Linux

- 核查与访谈（_____yum）_
- 核查与访谈（_____APT）_

??????yum?

以下命令针对的是依赖 DNF/YUM包管理器（例如 AlmaLinux/CentOS/Fedora/Rocky）

```
curl -fsSL https://www.nat.ac.cn/shell/collect_system_centos.sh | sudo env INSTALL_DEPS=0
INSTALL_AIDE=0 bash -s
```

部分等保测评项（身份鉴别 a、访问控制 f）需安装相关依赖实现

```
# 正常安装pwquality等依赖
curl -fsSL https://www.nat.ac.cn/shell/collect_system_centos.sh | sudo env INSTALL_DEPS=1
INSTALL_AIDE=0 bash -s
# 额外追加安全标记
curl -fsSL https://www.nat.ac.cn/shell/collect_system_centos.sh | sudo env INSTALL_DEPS=1
INSTALL_AIDE=1 bash -s
```

以下为脚本完整内容:

```
#!/bin/bash

set -euo pipefail

if [[ "$(uname)" != "Linux" ]]; then
  echo "仅支持在 Linux 上运行"; exit 1
fi

heartbeat() { while true; do echo "[heartbeat] $(date '+%F %T') 正在巡检..."; sleep 5; done; }
heartbeat & HEARTBEAT_PID=$!
cleanup() { kill "$HEARTBEAT_PID" 2>/dev/null || true; }
trap cleanup EXIT

SYSTEM_IP=$(ip addr show | grep -w inet | grep -v 127.0.0.1 | awk '{print $2}' | cut -d/ -f1 |
head -n1)
[ -z "$SYSTEM_IP" ] && SYSTEM_IP="unknown"
TIMESTAMP=$(date +%Y%m%d%H%M%S)
OUTPUT_FILE="$HOME/${SYSTEM_IP}_${TIMESTAMP}.txt"
```

```
touch "$OUTPUT_FILE"

run_command() {
  local cmd="$1" desc="$2"
  echo "$desc"
  {
    echo; echo "echo \"$desc\""; echo "echo \"Running: $cmd\""; echo "$cmd"
    eval "$cmd" 2>&1 || echo "命令缺失或执行失败"
    echo "----------------------------------------"
  } >> "$OUTPUT_FILE"
}

echo "开始采集..." > "$OUTPUT_FILE"
echo "输出文件: $OUTPUT_FILE" >> "$OUTPUT_FILE"
echo "采集时间: $(date)" >> "$OUTPUT_FILE"
echo "----------------------------------------" >> "$OUTPUT_FILE"

# 可选安装开关（默认不安装）
INSTALL_DEPS="${INSTALL_DEPS:-0}"   # sudo/util-linux/audit/pwquality/google-authenticator
INSTALL_SELINUX="${INSTALL_SELINUX:-0}"   # 单独控制 SELinux 相关工具

# 检测包管理器（CentOS 8+ 使用 dnf，CentOS 7 使用 yum）
if command -v dnf >/dev/null 2>&1; then
  PKG_MGR="dnf"
elif command -v yum >/dev/null 2>&1; then
  PKG_MGR="yum"
else
  PKG_MGR="yum"
fi

if [[ "$INSTALL_DEPS" == "1" || "$INSTALL_SELINUX" == "1" ]]; then
  run_command "$PKG_MGR makecache || true" "更新软件源缓存（失败忽略）"
fi
if [[ "$INSTALL_DEPS" == "1" ]]; then
  run_command "$PKG_MGR install -y sudo util-linux audit libpwquality google-authenticator ||
true" "可选安装巡检相关包（失败忽略）"
fi
if [[ "$INSTALL_SELINUX" == "1" ]]; then
  run_command "$PKG_MGR install -y policycoreutils policycoreutils-python-utils selinux-policy
selinux-policy-targeted || true" "可选安装 SELinux 工具（失败忽略）"
```

```
fi

if command -v sudo >/dev/null 2>&1; then SUDO="sudo"; else SUDO=""; fi

############ 基础信息 ############
run_command "hostnamectl" "主机名与操作系统信息"
run_command "timedatectl" "时间/时区同步状态"
run_command "ip addr show" "IP 配置"
run_command "uname -a" "内核与架构"
run_command "cat /etc/redhat-release 2>/dev/null || cat /etc/os-release" "发行版信息"

############ 账号与鉴别 ############
run_command "cat /etc/passwd" "本地账户"
run_command "cat /etc/group" "本地用户组"
run_command "${SUDO} cat /etc/shadow" "口令哈希（需 root）"
run_command "${SUDO} cat /etc/sudoers | grep -v ^# && ${SUDO} ls -l /etc/sudoers.d" "sudo 配置"
run_command "w" "当前登录会话"
run_command "who" "在线用户"
run_command "last | head" "近期登录记录（缺命令请安装 util-linux 或补 /var/log/wtmp）"
run_command "lastlog | head" "账户最近登录"
run_command "${SUDO} grep -v ^# /etc/login.defs" "登录/口令周期策略"
run_command "chage -l \$(whoami)" "当前用户口令有效期"

############ 口令复杂度/PAM ############
run_command "${SUDO} grep -v ^# /etc/pam.d/system-auth" "PAM 系统认证策略"
run_command "${SUDO} grep -v ^# /etc/pam.d/password-auth" "PAM 口令认证策略"
run_command "${SUDO} grep pam_pwquality /etc/pam.d/system-auth /etc/pam.d/password-auth" "是否启用
pwquality"
run_command "${SUDO} grep -v '^#' /etc/security/pwquality.conf" "pwquality 主配置"
run_command "${SUDO} grep -v '^#' /etc/security/pwquality.conf.d/*.conf 2>/dev/null"
"pwquality 追加配置"
run_command "rpm -qa | grep libpwquality || yum list installed 2>/dev/null | grep
libpwquality" "pwquality 模块是否安装"
run_command "${SUDO} grep -H 'pam_google_authenticator.so' /etc/pam.d/sshd /etc/pam.d/system-
auth /etc/pam.d/password-auth 2>/dev/null" "PAM 是否启用 Google Authenticator（二次认证）"

############ SSH 访问控制 ############
run_command "${SUDO} grep -E
'^(Protocol|PermitRootLogin|PasswordAuthentication|PermitEmptyPasswords|ChallengeResponseAuthe
ntication|AuthenticationMethods|ClientAliveInterval|ClientAliveCountMax)'
```

```
/etc/ssh/sshd_config" "SSH 核心配置"
run_command "cat \$HOME/.ssh/authorized_keys" "当前用户公钥授权"

############ 会话与最小权限 ############
run_command "${SUDO} grep -v ^# /etc/pam.d/su" "su 限制"
run_command "${SUDO} grep -v ^# /etc/pam.d/sudo" "sudo PAM 限制"
run_command "echo \${TMOUT:-unset}; ${SUDO} grep TMOUT /etc/profile /etc/bashrc 2>/dev/null" "
会话超时（bash）"

############ 审计与日志 ############
run_command "ps -eo user,pid,cmd | grep auditd" "审计进程"
run_command "${SUDO} systemctl status auditd" "审计服务状态"
run_command "${SUDO} auditctl -l" "审计规则加载情况"
run_command "${SUDO} cat /etc/audit/audit.rules 2>/dev/null" "审计规则文件"
run_command "${SUDO} grep -v ^# /etc/audit/rules.d/*.rules 2>/dev/null" "审计规则片段"
run_command "ls -ltr /var/log | tail" "日志目录概览"
run_command "${SUDO} head -n 20 /var/log/messages" "系统日志片段"
run_command "${SUDO} head -n 20 /var/log/secure" "认证日志片段"
run_command "${SUDO} grep -v ^# /etc/logrotate.conf" "日志轮转主配置"
run_command "ls -l /etc/logrotate.d" "日志轮转子配置"

############ 网络与边界 ############
run_command "ss -lntp" "监听 TCP 端口及进程"
run_command "ip route" "路由表"
run_command "ip neigh" "ARP 表"
run_command "${SUDO} firewall-cmd --list-all 2>/dev/null || echo 'firewalld 未安装或未启用'"
"firewalld 防火墙配置"
run_command "${SUDO} systemctl status firewalld" "firewalld 服务状态"
run_command "${SUDO} iptables -L -n -v" "iptables 规则列表"

############ 服务与自启 ############
run_command "systemctl list-unit-files --type=service --state=enabled" "开机自启服务"
run_command "systemctl show rsyslog.service -p User,Group,UID,GID" "rsyslog 运行身份"
run_command "systemctl show auditd.service -p User,Group,UID,GID" "auditd 运行身份"
run_command "ps -eo user,pid,cmd --sort=pid | head -n 30" "进程基线前 30 条"

############ SELinux 安全增强（可选） ############
if command -v getenforce >/dev/null 2>&1 && [[ "$(getenforce 2>/dev/null)" != "Disabled" ]];
then
  run_command "getenforce" "SELinux 当前状态"
```

```
  run_command "${SUDO} sestatus" "SELinux 详细状态"
  run_command "${SUDO} cat /etc/selinux/config" "SELinux 配置文件"
  run_command "${SUDO} semodule -l | head -n 20" "SELinux 已加载模块（前20）"
  run_command "${SUDO} getsebool -a | head -n 30" "SELinux 布尔值配置（前30）"
  run_command "${SUDO} ls -Z /etc/passwd /etc/shadow /etc/group 2>/dev/null" "关键文件 SELinux 上下文
"
  run_command "${SUDO} ps -eZ | head -n 20" "进程 SELinux 上下文（前20）"
  run_command "${SUDO} ausearch -m avc -ts recent 2>/dev/null | head -n 20 || echo 'audit 日志无
AVC 拒绝记录或 ausearch 未安装'" "SELinux 最近拒绝记录"
else
  echo "SELinux 未安装或已禁用，跳过 SELinux 检查" | tee -a "$OUTPUT_FILE"
fi

############ 加固与内核参数（选查） ############
run_command "${SUDO} sysctl -a | grep -E
'net.ipv4.conf.all.(accept_source_route|accept_redirects|send_redirects|rp_filter|log_martians
|forwarding)'" "关键内核网络安全参数"
run_command "mount | grep -E 'noexec|nodev|nosuid'" "挂载安全选项"

echo "采集完成，结果已保存到 $OUTPUT_FILE"
```

??????APT?

以下命令针对的是依赖 apt包管理器（例如 Debian/Ubuntu）

```
sudo env INSTALL_DEPS=0 INSTALL_AIDE=0 bash -s -- < <(curl -fsSL
https://www.nat.ac.cn/shell/collect_system_ubuntu.sh)
```

部分等保测评项（身份鉴别 a、访问控制 f）需安装相关依赖实现

```
# 正常安装pwquality等依赖
sudo env INSTALL_DEPS=1 INSTALL_AIDE=0 bash -s -- < <(curl -fsSL
https://www.nat.ac.cn/shell/collect_system_ubuntu.sh)
# 额外追加安全标记
sudo env INSTALL_DEPS=1 INSTALL_AIDE=0 bash -s -- < <(curl -fsSL
https://www.nat.ac.cn/shell/collect_system_ubuntu.sh)
```

以下为脚本完整内容：

```
#!/bin/bash

set -euo pipefail

if [[ "$(uname)" != "Linux" ]]; then
  echo "仅支持在 Linux 上运行"; exit 1
fi

heartbeat() { while true; do echo "[heartbeat] $(date '+%F %T') 正在巡检..."; sleep 5; done; }
heartbeat & HEARTBEAT_PID=$!
cleanup() { kill "$HEARTBEAT_PID" 2>/dev/null || true; }
trap cleanup EXIT

SYSTEM_IP=$(ip addr show | grep -w inet | grep -v 127.0.0.1 | awk '{print $2}' | cut -d/ -f1 |
head -n1)
[ -z "$SYSTEM_IP" ] && SYSTEM_IP="unknown"
TIMESTAMP=$(date +%Y%m%d%H%M%S)
OUTPUT_FILE="$HOME/${SYSTEM_IP}_${TIMESTAMP}.txt"
touch "$OUTPUT_FILE"
```

```
run_command() {
  local cmd="$1" desc="$2"
  echo "$desc"
  {
    echo; echo "echo \"$desc\""; echo "echo \"Running: $cmd\""; echo "$cmd"
    eval "$cmd" 2>&1 || echo "命令缺失或执行失败"
    echo "----------------------------------------"
  } >> "$OUTPUT_FILE"
}

echo "开始采集..." > "$OUTPUT_FILE"
echo "输出文件: $OUTPUT_FILE" >> "$OUTPUT_FILE"
echo "采集时间: $(date)" >> "$OUTPUT_FILE"
echo "----------------------------------------" >> "$OUTPUT_FILE"

# 可选安装开关（默认不安装）
INSTALL_DEPS="${INSTALL_DEPS:-0}"   # sudo/util-linux/auditd/pwquality/google-authenticator
INSTALL_AIDE="${INSTALL_AIDE:-0}"   # 单独控制 AIDE

if [[ "$INSTALL_DEPS" == "1" || "$INSTALL_AIDE" == "1" ]]; then
  run_command "apt-get update || true" "更新软件源（失败忽略）"
fi
if [[ "$INSTALL_DEPS" == "1" ]]; then
  run_command "apt-get install -y sudo util-linux auditd libpam-pwquality libpam-google-
authenticator || true" "可选安装巡检相关包（失败忽略）"
fi
if [[ "$INSTALL_AIDE" == "1" ]]; then
  run_command "apt-get install -y aide || true" "可选安装 AIDE（失败忽略）"
fi

if command -v sudo >/dev/null 2>&1; then SUDO="sudo"; else SUDO=""; fi

############ 基础信息 ############
run_command "hostnamectl" "主机名与操作系统信息"
run_command "timedatectl" "时间/时区同步状态"
run_command "ip addr show" "IP 配置"
run_command "uname -a" "内核与架构"
run_command "lsb_release -a 2>/dev/null || cat /etc/os-release" "发行版信息"
```

```
############ 账号与鉴别 ############
run_command "cat /etc/passwd" "本地账户"
run_command "cat /etc/group" "本地用户组"
run_command "${SUDO} cat /etc/shadow" "口令哈希（需 root）"
run_command "${SUDO} cat /etc/sudoers | grep -v ^# && ${SUDO} ls -l /etc/sudoers.d" "sudo 配置"
run_command "w" "当前登录会话"
run_command "who" "在线用户"
run_command "last | head" "近期登录记录（缺命令请安装 util-linux 或补 /var/log/wtmp）"
run_command "lastlog | head" "账户最近登录"
run_command "${SUDO} grep -v ^# /etc/login.defs" "登录/口令周期策略"
run_command "chage -l \$(whoami)" "当前用户口令有效期"

############ 口令复杂度/PAM ############
run_command "${SUDO} grep -v ^# /etc/pam.d/common-password" "PAM 口令策略"
run_command "${SUDO} grep pam_pwquality /etc/pam.d/common-password" "是否启用 pwquality"
run_command "${SUDO} grep -v '^#' /etc/security/pwquality.conf" "pwquality 主配置"
run_command "${SUDO} grep -v '^#' /etc/security/pwquality.conf.d/*.conf 2>/dev/null"
"pwquality 追加配置"
run_command "dpkg -l | grep libpwquality || apt list --installed 2>/dev/null | grep
libpwquality" "pwquality 模块是否安装"
run_command "${SUDO} grep -H 'pam_google_authenticator.so' /etc/pam.d/sshd /etc/pam.d/common-
auth /etc/pam.d/common-account 2>/dev/null" "PAM 是否启用 Google Authenticator（二次认证）"

############ SSH 访问控制 ############
run_command "${SUDO} grep -E
'^(Protocol|PermitRootLogin|PasswordAuthentication|PermitEmptyPasswords|ChallengeResponseAuthe
ntication|AuthenticationMethods|ClientAliveInterval|ClientAliveCountMax)'
/etc/ssh/sshd_config" "SSH 核心配置"
run_command "cat \$HOME/.ssh/authorized_keys" "当前用户公钥授权"

############ 会话与最小权限 ############
run_command "${SUDO} grep -v ^# /etc/pam.d/su" "su 限制"
run_command "${SUDO} grep -v ^# /etc/pam.d/sudo" "sudo PAM 限制"
run_command "echo \${TMOUT:-unset}; ${SUDO} grep TMOUT /etc/profile /etc/bash.bashrc
2>/dev/null" "会话超时（bash）"

############ 审计与日志 ############
run_command "ps -eo user,pid,cmd | grep auditd" "审计进程"
run_command "${SUDO} systemctl status auditd" "审计服务状态"
run_command "${SUDO} auditctl -l" "审计规则加载情况"
```

```
run_command "${SUDO} cat /etc/audit/audit.rules 2>/dev/null" "审计规则文件"
run_command "${SUDO} grep -v ^# /etc/audit/rules.d/*.rules 2>/dev/null" "审计规则片段"
run_command "ls -ltr /var/log | tail" "日志目录概览"
run_command "${SUDO} head -n 20 /var/log/syslog" "系统日志片段"
run_command "${SUDO} head -n 20 /var/log/auth.log" "认证日志片段"
run_command "${SUDO} grep -v ^# /etc/logrotate.conf" "日志轮转主配置"
run_command "ls -l /etc/logrotate.d" "日志轮转子配置"

############ 网络与边界 ############
run_command "ss -lntp" "监听 TCP 端口及进程"
run_command "ip route" "路由表"
run_command "ip neigh" "ARP 表"
run_command "${SUDO} ufw status verbose" "UFW 防火墙状态"
run_command "command -v firewall-cmd >/dev/null 2>&1 && ${SUDO} firewall-cmd --list-all ||
echo 'firewalld 未安装或未启用'" "若有 firewalld 则显示配置"

############ 服务与自启 ############
run_command "systemctl list-unit-files --type=service --state=enabled" "开机自启服务"
run_command "systemctl show rsyslog.service -p User,Group,UID,GID" "rsyslog 运行身份"
run_command "systemctl show auditd.service -p User,Group,UID,GID" "auditd 运行身份"
run_command "ps -eo user,pid,cmd --sort=pid | head -n 30" "进程基线前 30 条"

############ 加固与内核参数（选查） ############
run_command "dpkg -l | grep aide" "AIDE 是否已安装"
run_command "${SUDO} sysctl -a | grep -E
'net.ipv4.conf.all.(accept_source_route|accept_redirects|send_redirects|rp_filter|log_martians
|forwarding)'" "关键内核网络安全参数"
run_command "mount | grep -E 'noexec|nodev|nosuid'" "挂载安全选项"

echo "采集完成，结果已保存到 $OUTPUT_FILE"
```