Set 2: Script for Automating Security Audits and Server Hardening on Linux Servers

```bash
#!/bin/bash

# Colors for reporting
RED='\033[0;31m'
GREEN='\033[0;32m'
YELLOW='\033[1;33m'
NC='\033[0m' # No Color

# Log file
LOGFILE="/var/log/security_audit.log"
SUMMARY_REPORT="/var/log/security_audit_summary.log"
CONFIG_FILE="/etc/security_audit.conf"

# Email settings
EMAIL_ALERTS_ENABLED=false
EMAIL_RECIPIENT="admin@example.com"

# Helper function to log output
log() {
  echo -e "$1" | tee -a "$LOGFILE"
}

# Helper function to log summary report
log_summary() {
  echo -e "$1" | tee -a "$SUMMARY_REPORT"
}

# 1. User and Group Audits
```

```
user_group_audit() {
    log "${YELLOW}--- User and Group Audits ---${NC}"

    # List all users and groups
    log "${GREEN}Listing all users:${NC}"
    cut -d: -f1 /etc/passwd | tee -a "$LOGFILE"

    log "${GREEN}Listing all groups:${NC}"
    cut -d: -f1 /etc/group | tee -a "$LOGFILE"

    # Check for users with UID 0
    log "${GREEN}Users with UID 0:${NC}"
    awk -F: '($3 == 0) {print $1}' /etc/passwd | tee -a "$LOGFILE"

    # Check for users without passwords or with weak passwords
    log "${GREEN}Users without a password:${NC}"
    awk -F: '($2 == "" ) { print $1 }' /etc/shadow | tee -a "$LOGFILE"
}

# 2. File and Directory Permissions
file_permission_audit() {
    log "${YELLOW}--- File and Directory Permissions ---${NC}"

    # World-writable files
    log "${GREEN}World-writable files:${NC}"
    find / -xdev -type f -perm -o+w -exec ls -l {} \; | tee -a "$LOGFILE"

    # SUID/SGID files
    log "${GREEN}SUID/SGID files:${NC}"
    find / -xdev \( -perm -4000 -o -perm -2000 \) -type f -exec ls -l {} \; | tee -a "$LOGFILE"
    # SSH directory permissions
    log "${GREEN}.ssh directory permissions:${NC}"
    find /home -type d -name ".ssh" -exec ls -ld {} \; | tee -a "$LOGFILE"
}

# 3. Service Audits
service_audit() {
    log "${YELLOW}--- Service Audits ---${NC}"

    # List all running services
    log "${GREEN}Running services:${NC}"
    systemctl list-units --type=service --state=running | tee -a "$LOGFILE"

    # Ensure critical services are running
    log "${GREEN}Checking critical services:${NC}"
    for service in sshd iptables; do
        if systemctl is-active --quiet "$service"; then
            log "${service} is running"
        else
            log "${RED}${service} is not running!${NC}"
        fi
    done
}

# 4. Firewall and Network Security
network_security_audit() {
    log "${YELLOW}--- Firewall and Network Security ---${NC}"

    # Check if firewall is active
    log "${GREEN}Checking firewall status:${NC}"
    if systemctl is-active --quiet firewalld || systemctl is-active --quiet iptables; then
```

```
        log "Firewall is active"
    else
        log "${RED}Firewall is not active!${NC}"
    fi

    # List open ports and services
    log "${GREEN}Open ports and associated services:${NC}"
    ss -tuln | tee -a "$LOGFILE"

    # Check for IP forwarding
    log "${GREEN}IP forwarding status:${NC}"
    sysctl net.ipv4.ip_forward | tee -a "$LOGFILE"
}

# 5. IP and Network Configuration Checks
ip_network_check() {
    log "${YELLOW}--- IP and Network Configuration Checks ---${NC}"

    # Public vs. Private IP Checks
    log "${GREEN}IP addresses (Public vs. Private):${NC}"
    ip addr show | grep "inet " | tee -a "$LOGFILE"
}

# 6. Security Updates and Patching
security_updates_check() {
    log "${YELLOW}--- Security Updates and Patching ---${NC}"

    # Check for available updates
    log "${GREEN}Checking for available updates:${NC}"
    yum check-update | tee -a "$LOGFILE"
}
```

```
# 7. Log Monitoring
log_monitoring() {
  log "${YELLOW}--- Log Monitoring ---${NC}"

  # Check recent suspicious log entries
  log "${GREEN}Checking for suspicious log entries:${NC}"
  grep "Failed password" /var/log/secure | tail -n 10 | tee -a "$LOGFILE"
}

# 8. Server Hardening Steps
server_hardening() {
  log "${YELLOW}--- Server Hardening ---${NC}"

  # SSH Configuration
  log "${GREEN}Configuring SSH:${NC}"
  sed -i 's/#PermitRootLogin.*/PermitRootLogin no/' /etc/ssh/sshd_config
  sed -i 's/PasswordAuthentication.*/PasswordAuthentication no/' /etc/ssh/sshd_config
  systemctl reload sshd

  # Disable IPv6
  log "${GREEN}Disabling IPv6:${NC}"
  sysctl -w net.ipv6.conf.all.disable_ipv6=1
  sysctl -w net.ipv6.conf.default.disable_ipv6=1
  sysctl -w net.ipv6.conf.lo.disable_ipv6=1

  # Set GRUB password
  log "${GREEN}Setting GRUB password:${NC}"
  # Uncomment and set the password after generating it using `grub2-mkpasswd-pbkdf2`

  # Configure automatic updates
```

```
    log "${GREEN}Configuring automatic updates:${NC}"
    yum install -y yum-cron
    systemctl enable yum-cron
    systemctl start yum-cron
}

# 9. Custom Security Checks
custom_security_checks() {
    log "${YELLOW}--- Custom Security Checks ---${NC}"

    if [[ -f "$CONFIG_FILE" ]]; then
        while IFS= read -r check; do
            if [[ "$check" =~ ^# || -z "$check" ]]; then
                continue
            fi
            log "${GREEN}Running custom check: ${check}${NC}"
            eval "$check" | tee -a "$LOGFILE"
        done < "$CONFIG_FILE"
    else
        log "${RED}Custom configuration file not found: ${CONFIG_FILE}${NC}"
    fi
}

# 10. Reporting and Alerting
generate_summary_report() {
    log_summary "${YELLOW}--- Security Audit Summary Report ---${NC}"

    log_summary "Users with UID 0:"
    awk -F: '($3 == 0) {print $1}' /etc/passwd | tee -a "$SUMMARY_REPORT"

    log_summary "World-writable files:"
    find / -xdev -type f -perm -o+w | tee -a "$SUMMARY_REPORT"

    log_summary "SUID/SGID files:"
    find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | tee -a "$SUMMARY_REPORT"

    log_summary "Running services:"
    systemctl list-units --type=service --state=running | tee -a "$SUMMARY_REPORT"

    # Send email alert if enabled
    if $EMAIL_ALERTS_ENABLED; then
        log "${GREEN}Sending email alert to ${EMAIL_RECIPIENT}${NC}"
        mail -s "Security Audit Report" "$EMAIL_RECIPIENT" < "$SUMMARY_REPORT"
    fi
}

# Main Execution
main() {
    user_group_audit
    file_permission_audit
    service_audit
    network_security_audit
    ip_network_check
    security_updates_check
    log_monitoring
    server_hardening
    custom_security_checks
    generate_summary_report
    log "${GREEN}Security audit and server hardening complete. Please review ${LOGFILE} and ${SUMMARY_REPORT} for details.${NC}"
}
```

```
# Run the script

main
```