```bash
#!/bin/bash
# AutoRecon - Linux System Audit Tool

# Colors
RED="\e[31m"
GREEN="\e[32m"
YELLOW="\e[33m"
NC="\e[0m"

# Create log directory
LOG_DIR="logs"
mkdir -p "$LOG_DIR"
LOG_FILE="$LOG_DIR/report_$(date +%F_%T).txt"

# Logging Function
log() {
  echo -e "$1" | tee -a "$LOG_FILE"
}

# System Info
system_info() {
  log "${YELLOW}--- SYSTEM INFORMATION ---${NC}"
  log "Hostname: $(hostname)"
  log "OS: $(lsb_release -d | cut -f2)"
  log "Kernel: $(uname -r)"
  log "Uptime: $(uptime -p)"
  log "CPU: $(lscpu | grep 'Model name' | cut -d ':' -f2)"
  log "Memory: $(free -h | grep Mem | awk '{print $2}')"
}

# User Audit
user_audit() {
  log "${YELLOW}--- USER AUDIT ---${NC}"
  log "Logged in users:"
  who
  log "\nAll system users:"
  cut -d: -f1 /etc/passwd
}

# Network Check
network_check() {
  log "${YELLOW}--- NETWORK INFORMATION ---${NC}"
  ip a | tee -a "$LOG_FILE"
  log "\nOpen Ports:"
  ss -tuln | tee -a "$LOG_FILE"
}

# Firewall Audit
firewall_audit() {
  log "${YELLOW}--- FIREWALL STATUS ---${NC}"
  if command -v ufw &>/dev/null; then
    ufw status verbose | tee -a "$LOG_FILE"
  else
```

```
    log "UFW not installed."
  fi
}

# Vulnerability Check (basic)
vuln_check() {
  log "${YELLOW}--- VULNERABILITY CHECK ---${NC}"
  log "Outdated Packages:"
  if command -v apt &>/dev/null; then
    apt list --upgradable | tee -a "$LOG_FILE"
  else
    log "APT not found. Skipping."
  fi
}

# Main
main() {
  log "${GREEN}Starting AutoRecon Audit...${NC}"
  system_info
  user_audit
  network_check
  firewall_audit
  vuln_check
  log "${GREEN}Audit completed. Report saved to $LOG_FILE${NC}"
}

main
```