Linux Threat Hunt Script (Python Enhanced) Guide

# 🐍 Linux Threat Hunt Script (Python Enhanced)

\*\*Author:\*\* Charles G. | Auroch Security

\*\*Purpose:\*\* Perform advanced threat hunting on Linux systems using Python for improved control and parsing.

---

## 🔍 Checks Performed

- Suspicious processes running from `/tmp`, `/dev`, or `/var`

- User and system cron jobs

- Hidden files in key directories

- Established outbound connections

- Persistence mechanisms (`rc.local`, `init.d`, systemd timers)

- UID 0 (non-root) user accounts

- SUID/SGID files

- Recently modified files in `/etc`, `/var`, and `/tmp`

---

## 🚀 Usage

```bash

sudo python3 linux\_threat\_hunt\_enhanced.py

```

> Requires `sudo` to access protected system files and process lists.

---

## 📄 Sample Output

```

[+] Suspicious Processes:

/tmp/xminer - running under UID 1001

[+] Non-root UID 0 Users:

backdooruser has UID 0

[+] Recently Modified Files:

/etc/ssh/sshd\_config modified within last 2 days

```

---

> \*This tool is provided by Auroch Security for internal assessments, educational use, and portfolio demonstrations.\*