```
echo "REMINDER: Create a Snapshot before running. If you haven't stop this now."
echo " "
echo " "
echo " "
echo " "
echo " "
echo "This section sets/resets permissions and ownership of critical files."
#
#
touch /etc/cron.deny
touch /usr/share/infopage
touch /etc/at.allow
touch /etc/.login
touch /etc/security/opasswd
touch /var/log/wtmp
touch /var/log/btmp
touch /dev/audio
touch /etc/cron.allow
touch /etc/security/environ
#
mkdir /rootdir
cp -r /.??* /rootdir/.
#
chmod 0400 /etc/gshadow
chmod 0640 /etc/security/access.conf
chmod 0600 /etc/sysctl.conf
chmod 0600 /etc/securetty
chmod 0640 /etc/ntp.conf\
chmod 0600 /etc/security/opasswd
chmod -R 755 /etc/init.d/*
chmod -R 700 /root
chmod 0700 /rootdir
chmod -R 644 /etc/.login
chmod 0640 /path/to/system-log-file
chmod 0644 /path/to/manpage
chmod 0644 /etc/resolv.conf
chmod 0644 /etc/hosts
chmod 0644 /etc/nsswitch.conf
chmod 0644 /etc/passwd
chmod 0644 /etc/group
chmod 0400 /etc/shadow
chmod 600 /etc/hosts.equiv
chmod 600 /etc/ssh/shosts.equiv
```

chmod 0644 /etc/ssh/*key.pub
chmod 1777 /tmp
chmod 644 /etc/profile
chmod 644 /etc/bashr
chmod 644 /etc/environment
chmod 644 /etc/security/environ
chmod 644 /etc/skel
chmod 644 /dev/audio
chmod 640 /var/log/*
chmod 600 /etc/cron.allow
chmod 600 /etc/cron.deny
chmod 600 /var/spool/cron/*
chmod 600 /etc/cron.d/*
chmod 600 /etc/crontab
chmod 700 /etc/cron.daily/
chmod 700 /etc/cron.hourly/
chmod 700 /etc/cron.monthly/
chmod 700 /etc/cron.weekly/
chmod 600 /var/log/cron
chmod 600 /etc/at.allow
chmod 755 /var/spool/at/spool
chmod 700 /var/crash
chmod 640 /etc/xinetd.conf
chmod 640 /etc/xinetd.d
chmod 0644 /etc/services
chmod 0664 /etc/cups/printers.conf
chmod 700 /bin/traceroute
chmod 0644 /etc/aliases /etc/aliases.db
chmod 0644 /etc/postfix/aliases /etc/postfix/aliases.db
chmod 0640 /etc/ftpuserschmod 0640 /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers
chmod 0600 .Xauthority
chmod 640 /etc/syslog.conf
chmod 0644 /etc/ssh/*key.pub
chmod 0600 /etc/ssh/*key
chmod 0644 /etc/exports
chmod 0644 smb.conf.
chmod 0600 /etc/samba/passdb.tdb /etc/samba/secrets.tdb
chmod 0600 /etc/news/incoming.conf
chmod 600 /etc/grub.conf
chmod 755 /usr/lib/*
chmod 640 /etc/security/access.conf
chmod 644 /usr/share/man
chmod 644 /usr/share/info

```
chmod 644 /usr/share/infopage
chmod 744 /selinux
chmod 744 /sys/class/scsi_host/*
chmod 0600 /boot/grub/grub.conf
#
#
echo " "
echo "This section sets/resets file chown owner-user:owner-group file."
chown root:root /etc/security/access.conf
chown root:root /etc/sysctl.conf
chown root:root /etc/securetty
chown root:root /etc/ntp.conf
chown root:root /rootdir
chown root:root /etc/security/opasswd
chown root:root /etc/gshadow
chown root:root /etc/security/access.conf
chown root:root /etc/.login
chown root:root /tmp
chown root:root /etc/profile
chown root:root /etc/bashrc
chown root:root /etc/environment
chown root:root /etc/security/environ
chown root:root /dev/audio
chown root:root /var/spool/cron/
chown root:root /etc/cron.d/
chown root:root /etc/crontab
chown root:root /etc/cron.daily/
chown root:root /etc/cron.hourly/
chown root:root /etc/cron.monthly/
chown root:root /etc/cron.weekly/
chown root:root /var/spool/at/
chown root:root /etc/sysctl.conf
chown root:root /etc/xinetd.conf
chown root:root /etc/xinetd.d
chown root:root /etc/services
chown root:root /bin/traceroute
chown root:root /etc/syslog.conf
chown root:root /etc/security/access.conf
chown root:root /etc/securetty
chown root:root /boot/grub/grub.conf
#
#
echo " "
```

```
echo "This section removes extended ACL from file."
setfacl --remove-all /etc/gshadow
setfacl --remove-all /etc/security/access.conf
setfacl --remove-all /etc/sysctl.conf
setfacl --remove-all /etc/ntp.conf
setfacl --remove-all /usr/sbin/*
setfacl --remove-all /usr/share/man/* /usr/share/info/* /usr/share/infopage/*
setfacl --remove-all /usr/lib/* /lib/*
setfacl --remove-all /var/yp/*
setfacl --remove-all /etc/resolv.conf
setfacl --remove-all /etc/hosts
setfacl --remove-all /etc/nsswitch.conf
setfacl --remove-all /etc/passwd
setfacl --remove-all /etc/group
setfacl --remove-all /etc/shadow
setfacl --remove-all /etc/cron.allow
setfacl --remove-all /var/log/cron
setfacl --remove-all /etc/cron.deny
setfacl --remove-all /etc/at.allow
setfacl --remove-all /etc/at.deny
setfacl --remove-all /var/spool/at
setfacl --remove-all /etc/xinetd.conf
setfacl --remove-all /etc/cups/printers.conf
setfacl --remove-all /bin/traceroute
setfacl --remove-all /etc/aliases /etc/aliases.db
setfacl --remove-all /etc/postfix/aliases /etc/postfix/aliases.db
setfacl --remove-all /etc/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers
setfacl --remove-all .Xauthority
setfacl --remove-all /etc/syslog.conf
setfacl --remove-all /etc/exports
setfacl --remove-all /etc/samba/smb.conf
setfacl --remove-all /etc/samba/passdb.tdb /etc/samba/secrets.tdb
setfacl --remove-all /etc/news/hosts.nntp
setfacl --remove-all /etc/news/hosts.nntp.nolimit
setfacl --remove-all /etc/news/nnrp.access
setfacl --remove-all /etc/news/passwd.nntp
setfacl --remove-all /etc/ldap.conf
setfacl --remove-all /etc/grub.conf
#
#
echo " "
echo "This section removes unnecessary users."
-w /usr/sbin/userdel -p x
```

```
-w /usr/sbin/groupdel -p x
userdel lp
userdel sync
userdel shutdown
userdel halt
userdel news
userdel gopher
userdel operator
userdel games
userdel mail
userdel uucp
userdel ftp
userdel netdump
userdel adm
userdel pcap
userdel avahi-autoipd
userdel sabayon
userdel lp
userdel sync
userdel shutdown
userdel halt
userdel news
userdel gopher
userdel operator
userdel games
userdel mail
userdel uucp
userdel ftp
userdel netdump
userdel adm
userdel pcap
userdel avahi-autoipd
userdel sabayon
userdel reboot
#
#
#
#
# /etc/pam.d/passwd > /etc/pam.d/oldpasswd
# cp ./etc-pam.d/passwd /etc/pam.d/passwd
#
#echo "Replacing /etc/pam.d/system-auth..."
#/bin/cp /etc/pam.d/system-auth /etc/pam.d/system-auth_`date +%m-%d-20%y-%H%M`
```

```
#cp ./etc-pam.d-system-auth /etc/pam.d/system-auth
#
echo " "
echo "Password Complexity Compliance"
echo "Replacing /etc/pam.d/system-auth..."
/bin/cp /etc/pam.d/system-auth cat >> /etc/pam.d/system-auth
#
#/text
auth required pam_env.so
auth sufficient pam_unix.so nullok try_first_pass
#auth sufficient pam_smb_auth.so use_first_pass nolocal
auth requisite pam_succeed_if.so uid >= 500 quiet
auth required pam_deny.so
auth required pam_tally.so onerr=succeed no_magic_root
#
#account required pam_tally.so deny=3 no_magic_root reset
account required pam_unix.so broken_shadow
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 500 quiet
account required pam_permit.so
#
password sufficient pam_unix.so use_authtok md5 shadow remember=24
password requisite pam_cracklib.so retry=5 type= minlen=14 lcredit=-1 dcredit=-1 ocredit=-1
ucredit=-1 difok=3
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password required pam_deny.so
#
session optional pam_keyinit.so revoke
session required pam_limits.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
#end
#/text
#
#
#
#
#
#Edit /etc/gdm/custom.conf and add the following:
>> /etc/gdm/custom.conf
[server-Standard]
name=Standard server
command=/usr/bin/Xorg -br -audit 4 -s 15
```

```
chooser=false
handled=true
flexible=true
priority=0
#
#
#
#
#
echo "Replacing /etc/securetty..."
/bin/cp /etc/securetty /etc/securetty_`date +%m-%d-20%y-%H%M`
cp ./etc-securetty /etc/securetty
#
echo "Replacing /etc/security/opasswd"
/bin/cp /etc/security/opasswd /etc/security/opasswd_`date +%m-%d-20%y-%H%M`
cp ./etc-security-opasswd /etc/security/opasswd
#
echo "Replacing /etc/shadow..."
/bin/cp /etc/shadow /etc/shadow_`date +%m-%d-20%y-%H%M`
echo "WARNING - THIS WILL RESET THE ROOT PASSWD "
cp ./etc-shadow /etc/shadow
#
echo "Replacing /etc/shells..."
/bin/cp /etc/shells /etc/shells_`date +%m-%d-20%y-%H%M`
cp ./etc-shells /etc/shells
#
echo "Replacing /etc/ssh/sshd_config..."
/bin/cp /etc/ssh/sshd_config /etc/ssh/sshd_config_`date +%m-%d-20%y-%H%M`
cp ./etc-ssh-sshd_config /etc/ssh/sshd_config
#
echo "Replacing /etc/sysctl.conf..."
/bin/cp /etc/sysctl.conf /etc/sysctl.conf_`date +%m-%d-20%y-%H%M`
cp ./etc-sysctl.conf /etc/sysctl.conf
#
echo "Replacing /etc/syslog.conf..."
/bin/cp /etc/syslog.conf /etc/syslog.conf_`date +%m-%d-20%y-%H%M`
cp ./etc-syslog.conf /etc/syslog.conf
#
echo "Replacing /etc/xinetd.conf..."
/bin/cp /etc/xinetd.conf /etc/xinetd.conf_`date +%m-%d-20%y-%H%M`
cp ./etc-xinetd.conf /etc/xinetd.conf
#
#
```

```
#
#
#
#
>>/etc/audit/audit.rules
-a exit,always -F arch=<ARCH> -S creat -F exit=-EPERM
-a exit,always -F arch=<ARCH> -S creat -F exit=-EACCES
-a exit,always -F arch=<ARCH> -S open -F exit=-EPERM
-a exit,always -F arch=<ARCH> -S open -F exit=-EACCES
-a exit,always -F arch=<ARCH> -S openat -F exit=-EPERM
-a exit,always -F arch=<ARCH> -S openat -F exit=-EACCES
-a exit,always -F arch=<ARCH> -S truncate -F exit=-EPERM
-a exit,always -F arch=<ARCH> -S truncate -F exit=-EACCES
-a exit,always -F arch=<ARCH> -S ftruncate -F exit=-EPERM
-a exit,always -F arch=<ARCH> -S ftruncate -F exit=-EACCES
-a exit,always -S unlink
-a exit,always -S rmdir
-w /usr/sbin/useradd -p x -k useradd
-w /usr/sbin/groupadd -p x -k groupadd
-w /etc/passwd -p a -k passwd
-w /etc/shadow -p a -k shadow
-w /etc/group -p a -k group
-w /etc/gshadow -p a -k gshadow1
-w /usr/sbin/usermod -p x -k usermod
-w /usr/sbin/groupmod -p x -k groupmod
-w /etc/passwd -p w -k passwd
-w /etc/shadow -p w -k shadow
-w /etc/group -p w -k group
-w /etc/gshadow -p w -k gshadow
-w /usr/bin/passwd -p x -k passwd
-w /usr/sbin/userdel -p x
-w /usr/sbin/groupdel -p x
-a exit,always -F arch=<ARCH> -S sched_setscheduler
-w /etc/audit.rules
-w /etc/audit/audit.rules
-a exit,always -F arch=<ARCH> -S adjtimex
-a exit,always -F arch=<ARCH> -S settimeofday
-a exit,always -F arch=<ARCH> -S stime
-a exit,always -F arch=<ARCH> -S clock_settime
-a exit,always -F arch=<ARCH> -S sethostname
-a exit,always -F arch=<ARCH> -S setdomainname
-a exit,always -F arch=<ARCH> -S sched_setparam
#
```

```
#
#
#
#
#
#
echo " "
echo "post-h-script v1.1"
echo " "
echo "Running new job at `date +%m-%d-20%y-%H%M`"
echo " "
echo " "
#
echo " "
echo "Removing VNC"
yum -y remove vnc vnc-server
echo " "
echo "Removing Samba"
chkconfig smb off
yum -y remove smb
echo " "
echo "Removing TFTP Server"
yum -y remove tftp-server
echo " "
echo "Removing Telnet"
yum -y remove telnet telnet-server krb5-workstation
echo " "
echo "Removing MINICOM"
yum -y remove minicom
echo " "
echo "Removing RSH"
yum -y remove rsh rsh-server
echo " "
echo "Removing NIS"
chkconfig ypbind off
yum -y remove ypserv
echo " "
echo "Removing DHCP Server"
chkconfig dhcpd off
yum -y remove dhcp
echo " "
echo "Disabling FTP Server"
chkconfig vsftpd off
```

```
echo " "
echo "Install Console Screen Lock"
yum -y install vlock
echo " "
echo "Removing IP6Tables"
chkconfig ip6tables off
yum -y remove ip6tables
#
#
#
#
#
#
echo " "
echo "Disabling Unnecessary Services"
chkconfig anacron off
chkconfig apmd off
service autofs stop ; chkconfig autofs off
chkconfig avahi-daemon offy
chkconfig bluetooth off
chkconfig cups off
chkconfig firstboot off
chkconfig gpm off
chkconfig gssftp off
chkconfig haldaemon off
chkconfig hidd off
chkconfig hplip off
chkconfig ip6tables off
chkconfig isdn off
service kdump stop ; chkconfig kdump off
chkconfig kudzu off
chkconfig mcstrans off
chkconfig mdmonitor off
chkconfig messagebus off
chkconfig microcode_ctl off
chkconfig pcscd off
service portmap stop ; chkconfig portmap off
chkconfig readahead_early off
chkconfig readahead_later off
chkconfig setroubleshoot off
chkconfig tftp off
chkconfig telnet off
chkconfig uucp off
```

```
service uucp stop
chkconfig vsftpd off
service xinetd stop ; chkconfig xinetd off
chkconfig xfs off
chkconfig yum-updatesd off ; service yum-updatesd stop
#
#
echo " "
echo "Enabling Necessary Services"
service auditd start ; chkconfig auditd on
chkconfig iptables on; service iptables start
service ntpd start ; chkconfig ntpd on
#
#
#
echo "Prevent the usb-storage module from loading."
echo'install usb-storage /bin/true' >> /etc/modprobe.conf
# MODPROBE=/etc/modprobe.conf
# if [ -f ${MODPROBE} ]; then
# if [ $(grep -c "install[[:space:]]cransfs[[:space:]]/bin/true" # ${MODPROBE}) -lt 1 ]; then
# echo "install cramfs /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]freevxfs[[:space:]]/bin/true" #${MODPROBE}) -lt 1 ]; then
# echo "install freevxfs /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]jffs2[[:space:]]/bin/true" ${MODPROBE}) -lt 1 ]; then
# echo "install jffs2 /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]hfs[[:space:]]/bin/true" ${MODPROBE}) -lt 1 ]; then
# echo "install hfs /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]hfsplus[[:space:]]/bin/true" # ${MODPROBE}) -lt 1 ]; then
# echo "install hfsplus /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]squashfs[[:space:]]/bin/true" #${MODPROBE}) -lt 1 ]; then
# echo "install squashfs /bin/true" >> ${MODPROBE}
# fi
# if [ $(grep -c "install[[:space:]]udf[[:space:]]/bin/true" ${MODPROBE}) -lt 1 ]; then
# echo "install udf /bin/true" >> ${MODPROBE}
# fi
# fi
# NETWORK_SYS=/etc/sysconfig/network
# if [ -f ${MODPROBE} ]; then
```

```
# if [ $(grep -c "NETWORKING_IPV6=no" ${NETWORK_SYS}) -lt 1 ]; then
# echo "NETWORKING_IPV6=no" >> ${NETWORK_SYS}
# fi
# if [ $(grep -c "IPV6INIT=no" ${NETWORK_SYS}) -lt 1 ]; then
# echo "IPV6INIT=no" >> ${NETWORK_SYS}
# fi
# if [ $(grep -c "IPV6_AUTOCONF=no" ${NETWORK_SYS}) -lt 1 ]; then
# echo "IPV6_AUTOCONF=no" >> ${NETWORK_SYS}
# fi
# fi
# LIMITS=/etc/security/limits.conf
# if [ -f ${LIMITS} ]; then
# if [ $(grep -c "*[[:space:]]hard[[:space:]]core[[:space:]] 0" # ${LIMITS}) -lt 1 ]; then
# echo "* hard core 0" >> ${LIMITS}
# fi
# fi
#
#
echo " "
echo " "
echo "Reboot System after script completes"
```