POC Task 7

Task 7: Port Scanner Script

1. Executive Summary

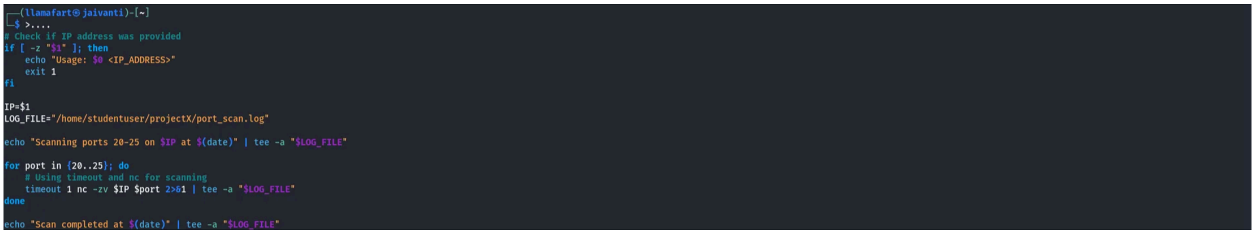
This PoC demonstrates a lightweight port scanning solution that checks common service ports (20-25) on a target IP address using timeout-based connection testing.

2. Objectives

- Develop CLI-based port scanner
- Test ports 20-25 using efficient connection methods
- Provide clear open/closed port status
- Maintain secure execution environment

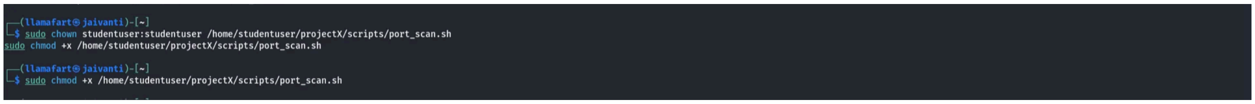
3. Implementation

3.1 Script Creation



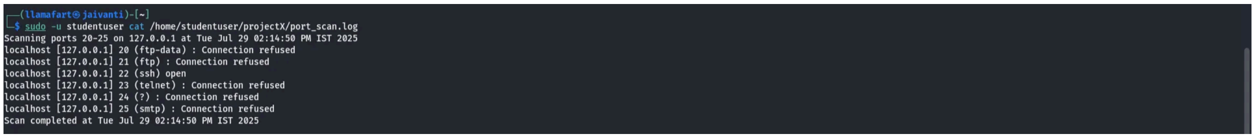
```
┌──(llamafart㉿jaivanti)-[~]
└─$ >....
# Check if IP address was provided
if [ -z "$1" ]; then
    echo "Usage: $0 <IP_ADDRESS>"
    exit 1
fi

IP=$1
LOG_FILE="/home/studentuser/projectX/port_scan.log"

echo "Scanning ports 20-25 on $IP at $(date)" | tee -a "$LOG_FILE"

for port in {20..25}; do
    # Using timeout and nc for scanning
    timeout 1 nc -zv $IP $port 2>&1 | tee -a "$LOG_FILE"
done

echo "Scan completed at $(date)" | tee -a "$LOG_FILE"
```

3.2 Permission Configuration



```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chown studentuser:studentuser /home/studentuser/projectX/scripts/port_scan.sh
sudo chmod +x /home/studentuser/projectX/scripts/port_scan.sh

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chmod +x /home/studentuser/projectX/scripts/port_scan.sh
```

3.3 Execution



```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser cat /home/studentuser/projectX/port_scan.log
Scanning ports 20-25 on 127.0.0.1 at Tue Jul 29 02:14:50 PM IST 2025
localhost [127.0.0.1] 20 (ftp-data) : Connection refused
localhost [127.0.0.1] 21 (ftp) : Connection refused
localhost [127.0.0.1] 22 (ssh) open
localhost [127.0.0.1] 23 (telnet) : Connection refused
localhost [127.0.0.1] 24 (?) : Connection refused
localhost [127.0.0.1] 25 (smtp) : Connection refused
Scan completed at Tue Jul 29 02:14:50 PM IST 2025
```

4. Conclusion:

The port scanner successfully identifies open/closed ports (20-25) on target IPs using efficient timeout-based checks while maintaining security. The lightweight solution provides clear results without requiring elevated privileges or generating excessive network traffic.