

Bash Scripts on Security and Compliance { DevOps }

SSH Key Rotation:

```
#!/bin/bash

# Rotate SSH keys periodically
old_key_path="/path/to/old_key"
new_key_path="/path/to/new_key"

# Generate new SSH key
ssh-keygen -t rsa -b 4096 -f $new_key_path -N ""

# Replace old key with new key
sed -i "s/$(cat $old_key_path.pub)/$(cat $new_key_path.pub)/g"
~/.ssh/authorized_keys

# Remove old keys
rm $old_key_path*
```

SSL Certificate Renewal:

```
#!/bin/bash

# Check SSL certificate expiration and renew if necessary
cert_path="/path/to/certificate.pem"
exp_date=$(date -d "$(openssl x509 -enddate -noout -in $cert_path | cut -d= -f 2)" "+%s")
cur_date=$(date "+%s")
days_left=$(( ($exp_date - $cur_date) / (60*60*24) ))

if [ $days_left -lt 30 ]; then
    echo "SSL certificate is expiring soon. Renewing..."
    # Add certificate renewal command here
    echo "SSL certificate renewed successfully."
else
    echo "SSL certificate is valid for $days_left days. No action required."
fi
```

Vulnerability Scanning and Reporting:

```
#!/bin/bash
```

```
# Run vulnerability scanning tool
echo "Running vulnerability scan..."
# Replace 'vuln_scanner' with your preferred scanning tool
vuln_scanner --output-file report.txt
echo "Vulnerability scan completed."

# Email report to relevant stakeholders
echo "Sending report to stakeholders..."
# Replace 'mail' with your email command and specify recipients
mail -s "Vulnerability Report" admin@example.com < report.txt
echo "Report sent successfully."
```

Security Patch Management:

```
#!/bin/bash
```

```
# Update system packages to apply security patches
echo "Updating system packages..."
sudo apt update
sudo apt upgrade -y
echo "System packages updated successfully."
```

Password Policy Enforcement

```
#!/bin/bash
```

```
# Check password policy compliance
if grep -q "password\s*requisite\s*pam_pwquality.so" /etc/pam.d/common-
password; then
    echo "Password policy is compliant."
else
    echo "Password policy is not compliant. Updating..."
    echo "password requisite pam_pwquality.so retry=3 minlen=12 difok=3
ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1" | sudo tee -a /etc/pam.d/common-
password > /dev/null
    echo "Password policy updated successfully."
fi
```

Follow: [Amos Koech DevOps](#)