## 🎯 Hướng dẫn tóm gọn: Từ cài đặt → Scan → Fix

### 📦 Bước 1: Cài đặt OpenSCAP

```bash

sudo dnf install -y openscap-scanner scap-security-guide

```

---

### 🔍 Bước 2: Scan hệ thống

```bash

# Tạo thư mục lưu kết quả

sudo mkdir -p /var/tmp/scap

# Chạy scan

sudo oscap xccdf eval \

--fetch-remote-resources \

--profile xccdf\_org.ssgproject.content\_profile\_cis\_server\_l1 \

--results /var/tmp/scap/scan-results.xml \

--report /var/tmp/scap/scan-report.html \

/usr/share/xml/scap/ssg/content/ssg-almalinux9-ds.xml

```

---

### 📊 Bước 3: Xem kết quả

```bash

# Đếm số lỗi

FAIL=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/scan-results.xml | grep -c "^fail$")

PASS=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/scan-results.xml | grep -c "^pass$")

echo "❌ Failed: $FAIL"

echo "✅ Passed: $PASS"

# Download report về máy local để xem

# scp suricata@192.168.1.248:/var/tmp/scap/scan-report.html ~/Desktop/

```

---

### 💾 Bước 4: Backup (BẮT BUỘC trước khi fix!)

```bash

sudo tar -czf ~/backup\_$(date +%Y%m%d\_%H%M%S).tar.gz \

/etc/ssh/ /etc/pam.d/ /etc/security/ /etc/login.defs \

/etc/sudoers /etc/sysctl.conf /etc/fstab /etc/audit/ \

2>/dev/null

sudo chown $USER:$USER ~/backup\_\*.tar.gz

ls -lh ~/backup\_\*.tar.gz | tail -1

```

---

### 🔧 Bước 5: Khắc phục tự động

```bash

# ⚠️ CẢNH BÁO: Lệnh này sẽ FIX TRỰC TIẾP hệ thống!

sudo oscap xccdf eval \

--remediate \

--fetch-remote-resources \

--profile xccdf\_org.ssgproject.content\_profile\_cis\_server\_l1 \

--results /var/tmp/scap/after-fix.xml \

--report /var/tmp/scap/after-fix.html \

/usr/share/xml/scap/ssg/content/ssg-almalinux9-ds.xml \

2>&1 | tee /tmp/fix.log

```

---

### 📊 Bước 6: So sánh kết quả

```bash

BEFORE=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/scan-results.xml | grep -c "^fail$")

AFTER=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/after-fix.xml | grep -c "^fail$")

FIXED=$((BEFORE - AFTER))

echo "📊 ===== KẾT QUẢ ====="

echo "Trước: $BEFORE lỗi"

echo "Sau: $AFTER lỗi"

echo "Đã fix: $FIXED lỗi ($(echo "scale=1; ($FIXED\*100)/$BEFORE" | bc)%)"

```

---

### 🔙 Bước 7: Restore nếu có vấn đề

```bash

# Nếu hệ thống bị lỗi, restore backup

sudo tar -xzf ~/backup\_\*.tar.gz -C /

sudo systemctl restart sshd

sudo reboot

```

---

## 🚀 Script 1 lệnh (Copy & Run)

```bash

curl -sL https://pastebin.com/raw/YOUR\_LINK > /tmp/scap\_fix.sh || cat > /tmp/scap\_fix.sh << 'EOF'

#!/bin/bash

echo "🚀 OSCAP Auto-Fix Script"

PROFILE="xccdf\_org.ssgproject.content\_profile\_cis\_server\_l1"

SCAP="/usr/share/xml/scap/ssg/content/ssg-almalinux9-ds.xml"

# 1. Install

sudo dnf install -y openscap-scanner scap-security-guide

# 2. Scan

sudo oscap xccdf eval --fetch-remote-resources --profile $PROFILE \

--results /var/tmp/scap/before.xml --report /var/tmp/scap/before.html $SCAP || true

BEFORE=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/before.xml | grep -c "^fail$")

echo "❌ Lỗi hiện tại: $BEFORE"

# 3. Backup

sudo tar -czf ~/backup\_$(date +%Y%m%d\_%H%M%S).tar.gz /etc/ssh/ /etc/pam.d/ /etc/security/ /etc/sudoers /etc/sysctl.conf /etc/fstab 2>/dev/null

sudo chown $USER:$USER ~/backup\_\*.tar.gz

# 4. Confirm

read -p "⚠️ Fix $BEFORE lỗi? (yes/NO): " CONFIRM

[ "$CONFIRM" != "yes" ] && exit 0

# 5. Fix

sudo oscap xccdf eval --remediate --fetch-remote-resources --profile $PROFILE \

--results /var/tmp/scap/after.xml --report /var/tmp/scap/after.html $SCAP | tee /tmp/fix.log

# 6. Compare

AFTER=$(sed -n 's/.\*<result>\([^<]\*\)<\/result>.\*/\1/p' /var/tmp/scap/after.xml | grep -c "^fail$")

FIXED=$((BEFORE - AFTER))

echo ""

echo "📊 Trước: $BEFORE | Sau: $AFTER | Fixed: $FIXED ($(echo "scale=1;($FIXED\*100)/$BEFORE"|bc)%)"

echo "📄 Report: /var/tmp/scap/after.html"

EOF

chmod +x /tmp/scap\_fix.sh && /tmp/scap\_fix.sh

```

---

## 📋 Profiles khác (nếu cần)

```bash

# CIS Level 2 (nghiêm ngặt hơn)

--profile xccdf\_org.ssgproject.content\_profile\_cis

# DISA STIG (cho government)

--profile xccdf\_org.ssgproject.content\_profile\_stig

# PCI-DSS (cho payment systems)

--profile xccdf\_org.ssgproject.content\_profile\_pci-dss

# HIPAA (cho healthcare)

--profile xccdf\_org.ssgproject.content\_profile\_hipaa

```

---

## ⚠️ Lưu ý quan trọng

1. ✅ \*\*Luôn backup trước khi fix\*\*

2. ✅ \*\*Có console access\*\* (nếu SSH bị lock)

3. ✅ \*\*Test SSH ngay sau khi fix\*\* - Mở terminal mới

4. ✅ \*\*Reboot\*\* sau khi fix xong để apply đầy đủ

Chạy script trên hoặc copy từng lệnh! 🎯