

# CyberX Security Report

Generated: 2025-10-28 08:08:28

## System Information

```
os: Linux
version: #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24)
kernel: 6.16.8+kali-amd64
hostname: NoirHat
uptime: 2:52:51
cpu: {'model': 'Intel(R) Core(TM) i5-8365U CPU @ 1.60GHz', 'cores': 4, 'threads': 8, 'usage': 38, 'frequency': '899.88 MHz'}
memory: {'total': '7.54 GB', 'used': '5.0 GB', 'available': '2.54 GB', 'usage': 66}
disks: [{"mountpoint": "/", "fstype": "ext4", "total": "64.2 GB", "used": "28.85 GB", "usage": 47}, {"mountpoint": '/boot/efi', "fstype": 'vfat', 'total': '0.95 GB', 'used': '0.0 GB', 'usage': 0}]
network: {'interfaces': [{"name": 'lo', 'type': 'ethernet', 'status': 'up', 'ip': '127.0.0.1', 'mac': ''}, {"name": 'wlan0', 'type': 'wireless', 'status': 'up', 'ip': '192.168.3.213', 'mac': ''}, {"name": 'docker0', 'type': 'ethernet', 'status': 'down', 'ip': '172.17.0.1', 'mac': ''}, {"name": 'eth0', 'type': 'ethernet', 'status': 'down', 'ip': '', 'mac': ''}], 'activeConnections': 75}
gpu: [{"name": 'None detected', 'memory': 'N/A'}]
battery: {'percent': 56.02642603931679, 'plugged_in': False, 'time_left': '2:21:49'}
top_processes: [{"pid": 1, "name": 'systemd', 'status': 'sleeping'}, {"pid": 2, "name": 'kthreadd', 'status': 'sleeping'}, {"pid": 3, "name": 'pool_workqueue_release', 'status': 'sleeping'}, {"pid": 4, "name": 'kworker/R-rcu_gp', 'status': 'idle'}, {"pid": 5, "name": 'kworker/R-sync_wq', 'status': 'idle'}, {"pid": 6, "name": 'kworker/R-kvfree_rcu_reclaim', 'status': 'idle'}, {"pid": 7, "name": 'kworker/R-slub_flushwq', 'status': 'idle'}, {"pid": 8, "name": 'kworker/R-netns', 'status': 'idle'}, {"pid": 10, "name": 'kworker/0:0H-events_highpri', 'status': 'idle'}, {"pid": 11, "name": 'kworker/0:1-events', 'status': 'idle'}]
```

## Summary

Total Issues	6
Fixed Issues	0
Open Issues	6

## Vulnerabilities

### 1. Pending OS Updates

Severity: high  
Category: os  
Status: open  
Fixable: True  
Description: There are packages available for upgrade on this system.  
Impact: Outdated packages may contain known CVEs that attackers can exploit.

### 2. Open Port 36257 (Unknown)

Severity: low  
Category: network  
Status: open  
Fixable: False  
Port: 36257  
Description: Unknown service is running on this port  
Impact: Service listening on port 36257.  
Suggested Fix: Check service on port 36257: sudo lsof -i :36257

### 3. Open Port 5000 (Dev/HTTP)

Severity: low

Category: network

Status: open

Fixable: False

Port: 5000

Description: Common dev server port (Flask, etc.). Not recommended on public interfaces.

Impact: Service listening on port 5000 (python).

Suggested Fix: Check service on port 5000: sudo lsof -i :5000

### 4. Open Port 21 (FTP)

Severity: high

Category: network

Status: open

Fixable: False

Port: 21

Description: FTP transmits credentials in cleartext; prefer SFTP/FTPS.

Impact: Service listening on port 21.

Suggested Fix: Check service on port 21: sudo lsof -i :21

### 5. Open Port 1716 (Unknown)

Severity: low

Category: network

Status: open

Fixable: False

Port: 1716

Description: Unknown service is running on this port

Impact: Service listening on port 1716 (kdeconnectd).

Suggested Fix: Check service on port 1716: sudo lsof -i :1716

### 6. Open Port 8080 (HTTP-alt)

Severity: medium

Category: network

Status: open

Fixable: False

Port: 8080

Description: Alternate HTTP port — check app security.

Impact: Service listening on port 8080 (node).

Suggested Fix: Check service on port 8080: sudo lsof -i :8080

Generated by CyberX