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

1.# 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"
```

Explination:-

 Colors: Define color codes for text formatting in the terminal output.

 Log File: LOGFILE and SUMMARY_REPORT are used to store detailed logs and summary reports respectively.

 Configuration File: CONFIG_FILE holds custom security checks.

 Email Settings: EMAIL_ALERTS_ENABLED determines if email alerts should be sent, and EMAIL_RECIPIENT is the recipient of those alerts

```
# 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"
```

}

Explination:-

- **log**: Writes messages to both the terminal and the LOGFILE.
- **log_summary**: Writes messages to both the terminal and the SUMMARY_REPORT

2.User and Group Audits:-

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

3. # 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"
}
```

Explination:-

User and Group Audits: Lists all users and groups, identifies users with UID 0 (typically root), and checks for users with no passwords or weak passwords.

4.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"
}
```

Explination:-

File and Directory Permissions: Finds world-writable files, files with SUID/SGID bits set (potentially insecure), and checks permissions on .ssh directories

5.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
}
```

Explination:-

Service Audits: Lists all running services and checks if critical services (like sshd and iptables) are active.

6. 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"
}
```

Explination:-

Firewall and Network Security: Checks if the firewall is active, lists open ports and services, and checks IP forwarding status.

8. 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"
}
```

Explination:-

IP and Network Configuration Checks: Lists the IP addresses on the system and differentiates between public and private IPs.

9. 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"
}
```

10. 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"
}
```

Explination:-

Log Monitoring: Looks for recent failed login attempts in the system logs.

11. 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
}
```

Explination:-

Server Hardening:

- Configures SSH to disable root login and password authentication.
- Disables IPv6.
- Provides a placeholder for setting a GRUB password.
- Configures automatic updates with yum-cron.

11. 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}"
```

Custom Security Checks: Runs additional custom checks defined in CONFIG_FIL

12. 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
```