

**Name: Usama Habib**

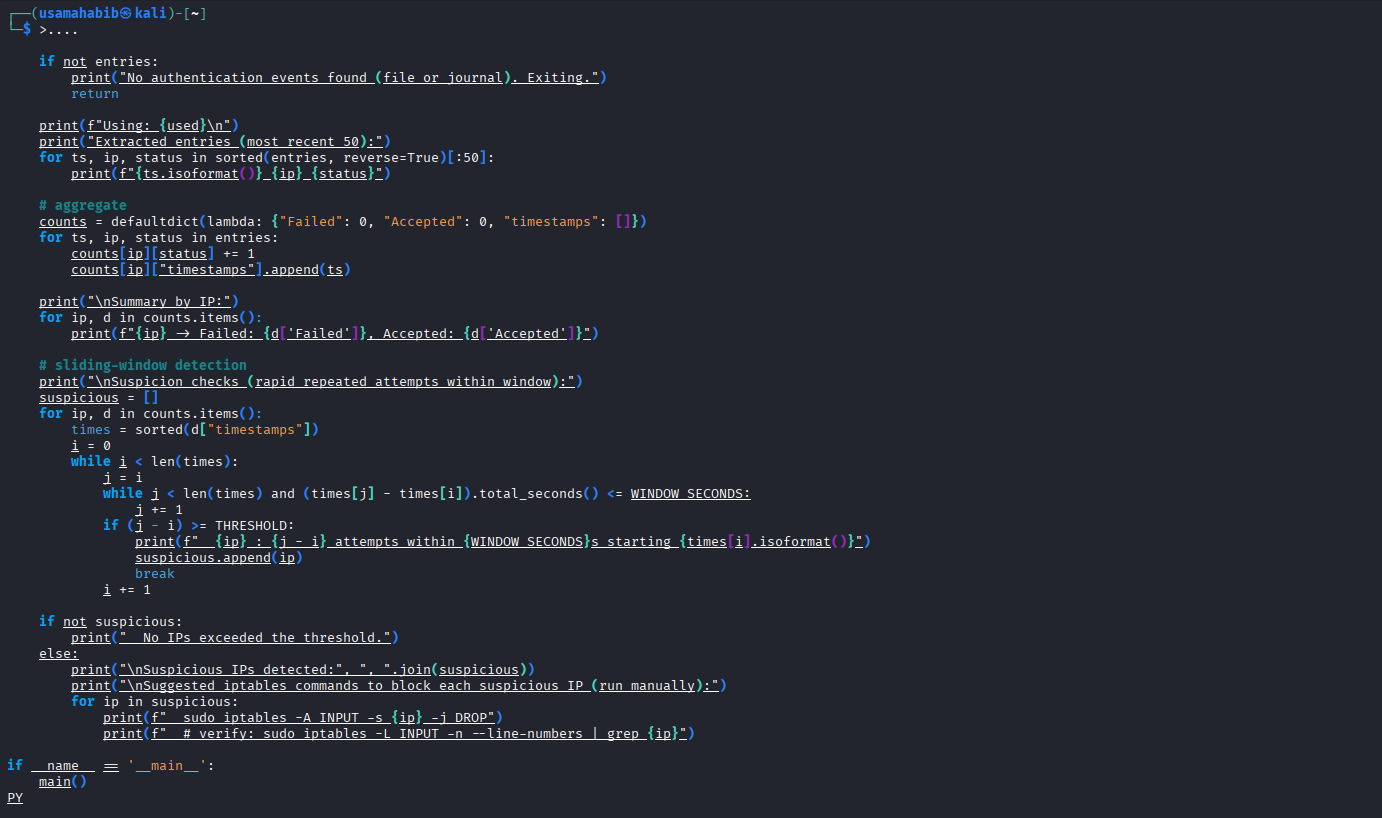
**Regno: BCSP253027**

**Course: Information Security and Forensic Lab**

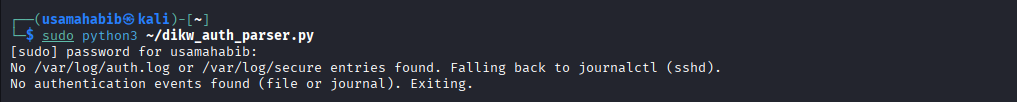
**Quiz: 1**

**Instructor: Sir, Moeez Javed**

**Practice Task 1:**



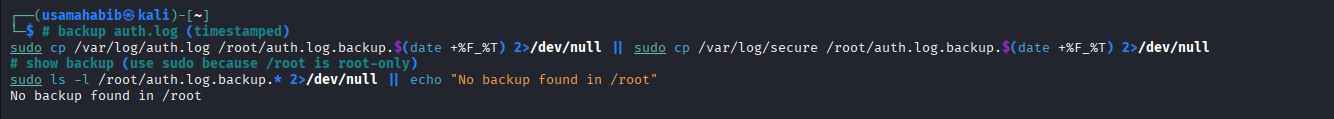
**sudo python3 ~/dikw\_auth\_parser.py**



**sudo cp /var/log/auth.log /root/auth.log.backup.$(date +%F\_%T) 2>/dev/null || sudo cp /var/log/secure /root/auth.log.backup.$(date +%F\_%T) 2>/dev/null**

**# show backup (use sudo because /root is root-only)**

**sudo ls -l /root/auth.log.backup.\* 2>/dev/null || echo "No backup found in /root"**



**sudo chown root:root /var/log/auth.log 2>/dev/null || true**

**sudo chmod 600 /var/log/auth.log 2>/dev/null || true**

**# or for /var/log/secure:**

**sudo chown root:root /var/log/secure 2>/dev/null || true**

**sudo chmod 600 /var/log/secure 2>/dev/null || true**

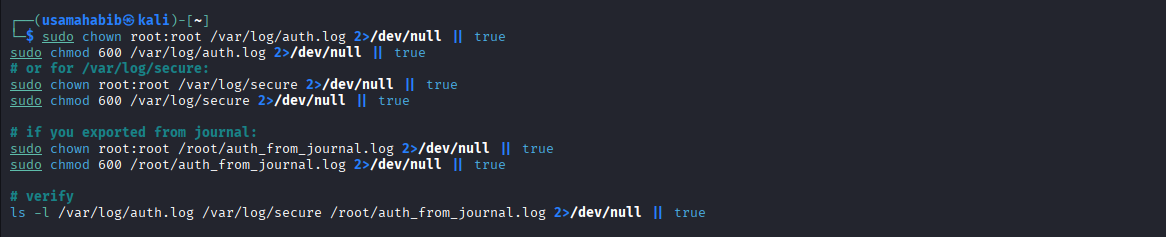
**# if you exported from journal:**

**sudo chown root:root /root/auth\_from\_journal.log 2>/dev/null || true**

**sudo chmod 600 /root/auth\_from\_journal.log 2>/dev/null || true**

**# verify**

**ls -l /var/log/auth.log /var/log/secure /root/auth\_from\_journal.log 2>/dev/null || true**

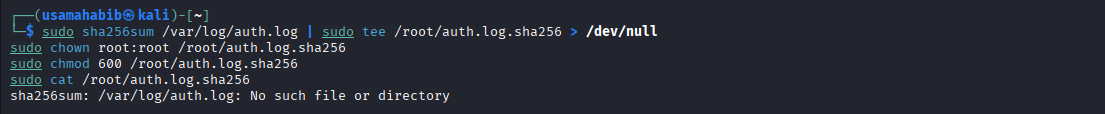


**sudo sha256sum /var/log/auth.log | sudo tee /root/auth.log.sha256 > /dev/null**

**sudo chown root:root /root/auth.log.sha256**

**sudo chmod 600 /root/auth.log.sha256**

**sudo cat /root/auth.log.sha256**



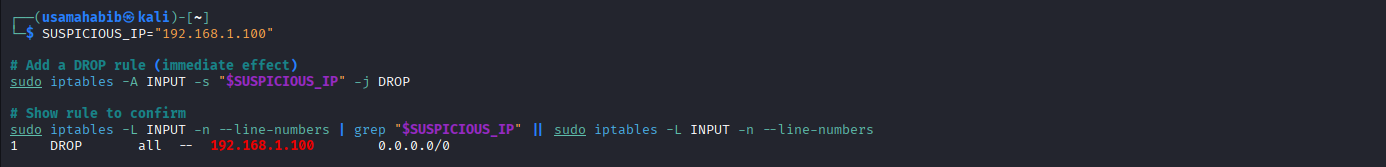
**SUSPICIOUS\_IP="192.168.1.100"**

**# Add a DROP rule (immediate effect)**

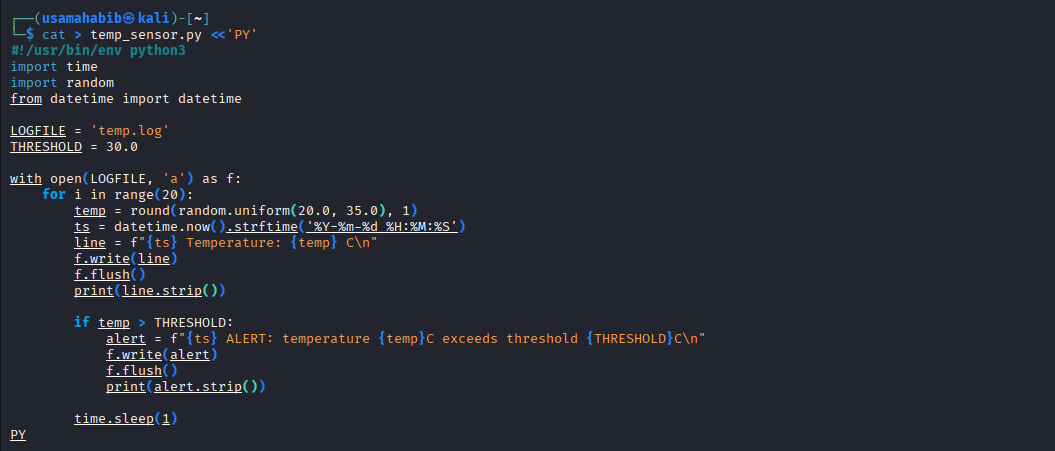
**sudo iptables -A INPUT -s "$SUSPICIOUS\_IP" -j DROP**

**# Show rule to confirm**

**sudo iptables -L INPUT -n --line-numbers | grep "$SUSPICIOUS\_IP" || sudo iptables -L INPUT -n --line-numbers**



**Practice Task 2:**



chmod +x temp\_sensor.py

python3 temp\_sensor.py

