**Key Features**

**1. Password Generation Tools**

* Random password generation using /dev/urandom and base64
* OpenSSL-based password generation
* Passphrase creation using dictionary words
* pwgen integration for secure password generation

**2. Password Strength Analysis**

* Built-in password analysis function
* Character type detection (uppercase, lowercase, numbers, symbols)
* Length-based strength assessment
* Real-time testing of sample passwords

**3. System Security Checks**

* Password aging information analysis
* Password policy configuration review
* Failed login attempt monitoring
* Password hash algorithm verification

**4. Network-Based Testing**

* Integration with online password strength checkers
* Have I Been Pwned API integration
* Breach database checking capabilities

**5. Security Monitoring**

* Authentication log analysis
* User session monitoring
* Suspicious activity detection
* System user audit functionality

**Usage Instructions**

**Make the script executable:**

chmod +x password\_security\_tools.sh

**Run the complete analysis:**

./password\_security\_tools.sh

**Run specific sections (modify the script as needed):**

# Generate passwords only  
./password\_security\_tools.sh | head -50  
  
# Security audit only  
grep -A 20 "SECURITY AUDIT" password\_security\_tools.sh

**Additional Linux Commands for Password Security**

The script also includes these essential Linux security commands:

# Password generation  
openssl rand -base64 32  
head -c 32 /dev/urandom | base64  
  
# Security monitoring  
last -n 10  
who  
w  
lastb -n 10  
  
# Password policy checks  
chage -l username  
grep "^username:" /etc/shadow  
  
# System hardening  
passwd -l username # Lock account  
passwd -u username # Unlock account  
chage -d 0 username # Force password change