**Sri Lanka Institute of Information Technology**

****

**IE3092 – Information Security Project**

**Security Auditing Tool for Red Hat Enterprise Linux 7**

Submitted by,

IT20036652- Wijesinghe W.A.S.D

IT20034672 - Dissanayake D.M.I.H

**Video Link**

**Introduction**

**What is Red Hat**

Red Hat Enterprise Linux (RHEL) is a commercial open-source Linux distribution developed by Red Hat for the commercial market. Red Hat Enterprise Linux is released in server versions for x86-64, Power ISA, ARM64, and IBM Z, and a desktop version for x86-64. Fedora Linux serves as its upstream source. All of Red Hat's official support and training, together with the Red Hat Certification Program, focuses on the Red Hat Enterprise Linux platform.

The first version of Red Hat Enterprise Linux to bear the name originally came onto the market as "Red Hat Linux Advanced Server". In 2003, Red Hat rebranded Red Hat Linux Advanced Server to "Red Hat Enterprise Linux AS" and added two more variants, Red Hat Enterprise Linux ES and Red Hat Enterprise Linux WS.

Red Hat uses strict trademark rules to restrict free re-distribution of their officially supported versions of Red Hat Enterprise Linux but still freely provides its source code. Third-party derivatives can be built and redistributed by stripping away non-free components like Red Hat's trademarks. Examples include community-supported distributions like Rocky Linux and Alma Linux and commercial forks like Oracle Linux.

Red Hat Enterprise Linux is the world’s leading enterprise Linux platform, certified on hundreds of clouds and with thousands of hardware and software vendors. Red Hat Enterprise Linux can be purchased to support specific use cases like [edge computing](https://www.redhat.com/en/topics/edge-computing/what-is-edge-computing) or [SAP workloads](https://www.redhat.com/en/topics/linux/sap-hana-and-linux?percmp=7013a000002pwRCAAY), but every subscription includes these core benefits:

Automation and Management

Install and migration tool

Security and compliance

Consistent performance

**Overview For Security Auditing Tool for Red Hat Enterprise Linux 7**

This document provides prescriptive guidance for establishing a secure configuration posture for Red Hat Enterprise Linux 7 systems running on x86 and x64 platforms. This document was tested against Red Hat Enterprise Linux 7.2. The guidance within broadly assumes that operations are being performed as the root user. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify the root user's path integrity and the integrity of any programs being run prior to the execution of commands and scripts included in this benchmark.

**Literature**

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Linux on an x86 platform.

This product was created using a consensus review process comprised of subject matter experts and make easy the process.

By developing this product, we are expected to reduce the time that will take to audit the security of RedHat linux 7 one by one.

This tool will run all the security auditing scripts once and generate two file which, one is results and second one is for security issues.

Graphical user interface, text, application

Description automatically generated

**Research Based Product Functionalities**

By running this product, we can have a proper idea of the RedHat system including following topics.

1. Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection against resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

1. Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited

1. Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

1. Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

1. Access, Authentication and Authorization

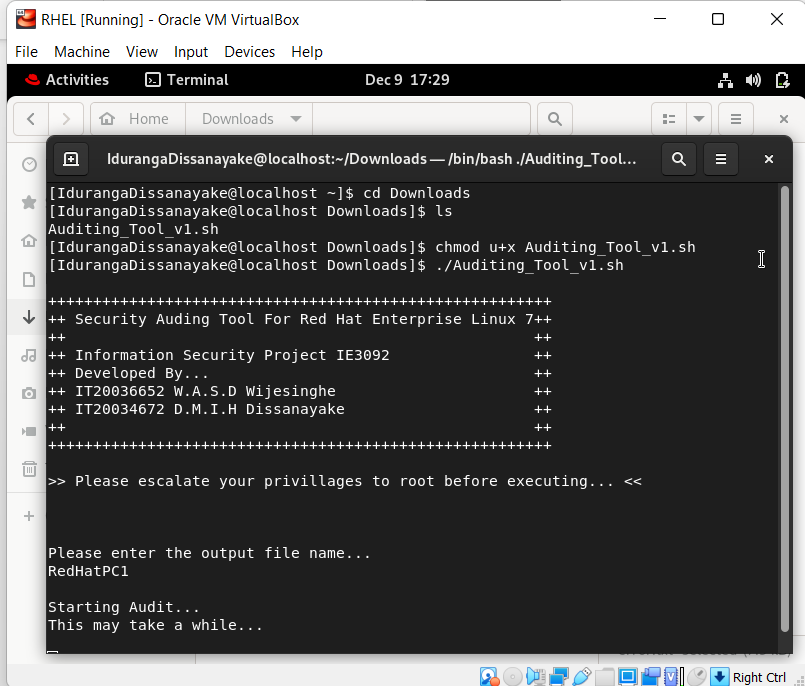
This part will audit the AAA status on RedHat Linux system.

1. System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.



**Technology and architecture**

****

***Script***

#!/bin/bash

echo ""

echo "++++++++++++++++++++++++++++++++++++++++++++++++++++++++"

echo "++ Security Auding Tool For Red Hat Enterprise Linux 7++"

echo "++                                                    ++"

echo "++ Information Security Project IE3092                ++"

echo "++ Developed By...                                    ++"

echo "++ IT20036652 W.A.S.D Wijesinghe                      ++"

echo "++ IT20034672 D.M.I.H Dissanayake                     ++"

echo "++                                                    ++"

echo "++++++++++++++++++++++++++++++++++++++++++++++++++++++++"

echo ""

echo ">> Please escalate your privileges to root before executing... <<"

echo ""

echo ""

#-----Begin Audit------------------

echo ""

echo "Please enter the output file name..."

read outF

echo Starting The Audit... > $outF.txt

echo AuditErrors... > error.txt

echo ""

echo "Starting Audit..."

echo "This may take a while..."

echo ""

now="$(date)"

echo "Current date and time ->" "$now" >> $outF.txt

#--IP and Hostname--#

echo "IP" >> $outF.txt

echo "IP" >> error.txt

ifconfig >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

echo "Host Name" >> $outF.txt

echo "Host Name" >> error.txt

hostname >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

echo "" >> $outF.txt

#--1.1.1.1

echo "s\_1.1.1.1" >> $outF.txt

echo "s\_1.1.1.1" >> error.txt

modprobe -n -v cramfs >> $outF.txt  2>> error.txt

lsmod | grep cramfs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.2

echo "s\_1.1.1.2" >> $outF.txt

echo "s\_1.1.1.2" >> error.txt

modprobe -n -v freevxfs >> $outF.txt  2>> error.txt

lsmod | grep freevxfs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.3

echo "s\_1.1.1.3" >> $outF.txt

echo "s\_1.1.1.3" >> error.txt

modprobe -n -v jffs2 >> $outF.txt  2>> error.txt

lsmod | grep jffs2 >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.4

echo "s\_1.1.1.4" >> $outF.txt

echo "s\_1.1.1.4" >> error.txt

modprobe -n -v hfs >> $outF.txt  2>> error.txt

lsmod | grep hfs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.5

echo "s\_1.1.1.5" >> $outF.txt

echo "s\_1.1.1.5" >> error.txt

modprobe -n -v hfsplus >> $outF.txt  2>> error.txt

lsmod | grep hfsplus >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.6

echo "s\_1.1.1.6" >> $outF.txt

echo "s\_1.1.1.6" >> error.txt

modprobe -n -v squashfs >> $outF.txt  2>> error.txt

lsmod | grep squashfs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.7

echo "s\_1.1.1.7" >> $outF.txt

echo "s\_1.1.1.7" >> error.txt

modprobe -n -v udf >> $outF.txt  2>> error.txt

lsmod | grep udf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.1.8

echo "s\_1.1.1.8" >> $outF.txt

echo "s\_1.1.1.8" >> error.txt

modprobe -n -v vfat >> $outF.txt  2>> error.txt

lsmod | grep vfat >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.2

echo "s\_1.1.2" >> $outF.txt

echo "s\_1.1.2" >> error.txt

mount | grep /tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.3

echo "s\_1.1.3" >> $outF.txt

echo "s\_1.1.3" >> error.txt

mount | grep /tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.4

echo "s\_1.1.4" >> $outF.txt

echo "s\_1.1.4" >> error.txt

mount | grep /tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.5

echo "s\_1.1.5" >> $outF.txt

echo "s\_1.1.5" >> error.txt

mount | grep /tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.6

echo "s\_1.1.6" >> $outF.txt

echo "s\_1.1.6" >> error.txt

mount | grep /var >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.7

echo "s\_1.1.7" >> $outF.txt

echo "s\_1.1.7" >> error.txt

mount | grep /var/tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.8

echo "s\_1.1.8" >> $outF.txt

echo "s\_1.1.8" >> error.txt

mount | grep /var/tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.9

echo "s\_1.1.9" >> $outF.txt

echo "s\_1.1.9" >> error.txt

mount | grep /var/tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.10

echo "s\_1.1.10" >> $outF.txt

echo "s\_1.1.10" >> error.txt

mount | grep /var/tmp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.11

echo "s\_1.1.11" >> $outF.txt

echo "s\_1.1.11" >> error.txt

mount | grep /var/log >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.12

echo "s\_1.1.12" >> $outF.txt

echo "s\_1.1.12" >> error.txt

mount | grep /var/log/audit >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.13

echo "s\_1.1.13" >> $outF.txt

echo "s\_1.1.13" >> error.txt

mount | grep /home >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.14

echo "s\_1.1.14" >> $outF.txt

echo "s\_1.1.14" >> error.txt

mount | grep /home >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.15

echo "s\_1.1.15" >> $outF.txt

echo "s\_1.1.15" >> error.txt

mount | grep /dev/shm >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.16

echo "s\_1.1.16" >> $outF.txt

echo "s\_1.1.16" >> error.txt

mount | grep /dev/shm >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.17

echo "s\_1.1.17" >> $outF.txt

echo "s\_1.1.17" >> error.txt

mount | grep /dev/shm >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.21

echo "s\_1.1.21" >> $outF.txt

echo "s\_1.1.21" >> error.txt

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.22

echo "s\_1.1.22" >> $outF.txt

echo "s\_1.1.22" >> error.txt

systemctl is-enabled autofs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.1.23

echo "s\_1.1.23" >> $outF.txt

echo "s\_1.1.23" >> error.txt

systemctl is-enabled autofs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.2.1

echo "s\_1.2.1" >> $outF.txt

echo "s\_1.2.1" >> error.txt

yum repolist >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.2.2

echo "s\_1.2.2" >> $outF.txt

echo "s\_1.2.2" >> error.txt

grep ^gpgcheck /etc/yum.conf >> $outF.txt  2>> error.txt

grep ^gpgcheck /etc/yum.repos.d/\* >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.2.3

echo "s\_1.2.3" >> $outF.txt

echo "s\_1.2.3" >> error.txt

rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n' >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.2.4

echo "s\_1.2.4" >> $outF.txt

echo "s\_1.2.4" >> error.txt

subscription-manager identity >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.2.5

echo "s\_1.2.5" >> $outF.txt

echo "s\_1.2.5" >> error.txt

subscription-manager identity >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.3.1

echo "s\_1.3.1" >> $outF.txt

echo "s\_1.3.1" >> error.txt

rpm -q aide >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.3.2

echo "s\_1.3.2" >> $outF.txt

echo "s\_1.3.2" >> error.txt

crontab -u root -l | grep aide >> $outF.txt  2>> error.txt

grep -r aide /etc/cron.\* /etc/crontab >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.4.1

echo "s\_1.4.1" >> $outF.txt

echo "s\_1.4.1" >> error.txt

stat /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.4.2

echo "s\_1.4.2" >> $outF.txt

echo "s\_1.4.2" >> error.txt

grep "^set superusers" /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

grep "^password" /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.4.3

echo "s\_1.4.3" >> $outF.txt

echo "s\_1.4.3" >> error.txt

grep /sbin/sulogin /usr/lib/systemd/system/rescue.service >> $outF.txt  2>> error.txt

grep /sbin/sulogin /usr/lib/systemd/system/emergency.service >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.4.1

echo "s\_1.4.1" >> $outF.txt

echo "s\_1.4.1" >> error.txt

grep selinux=0 /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

grep enforcing=0 /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.5.1

echo "s\_1.5.1" >> $outF.txt

echo "s\_1.5.1" >> error.txt

grep "hard core" /etc/security/limits.conf /etc/security/limits.d/\* >> $outF.txt  2>> error.txt

grep sysctl fs.suid\_dumpable >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.5.3

echo "s\_1.5.3" >> $outF.txt

echo "s\_1.5.3" >> error.txt

sysctl kernel.randomize\_va\_space >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.5.4

echo "s\_1.5.4" >> $outF.txt

echo "s\_1.5.4" >> error.txt

rpm -q prelink >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.1

echo "s\_1.6.1.1" >> $outF.txt

echo "s\_1.6.1.1" >> error.txt

grep "^\s\*linux" /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.2

echo "s\_1.6.1.2" >> $outF.txt

echo "s\_1.6.1.2" >> error.txt

grep SELINUX=enforcing /etc/selinux/config >> $outF.txt  2>> error.txt

sestatus >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.3

echo "s\_1.6.1.3" >> $outF.txt

echo "s\_1.6.1.3" >> error.txt

grep SELINUXTYPE=targeted /etc/selinux/config >> $outF.txt  2>> error.txt

sestatus >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.4

echo "s\_1.6.1.4" >> $outF.txt

echo "s\_1.6.1.4" >> error.txt

rpm -q setroubleshoot >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.5

echo "s\_1.6.1.5" >> $outF.txt

echo "s\_1.6.1.5" >> error.txt

rpm -q mcstrans >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.1.6

echo "s\_1.6.1.6" >> $outF.txt

echo "s\_1.6.1.6" >> error.txt

ps -eZ | egrep "initrc" | egrep -vw "tr|ps|egrep|bash|awk" | tr ':' ' ' | awk '{ print $NF }' >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.6.2

echo "s\_1.6.2" >> $outF.txt

echo "s\_1.6.2" >> error.txt

rpm -q libselinux >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.7.1.1

echo "s\_1.7.1.1" >> $outF.txt

echo "s\_1.7.1.1" >> error.txt

cat /etc/motd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.7.1.5

echo "s\_1.7.1.5" >> $outF.txt

echo "s\_1.7.1.5" >> error.txt

stat /etc/issue >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--1.7.2

echo "s\_1.7.2" >> $outF.txt

echo "s\_1.7.2" >> error.txt

rpm -q libselinux >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--- Inet Services ---

#--2.1.1

echo "s\_2.1.1" >> $outF.txt

echo "s\_2.1.1" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.2

echo "s\_2.1.2" >> $outF.txt

echo "s\_2.1.2" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.3

echo "s\_2.1.3" >> $outF.txt

echo "s\_2.1.3" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.4

echo "s\_2.1.4" >> $outF.txt

echo "s\_2.1.4" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.5

echo "s\_2.1.5" >> $outF.txt

echo "s\_2.1.5" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.6

echo "s\_2.1.6" >> $outF.txt

echo "s\_2.1.6" >> error.txt

chkconfig --list >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.7

echo "s\_2.1.7" >> $outF.txt

echo "s\_2.1.7" >> error.txt

systemctl is-enabled xinetd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.1.1

echo "s\_2.1.1.1" >> $outF.txt

echo "s\_2.1.1.1" >> error.txt

rpm -q ntp >> $outF.txt  2>> error.txt

rpm -q chrony >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.1.2

echo "s\_2.1.1.2" >> $outF.txt

echo "s\_2.1.1.2" >> error.txt

grep "^restrict" /etc/ntp.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.1.1.3

echo "s\_2.1.1.3" >> $outF.txt

echo "s\_2.1.1.3" >> error.txt

grep "^server" /etc/chrony.conf >> $outF.txt  2>> error.txt

grep ^OPTIONS /etc/sysconfig/chronyd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.2

echo "s\_2.2.2" >> $outF.txt

echo "s\_2.2.2" >> error.txt

rpm -qa xorg-x11\* >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.3

echo "s\_2.2.3" >> $outF.txt

echo "s\_2.2.3" >> error.txt

systemctl is-enabled avahi-daemon >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.4

echo "s\_2.2.4" >> $outF.txt

echo "s\_2.2.4" >> error.txt

systemctl is-enabled cups >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.5

echo "s\_2.2.5" >> $outF.txt

echo "s\_2.2.5" >> error.txt

systemctl is-enabled dhcpd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.6

echo "s\_2.2.6" >> $outF.txt

echo "s\_2.2.6" >> error.txt

systemctl is-enabled slapd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.7

echo "s\_2.2.7" >> $outF.txt

echo "s\_2.2.7" >> error.txt

systemctl is-enabled nfs >> $outF.txt  2>> error.txt

systemctl is-enabled nfs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.8

echo "s\_2.2.8" >> $outF.txt

echo "s\_2.2.8" >> error.txt

systemctl is-enabled named >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.9

echo "s\_2.2.9" >> $outF.txt

echo "s\_2.2.9" >> error.txt

systemctl is-enabled vsftpd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.10

echo "s\_2.2.10" >> $outF.txt

echo "s\_2.2.10" >> error.txt

systemctl is-enabled httpd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.11

echo "s\_2.2.11" >> $outF.txt

echo "s\_2.2.11" >> error.txt

systemctl is-enabled dovecot >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.12

echo "s\_2.2.12" >> $outF.txt

echo "s\_2.2.12" >> error.txt

systemctl is-enabled smb >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.13

echo "s\_2.2.13" >> $outF.txt

echo "s\_2.2.13" >> error.txt

systemctl is-enabled squid >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.14

echo "s\_2.2.14" >> $outF.txt

echo "s\_2.2.14" >> error.txt

systemctl is-enabled snmpd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.15

echo "s\_2.2.15" >> $outF.txt

echo "s\_2.2.15" >> error.txt

netstat -an | grep LIST | grep ":25[[:space:]]" >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.16

echo "s\_2.2.16" >> $outF.txt

echo "s\_2.2.16" >> error.txt

systemctl is-enabled ypserv >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.17

echo "s\_2.2.17" >> $outF.txt

echo "s\_2.2.17" >> error.txt

systemctl is-enabled rsh.socket >> $outF.txt  2>> error.txt

systemctl is-enabled rlogin.socket >> $outF.txt  2>> error.txt

systemctl is-enabled rexec.socket >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.18

echo "s\_2.2.18" >> $outF.txt

echo "s\_2.2.18" >> error.txt

systemctl is-enabled ntalk >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.19

echo "s\_2.2.19" >> $outF.txt

echo "s\_2.2.19" >> error.txt

systemctl is-enabled telnet.socket >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.20

echo "s\_2.2.20" >> $outF.txt

echo "s\_2.2.20" >> error.txt

systemctl is-enabled tftp.socket >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.2.21

echo "s\_2.2.21" >> $outF.txt

echo "s\_2.2.21" >> error.txt

systemctl is-enabled rsyncd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.3.1

echo "s\_2.3.1" >> $outF.txt

echo "s\_2.3.1" >> error.txt

rpm -q ypbind >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.3.2

echo "s\_2.3.2" >> $outF.txt

echo "s\_2.3.2" >> error.txt

rpm -q rsh >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.3.3

echo "s\_2.3.3" >> $outF.txt

echo "s\_2.3.3" >> error.txt

rpm -q talk >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.3.4

echo "s\_2.3.4" >> $outF.txt

echo "s\_2.3.4" >> error.txt

rpm -q telnet >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--2.3.5

echo "s\_2.3.5" >> $outF.txt

echo "s\_2.3.5" >> error.txt

rpm -q openldap-clients >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3 Network Configuration

#--3.1.1

echo "s\_3.1.1" >> $outF.txt

echo "s\_3.1.1" >> error.txt

sysctl net.ipv4.ip\_forward >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.1.2

echo "s\_3.1.2" >> $outF.txt

echo "s\_3.1.2" >> error.txt

sysctl net.ipv4.conf.all.send\_redirects >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.send\_redirects >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.1

echo "s\_3.2.1" >> $outF.txt

echo "s\_3.2.1" >> error.txt

sysctl net.ipv4.conf.all.accept\_source\_route >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.accept\_source\_route >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.2

echo "s\_3.2.2" >> $outF.txt

echo "s\_3.2.2" >> error.txt

sysctl net.ipv4.conf.all.accept\_redirects >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.accept\_redirects >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.3

echo "s\_3.2.3" >> $outF.txt

echo "s\_3.2.3" >> error.txt

sysctl net.ipv4.conf.all.secure\_redirects >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.secure\_redirects >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.4

echo "s\_3.2.4" >> $outF.txt

echo "s\_3.2.4" >> error.txt

sysctl net.ipv4.conf.all.log\_martians >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.log\_martians >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.5

echo "s\_3.2.5" >> $outF.txt

echo "s\_3.2.5" >> error.txt

sysctl net.ipv4.icmp\_echo\_ignore\_broadcasts >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.6

echo "s\_3.2.6" >> $outF.txt

echo "s\_3.2.6" >> error.txt

sysctl net.ipv4.icmp\_ignore\_bogus\_error\_responses >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.7

echo "s\_3.2.7" >> $outF.txt

echo "s\_3.2.7" >> error.txt

sysctl net.ipv4.conf.all.rp\_filter >> $outF.txt  2>> error.txt

sysctl net.ipv4.conf.default.rp\_filter >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.2.8

echo "s\_3.2.8" >> $outF.txt

echo "s\_3.2.8" >> error.txt

sysctl net.ipv4.tcp\_syncookies >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.3.1

echo "s\_3.3.1" >> $outF.txt

echo "s\_3.3.1" >> error.txt

sysctl net.ipv6.conf.all.accept\_ra >> $outF.txt  2>> error.txt

sysctl net.ipv6.conf.default.accept\_ra >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.3.2

echo "s\_3.3.2" >> $outF.txt

echo "s\_3.3.2" >> error.txt

sysctl net.ipv6.conf.all.accept\_redirects >> $outF.txt  2>> error.txt

sysctl net.ipv6.conf.default.accept\_redirects >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.4.1

echo "s\_3.4.1" >> $outF.txt

echo "s\_3.4.1" >> error.txt

rpm -q tcp\_wrappers >> $outF.txt  2>> error.txt

rpm -q tcp\_wrappers-libs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.4.2

echo "s\_3.4.2" >> $outF.txt

echo "s\_3.4.2" >> error.txt

cat /etc/hosts.allow >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.4.3

echo "s\_3.4.3" >> $outF.txt

echo "s\_3.4.3" >> error.txt

cat /etc/hosts.deny >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.4.4

echo "s\_3.4.4" >> $outF.txt

echo "s\_3.4.4" >> error.txt

stat /etc/hosts.allow >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.4.5

echo "s\_3.4.5" >> $outF.txt

echo "s\_3.4.5" >> error.txt

stat /etc/hosts.deny >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.5.1

echo "s\_3.5.1" >> $outF.txt

echo "s\_3.5.1" >> error.txt

modprobe -n -v dccp >> $outF.txt  2>> error.txt

lsmod | grep dccp >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.6.1

echo "s\_3.6.1" >> $outF.txt

echo "s\_3.6.1" >> error.txt

rpm -q iptables >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.6.2

echo "s\_3.6.2" >> $outF.txt

echo "s\_3.6.2" >> error.txt

iptables -L >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.6.3

echo "s\_3.6.3" >> $outF.txt

echo "s\_3.6.3" >> error.txt

iptables -L INPUT -v -n >> $outF.txt  2>> error.txt

iptables -L OUTPUT -v -n >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.6.4

echo "s\_3.6.4" >> $outF.txt

echo "s\_3.6.4" >> error.txt

iptables -L -v -n >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--3.6.5

echo "s\_3.6.5" >> $outF.txt

echo "s\_3.6.5" >> error.txt

netatat -ln >> $outF.txt  2>> error.txt

iptables -L INPUT -v -n >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--Logging and Auditing--

#--4.1.1.1

echo "s\_4.1.1.1" >> $outF.txt

echo "s\_4.1.1.1" >> error.txt

grep max\_log\_file /etc/audit/auditd.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.1.2

echo "s\_4.1.1.2" >> $outF.txt

echo "s\_4.1.1.2" >> error.txt

grep space\_left\_action /etc/audit/auditd.conf >> $outF.txt  2>> error.txt

grep action\_mail\_acct /etc/audit/auditd.conf >> $outF.txt  2>> error.txt

grep admin\_space\_left\_action /etc/audit/auditd.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.1.3

echo "s\_4.1.1.3" >> $outF.txt

echo "s\_4.1.1.3" >> error.txt

grep max\_log\_file\_action /etc/audit/auditd.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.2

echo "s\_4.1.2" >> $outF.txt

echo "s\_4.1.2" >> error.txt

systemctl is-enabled auditd >> $outF.txt  2>> error.txt

#--4.1.3

echo "s\_4.1.3" >> $outF.txt

echo "s\_4.1.3" >> error.txt

grep "^\s\*linux" /boot/grub2/grub.cfg >> $outF.txt  2>> error.txt

#--4.1.4

echo "s\_4.1.4" >> $outF.txt

echo "s\_4.1.4" >> error.txt

grep time-change /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.5

echo "s\_4.1.5" >> $outF.txt

echo "s\_4.1.5" >> error.txt

grep identity /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.6

echo "s\_4.1.6" >> $outF.txt

echo "s\_4.1.6" >> error.txt

grep system-locale /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.7

echo "s\_4.1.7" >> $outF.txt

echo "s\_4.1.7" >> error.txt

grep MAC-policy /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.8

echo "s\_4.1.8" >> $outF.txt

echo "s\_4.1.8" >> error.txt

grep logins /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.9

echo "s\_4.1.9" >> $outF.txt

echo "s\_4.1.9" >> error.txt

grep session /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.10

echo "s\_4.1.10" >> $outF.txt

echo "s\_4.1.10" >> error.txt

grep perm\_mod /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.11

echo "s\_4.1.11" >> $outF.txt

echo "s\_4.1.11" >> error.txt

grep access /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.12

echo "s\_4.1.12" >> $outF.txt

echo "s\_4.1.12" >> error.txt

find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged" }' >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.13

echo "s\_4.1.13" >> $outF.txt

echo "s\_4.1.13" >> error.txt

grep mounts /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.14

echo "s\_4.1.14" >> $outF.txt

echo "s\_4.1.14" >> error.txt

grep delete /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.15

echo "s\_4.1.15" >> $outF.txt

echo "s\_4.1.15" >> error.txt

grep scope /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.16

echo "s\_4.1.16" >> $outF.txt

echo "s\_4.1.16" >> error.txt

grep actions /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.17

echo "s\_4.1.17" >> $outF.txt

echo "s\_4.1.17" >> error.txt

grep modules /etc/audit/audit.rules >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.1.18

echo "s\_4.1.18" >> $outF.txt

echo "s\_4.1.18" >> error.txt

grep "^\s\*[^#]" /etc/audit/audit.rules | tail -1 >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.1.1

echo "s\_4.2.1.1" >> $outF.txt

echo "s\_4.2.1.1" >> error.txt

systemctl is-enabled rsyslog >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.1.2

echo "s\_4.2.1.2" >> $outF.txt

echo "s\_4.2.1.2" >> error.txt

ls -l /var/log/ >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.1.3

echo "s\_4.2.1.3" >> $outF.txt

echo "s\_4.2.1.3" >> error.txt

grep ^\$FileCreateMode /etc/rsyslog.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.1.4

echo "s\_4.2.1.4" >> $outF.txt

echo "s\_4.2.1.4" >> error.txt

grep "^\*.\*[^I][^I]\*@" /etc/rsyslog.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.1.5

echo "s\_4.2.1.5" >> $outF.txt

echo "s\_4.2.1.5" >> error.txt

grep '$ModLoad imtcp.so' /etc/rsyslog.conf >> $outF.txt  2>> error.txt

grep '$InputTCPServerRun' /etc/rsyslog.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.2.1

echo "s\_4.2.2.1" >> $outF.txt

echo "s\_4.2.2.1" >> error.txt

systemctl is-enabled syslog-ng >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.2.2

echo "s\_4.2.2.2" >> $outF.txt

echo "s\_4.2.2.2" >> error.txt

ls -l /var/log/ >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.2.3

echo "s\_4.2.2.3" >> $outF.txt

echo "s\_4.2.2.3" >> error.txt

grep ^options /etc/syslog-ng/syslog-ng.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.3

echo "s\_4.2.3" >> $outF.txt

echo "s\_4.2.3" >> error.txt

rpm -q rsyslog >> $outF.txt  2>> error.txt

rpm -q syslog-ng >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--4.2.4

echo "s\_4.2.4" >> $outF.txt

echo "s\_4.2.4" >> error.txt

rpm -q rsyslog >> $outF.txt  2>> error.txt

find /var/log -type f -ls >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5 Access, Authentication and Authorization

#--5.1.1

echo "s\_5.1.1" >> $outF.txt

echo "s\_5.1.1" >> error.txt

systemctl is-enabled crond >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.2

echo "s\_5.1.2" >> $outF.txt

echo "s\_5.1.2" >> error.txt

stat /etc/crontab >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.3

echo "s\_5.1.3" >> $outF.txt

echo "s\_5.1.3" >> error.txt

stat /etc/cron.hourly >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.4

echo "s\_5.1.4" >> $outF.txt

echo "s\_5.1.4" >> error.txt

stat /etc/cron.daily >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.5

echo "s\_5.1.5" >> $outF.txt

echo "s\_5.1.5" >> error.txt

stat /etc/cron.weekly >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.6

echo "s\_5.1.6" >> $outF.txt

echo "s\_5.1.6" >> error.txt

stat /etc/cron.monthly >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.7

echo "s\_5.1.7" >> $outF.txt

echo "s\_5.1.7" >> error.txt

stat /etc/cron.d >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.1.8

echo "s\_5.1.7" >> $outF.txt

echo "s\_5.1.7" >> error.txt

stat /etc/cron.deny >> $outF.txt  2>> error.txt

stat /etc/at.deny >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.1

echo "s\_5.2.1" >> $outF.txt

echo "s\_5.2.1" >> error.txt

stat /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.2

echo "s\_5.2.2" >> $outF.txt

echo "s\_5.2.2" >> error.txt

grep "^Protocol" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.3

echo "s\_5.2.3" >> $outF.txt

echo "s\_5.2.3" >> error.txt

grep "^LogLevel" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.4

echo "s\_5.2.4" >> $outF.txt

echo "s\_5.2.4" >> error.txt

grep "^X11Forwarding" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.5

echo "s\_5.2.5" >> $outF.txt

echo "s\_5.2.5" >> error.txt

grep "^MaxAuthTries" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.6

echo "s\_5.2.6" >> $outF.txt

echo "s\_5.2.6" >> error.txt

grep "^IgnoreRhosts" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.7

echo "s\_5.2.7" >> $outF.txt

echo "s\_5.2.7" >> error.txt

grep "^HostbasedAuthentication" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.8

echo "s\_5.2.8" >> $outF.txt

echo "s\_5.2.8" >> error.txt

grep "^PermitRootLogin" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.9

echo "s\_5.2.9" >> $outF.txt

echo "s\_5.2.9" >> error.txt

grep "^PermitEmptyPasswords" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.10

echo "s\_5.2.10" >> $outF.txt

echo "s\_5.2.10" >> error.txt

grep PermitUserEnvironment /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.11

echo "s\_5.2.11" >> $outF.txt

echo "s\_5.2.11" >> error.txt

grep "Ciphers" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.12

echo "s\_5.2.12" >> $outF.txt

echo "s\_5.2.12" >> error.txt

grep "MACs" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.13

echo "s\_5.2.13" >> $outF.txt

echo "s\_5.2.13" >> error.txt

grep "^ClientAliveInterval" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

grep "^ClientAliveCountMax" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.14

echo "s\_5.2.14" >> $outF.txt

echo "s\_5.2.14" >> error.txt

grep "^LoginGraceTime" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.15

echo "s\_5.2.15" >> $outF.txt

echo "s\_5.2.15" >> error.txt

grep "^AllowUsers" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

grep "^AllowGroups" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

grep "^DenyUsers" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

grep "^DenyGroups" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.2.16

echo "s\_5.2.16" >> $outF.txt

echo "s\_5.2.16" >> error.txt

grep "^Banner" /etc/ssh/sshd\_config >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.3.1

echo "s\_5.3.1" >> $outF.txt

echo "s\_5.3.1" >> error.txt

grep pam\_pwquality.so /etc/pam.d/password-auth >> $outF.txt  2>> error.txt

grep pam\_pwquality.so /etc/pam.d/system-auth >> $outF.txt  2>> error.txt

grep ^minlen /etc/security/pwquality.conf >> $outF.txt  2>> error.txt

grep ^dcredit /etc/security/pwquality.conf >> $outF.txt  2>> error.txt

grep ^lcredit /etc/security/pwquality.conf >> $outF.txt  2>> error.txt

grep ^ocredit /etc/security/pwquality.conf >> $outF.txt  2>> error.txt

grep ^ucredit /etc/security/pwquality.conf >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.3.3

echo "s\_5.3.3" >> $outF.txt

echo "s\_5.3.3" >> error.txt

egrep '^password\s+sufficient\s+pam\_unix.so' /etc/pam.d/password-auth >> $outF.txt  2>> error.txt

egrep '^password\s+sufficient\s+pam\_unix.so' /etc/pam.d/system-auth >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.3.4

echo "s\_5.3.4" >> $outF.txt

echo "s\_5.3.4" >> error.txt

egrep '^password\s+sufficient\s+pam\_unix.so' /etc/pam.d/password-auth >> $outF.txt  2>> error.txt

egrep '^password\s+sufficient\s+pam\_unix.so' /etc/pam.d/system-auth >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.1.1

echo "s\_5.4.1.1" >> $outF.txt

echo "s\_5.4.1.1" >> error.txt

grep PASS\_MAX\_DAYS /etc/login.defs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.1.2

echo "s\_5.4.1.2" >> $outF.txt

echo "s\_5.4.1.2" >> error.txt

grep PASS\_MIN\_DAYS /etc/login.defs >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.1.4

echo "s\_5.4.1.4" >> $outF.txt

echo "s\_5.4.1.4" >> error.txt

useradd -D | grep INACTIVE >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.2

echo "s\_5.4.2" >> $outF.txt

echo "s\_5.4.2" >> error.txt

egrep -v "^\+" /etc/passwd | awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $3<1000 && $7!="/sbin/nologin" && $7!="/bin/false") {print}' >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.3

echo "s\_5.4.3" >> $outF.txt

echo "s\_5.4.3" >> error.txt

grep "^root:" /etc/passwd | cut -f4 -d: >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.4.4

echo "s\_5.4.4" >> $outF.txt

echo "s\_5.4.4" >> error.txt

grep "^umask" /etc/bashrc >> $outF.txt  2>> error.txt

grep "^umask" /etc/profile >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--5.6

echo "s\_5.6" >> $outF.txt

echo "s\_5.6" >> error.txt

grep pam\_wheel.so /etc/pam.d/su >> $outF.txt  2>> error.txt

grep wheel /etc/group >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6 File System Permissions

#--6.1.2

echo "s\_6.1.2" >> $outF.txt

echo "s\_6.1.2" >> error.txt

stat /etc/passwd >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.3

echo "s\_6.1.3" >> $outF.txt

echo "s\_6.1.3" >> error.txt

stat /etc/shadow >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.4

echo "s\_6.1.4" >> $outF.txt

echo "s\_6.1.4" >> error.txt

stat /etc/group >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.5

echo "s\_6.1.5" >> $outF.txt

echo "s\_6.1.5" >> error.txt

stat /etc/gshadow >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.6

echo "s\_6.1.6" >> $outF.txt

echo "s\_6.1.6" >> error.txt

stat /etc/passwd- >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.7

echo "s\_6.1.7" >> $outF.txt

echo "s\_6.1.7" >> error.txt

stat /etc/shadow- >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.8

echo "s\_6.1.8" >> $outF.txt

echo "s\_6.1.8" >> error.txt

stat /etc/group- >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.9

echo "s\_6.1.9" >> $outF.txt

echo "s\_6.1.9" >> error.txt

stat /etc/gshadow- >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.10

echo "s\_6.1.10" >> $outF.txt

echo "s\_6.1.10" >> error.txt

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -perm -0002 >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.11

echo "s\_6.1.11" >> $outF.txt

echo "s\_6.1.11" >> error.txt

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

#--6.1.12

echo "s\_6.1.12" >> $outF.txt

echo "s\_6.1.12" >> error.txt

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nogroup >> $outF.txt  2>> error.txt

echo "" >> $outF.txt

##### --- END of Script --- ####

**References**

* <https://www.cisecurity.org/cis-benchmarks/>
* <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/index>
* <https://cisofy.com/lynis/>