoming connections.
   - Example: acting like a server.
3. **`-v` (verbose)**
   - Provides **detailed output** about what Netcat is doing.
   - Helps you see connection attempts and errors.
   - Without `-v`, it runs silently.
4. **`-p 4444` (port option)**
   - Specifies the **local port** number on which Netcat should listen.
   - Here, it's `4444`.
   - You can replace `4444` with any free port (commonly used ports: `4444`, `5555`, `1337`).



Then 39772 zip. Will successfully executed



In the 39722 zip, we can get the complete data



Step-10 :-

We can get the final flag