# Linux Hardening Settings

## Make sure OS is getting patched on a regular basis –

apt-get upgrade

## Make sure folders are secure–

**/tmp**

mount -o remount,nodev,nosuid,noexec /tmp

mount --bind /tmp /var/tmp

/tmp /var/tmp none bind 0 0

**/home**

mount -o remount,nodev /home

**/run/shm**

mount -o remount,nodev,nosuid,noexec /run/shm

**Set Sticky bit on writable directories**

df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -perm -0002 2>/dev/null | xargs chmod a+t

**Disable automounting \*Very important**

update-rc.d autofs disable

Audit: Ensure autofs is not enabled:

# ls /etc/rc\*.d | grep autofs Ensure no S\* lines are returned.

**Set User/Group Owner on bootloader config**

chown root:root /boot/grub/grub.cfg

chmod og-rwx /boot/grub/grub.cfg

**Create a boot password**

grub-mkpasswd-pbkdf2 Enter password: Reenter password: Your PBKDF2 is

**Make sure the root user has a password set**

passwd root

Add the following line to the /etc/sysctl.conf file.

kernel.randomize\_va\_space = 2

/usr/sbin/prelink –ua

apt-get purge nis

**Remove or comment out any shell, login, or exec lines in /etc/inetd.conf:**

#shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd #login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind #exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd

apt-get purge rsh-client rsh-reload-client

**Remove or comment out any talk or ntalk lines in /etc/inetd.conf:**

#talk dgram udp wait nobody.tty /usr/sbin/in.talkd in.ta lkd #ntalk dgram udp wait nobody.tty /usr/sbin/in.ntalkd in.nt alkd

apt-get purge talk

**Remove or comment out any telnet lines in /etc/inetd.conf:**

#telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd

Remove or comment out any tftp lines in /etc/inetd.conf:

#tftp stream tcp nowait root internal

update-rc.d xinetd disable

**Remove or comment out any chargen lines in /etc/inetd.conf:**

#chargen stream tcp nowait root internal

**Remove or comment out any echo lines in /etc/inetd.conf:**

#echo stream tcp nowait root internal

**Remove or comment out any discard lines in /etc/inetd.conf:**

#discard stream tcp nowait root internal

# apt-get purge xserver-xorg-core\*

**Disable Services**

systemctl disable avahi-daemon

systemctl disable cups

update-rc.d isc-dhcp-server disable

apt-get purge slapd

update-rc.d rpcbind disable

update-rc.d nfs-kernel-server disable

systemctl disable bind9

systemctl disable vsftpd

update-rc.d apache2 disable

systemctl disable dovecot

update-rc.d smbd disable

update-rc.d squid3 disable

update-rc.d snmpd disable

Set RSYNC\_ENABLE to false in /etc/default/rsync:

RSYNC\_ENABLE=false

Set the net.ipv4.ip\_forward parameter to 0 in /etc/sysctl.conf:

net.ipv4.ip\_forward=0 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.ip\_forward=0

/sbin/sysctl -w net.ipv4.route.flush=1

Set the net.ipv4.conf.all.send\_redirects and net.ipv4.conf.default.send\_redirects parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.send\_redirects=0 net.ipv4.conf.default.send\_redirects=0 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.conf.all.send\_redirects=0

/sbin/sysctl -w net.ipv4.conf.default.send\_redirects=0

/sbin/sysctl -w net.ipv4.route.flush=1

Install ntp:

apt-get install ntp

Ensure the following lines are in /etc/ntp.conf:

restrict -4 default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery

Also, make sure /etc/ntp.conf has at least one NTP server specified: server

Set the net.ipv4.conf.all.accept\_source\_route and net.ipv4.conf.default.accept\_source\_route parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.accept\_source\_route=0 net.ipv4.conf.default.accept\_source\_route=0 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.conf.all.accept\_source\_route=0

/sbin/sysctl -w net.ipv4.conf.default.accept\_source\_route=0

/sbin/sysctl -w net.ipv4.route.flush=1

Set the net.ipv4.conf.all.accept\_redirects and net.ipv4.conf.default.accept\_redirects parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.accept\_redirects=0 net.ipv4.conf.default.accept\_redirects=0 Modify active kernel parameters to match: 60 | P a g e

/sbin/sysctl -w net.ipv4.conf.all.accept\_redirects=0

/sbin/sysctl -w net.ipv4.conf.default.accept\_redirects=0

/sbin/sysctl -w net.ipv4.route.flush=1

Set the net.ipv4.conf.all.secure\_redirects and net.ipv4.conf.default.secure\_redirects parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.secure\_redirects=0 net.ipv4.conf.default.secure\_redirects=0 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.conf.all.secure\_redirects=0

/sbin/sysctl -w net.ipv4.conf.default.secure\_redirects=0

/sbin/sysctl -w net.ipv4.route.flush=1

Set the net.ipv4.icmp\_ignore\_bogus\_error\_responses parameter to 1 in /etc/sysctl.conf: net.ipv4.icmp\_ignore\_bogus\_error\_responses=1 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.icmp\_ignore\_bogus\_error\_responses=1

/sbin/sysctl -w net.ipv4.route.flush=1

Set the net.ipv4.tcp\_syncookies parameter to 1 in /etc/sysctl.conf:

net.ipv4.tcp\_syncookies=1 Modify active kernel parameters to match:

/sbin/sysctl -w net.ipv4.tcp\_syncookies=1

/sbin/sysctl -w net.ipv4.route.flush=1

Create or edit the file /etc/sysctl.conf and add the following lines:

net.ipv6.conf.all.disable\_ipv6=1 net.ipv6.conf.default.disable\_ipv6=1

net.ipv6.conf.lo.disable\_ipv6=1

Run the following command or reboot to apply the changes: # sysctl –p

echo "install dccp /bin/true" >> /etc/modprobe.d/CIS.conf

echo "install sctp /bin/true" >> /etc/modprobe.d/CIS.conf

echo "install rds /bin/true" >> /etc/modprobe.d/CIS.conf

echo "install tipc /bin/true" >> /etc/modprobe.d/CIS.conf

Enable cron and anacron:

systemctl enable cron

systemctl enable anacron

chown root:root /etc/crontab

chmod og-rwx /etc/crontab

chown root:root /etc/cron.hourly

chmod og-rwx /etc/cron.hourly

chown root:root /etc/cron.daily

chmod og-rwx /etc/cron.daily

chown root:root /etc/cron.weekly

chmod og-rwx /etc/cron.weekly

chown root:root /etc/cron.monthly

chmod og-rwx /etc/cron.monthly

chown root:root /etc/cron.d

chmod og-rwx /etc/cron.d

/bin/rm /etc/cron.deny

/bin/rm /etc/at.deny

touch /etc/cron.allow

touch /etc/at.allow

chmod og-rwx /etc/cron.allow

chmod og-rwx /etc/at.allow

chown root:root /etc/cron.allow

chown root:root /etc/at.allow

Install the iptables and iptables-persistent packages:

apt-get install iptables iptables-persistent Enable the netfilter-persistent service:

update-rc.d netfilter-persistent enable

Install the libpam-cracklib package:

apt-get install libpam-cracklib Set the pam\_cracklib.so parameters as follows in /etc/pam.d/common-password: password required pam\_cracklib.so retry=3 minlen=14 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1

Edit the /etc/pam.d/login file and add the auth line below: auth required pam\_tally2.so onerr=fail audit silent deny=5 unlock\_time=900

Set the pam\_unix.so remember parameter to 5 in /etc/pam.d/common-password: password [success=1 default=ignore] pam\_unix.so obscure sha512 remember=5

dpkg -s openssh-server

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: Protocol 2

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: LogLevel INFO

chown root:root /etc/ssh/sshd\_config

chmod 600 /etc/ssh/sshd\_config

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: X11Forwarding no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: MaxAuthTries 4

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: IgnoreRhosts yes

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: HostbasedAuthentication no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: PermitRootLogin no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: PermitEmptyPasswords no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: PermitUserEnvironment no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: Ciphers aes128-ctr,aes192-ctr,aes256-ctr

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: ClientAliveInterval 300 ClientAliveCountMax 0

Edit the /etc/ssh/sshd\_config file to set one or more of the parameter as follows: AllowUsers AllowGroups DenyUsers DenyGroups

Edit the /etc/ssh/sshd\_config file to set the parameter as follows: Banner /etc/issue.net

add the following line to the /etc/pam.d/su file. auth required pam\_wheel.so use\_uid Once this is done, create a comma separated list of users in the wheel statement in the /etc/group file.

Set the PASS\_MAX\_DAYS parameter to 90 in /etc/login.defs: PASS\_MAX\_DAYS 90 Modify user parameters for all users with a password set to match: # chage --maxdays 90

Set the PASS\_WARN\_AGE parameter to 7 in /etc/login.defs: 129 | P a g e PASS\_WARN\_AGE 7 Modify user parameters for all users with a password set to match: # chage --warndays 7

!/bin/bash for user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [ $user != "root" ] then /usr/sbin/usermod -L $user if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ] then /usr/sbin/usermod -s /usr/sbin/nologin $user fi 130 | P a g e fi done

usermod -g 0 root

Edit the /etc/bash.bashrc and /etc/profile.d/cis.sh files (and the appropriate files for any other shell supported on your system) and add the following the UMASK parameter as shown: umask 077

useradd -D -f 35

touch /etc/motd # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue # echo "Authorized uses only. All activity may be \ monitored and reported." > /etc/issue.net chown root:root /etc/motd # chmod 644 /etc/motd

chown root:root /etc/issue

chmod 644 /etc/issue

chown root:root /etc/issue.net

chmod 644 /etc/issue.net

Edit the /etc/motd, /etc/issue and /etc/issue.net files and remove any lines containing \m, \r, \s or \v

banner-message-enable=true banner-message-text=''

/bin/chmod 644 /etc/passwd

/bin/chmod 640 /etc/shadow

/bin/chmod 644 /etc/group

/bin/chown root:root /etc/passwd

/bin/chown root:shadow /etc/shadow

/bin/chown root:root /etc/group

/usr/bin/passwd –l <username>

OS 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. The actions in this section of the document provide guidance on what services can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system.

Optional – I would play with this if you have the time

2.18 Disable Mounting of cramfs Filesystems (Not Scored) Profile Applicability: • Level 2 Description: The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image.

Rationale: Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit: # /sbin/modprobe -n -v cramfs install /bin/true # /sbin/lsmod | grep cramfs 22 | P a g e

Remediation: Edit or create the file /etc/modprobe.d/CIS.conf and add the following line:

install cramfs /bin/true