USB Intrusion Monitoring Report

By Imad Abdulmalik Baraja - May 26th, 2025

1. Project Overview

This project detects unauthorized USB device connections on Linux systems using real-time monitoring with udevadm and Bash scripting. The goal is to log every USB insertion event with timestamp details and notify the user immediately.

2. Tools and Technologies

- Bash Scripting
- Udevadm for device event monitoring
- System logging (logger)
- Real-time user alerts (wall)

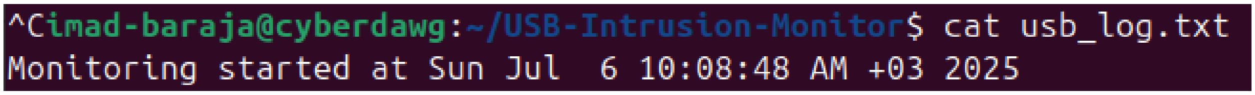
3. How It Works

- The script uses udevadm monitor filtered to the USB subsystem to listen for add events (when USB devices are connected).
- Upon detecting a device connection, it logs the event in usb_log.txt, sends a system log entry, and alerts logged-in users.
- Optional audio alert script can play a sound on detection.

4. Usage Instructions

- Place the script monitor_usb.sh in your project folder.
- Make executable: chmod +x monitor_usb.sh
- Run with sudo: sudo ./monitor_usb.sh
- Connect USB devices and observe logs and alerts.

5. Sample Log Output



```
^Cimad-baraja@cyberdawg:~/USB-Intrusion-Monitor$ cat usb_log.txt
Monitoring started at Sun Jul  6 10:08:48 AM +03 2025
```

6. Benefits & Applications

- Provides real-time monitoring for unauthorized device usage.
- Helps prevent data theft via USB devices.
- Useful for corporate endpoint security and compliance.