ULTIMATE LINUX CHECKLIST

“Please help im dying” - Danh Alpha
“Shoot im back” - Ayaan Beta

GREEN - paste into terminal and run
ORANGE - should be in a text file
Blue Highlight - included in script already
Red Highlight - NOT included in script MUST DO MANUALLY

---

1. Packages

Updates

- Update system
  apt update && apt upgrade && apt dist-upgrade

Package Management

- Check sources list at
  gedit /etc/apt/sources.list
  gedit /etc/apt/sources.list.d/
    - Remove suspicious entries
- Install Packages from README and for auditing software
  apt install apt-listbugs -y
  apt install apt-listchanges -y
- Remove unauthorized packages
- Remove games, hacking tools, networking tools, servers, etc
- To list packages: apt list --installed | cut -d/ -f1
- To remove package:
  apt purge [package]
  apt purge ssh ftp telnet openssh-* samba-* *-samba smbd telnet avahi-* cups cups-* *-cups slapd ldap-utils nfs-common nfs-kernel-server rsync talk

---

2. Security Policies

Remove media files, backdoors, PII files, etc

ls -alR /home/*/*

Install security packages

```
apt install libpam-cracklib -y
apt install libpam-tmpdin -y
apt install libpam-usb -y
apt install auditd -y
apt install libpam-pwquality -y
```

Password policy

- Secure common-password file

```
gedit /etc/pam.d/common-password
auth    required        pam_cracklib.so reject_username enforce_for_root
maxclassrepeat=5 maxsequence=5 dcredit=-1 ocredit=-1 lcredit=-1 ucredit=-1
minlen=16 difok=5 retry=3
auth    required        pam_unix.so sha512 use_authtok remember=5
password requisite      pam_pwquality.so retry=3
password [success=1 default=ignore] pam_unix.so sha512
password required       pam_pwhistory.so remember=5
```

- What the hell is this but it works?

```
cat /etc/passwd | awk -F: '( $3 >= 1000 && $1 != "nfsnobody" ) { print $1 }' | xargs
-n 1 chage -d 0
```

- Secure login.defs file

```
gedit /etc/login.defs:
PASS_MAX_DAYS 90
PASS_MIN_DAYS 10
PASS_WARN_AGE 7
umask 027
```

- Secure pwquality.conf file

```
gedit /etc/security/pwquality.conf:
minlen = 16
dcredit = -1
ucredit = -1
ocredit = -1
lcredit = -1
try_first_pass
```

- Set default inactivity to be 30 days till disabled **(IDK ABT THIS ONE)**

```
useradd -D -f 30
chage --inactive 30 <user> # make script for every user
usermod -s /usr/sbin/nologin <user> #make scripte for every system user
echo "don't let any user have password change date in the future"
#!/bin/bash
for user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do
        if [ $user != "root" ]; then
                usermod -L $user
```

```
                if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ]; then
                        usermod -s /usr/sbin/nologin $user
                fi
        fi
done
```

Audit policy

- Secure audit.rules file
  gedit /etc/audit/audit.rules
  -D
  -w / -p rwax -k filesystem_change
  -a always,exit -S all
  -e 2
- Secure auditd.conf file
  gedit /etc/audit/auditd.conf:
  max_log_file_action=keep_log

Account lockout policy

- Be careful with this, you may lock yourself out of root, do this at the end if you still need points
- Secure common-auth file
  gedit /etc/pam.d/common-auth
  auth required pam_tally2.so deny=5 onerr=fail audit even_deny_root lock_time=1200 unlock_time=1800
- OR
  auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900
- Secure /etc/bash.bashrc | /etc/profile | /etc/profile.d/*.sh
  gedit /etc/bash.bashrc | /etc/profile | /etc/profile.d/*.sh
  TMOUT=600
  umask 027
- Make sure you don't lock yourself out by running /sbin/pam_tally2 -u $USER --reset often

banners (very serious)

- /etc/motd | /etc/issue | /etc/issue.net | replace with:
- waRnINg: if yOu HAx0R, ExIt SYSTEM noW! sySTEM no liKe hAX0rs. anYtHiNG You DO HerE mAy Be recORdEd WITH SuRVEILLanCE SyStemS, So wE KNow IF YOU BAD.

Security Options

USB

- Disable USB
  service autofs stop

systemctl disable autofs
apt install usb-storage -y
apt install USBGaurdd -y
systemctl enable USBGaurdd

Users

- lock unauthorized users
  chown root:root /etc/passwd
  chmod 644 /etc/passwd
  chown root:root /etc/shadow
  chmod o-rwx,g-wx /etc/shadow
  chown root:root /etc/group
  chmod 644 /etc/group
  chown root:shadow /etc/gshadow
  chmod o-rwx,g-rw /etc/gshadow
  chown root:root /etc/passwd-
  chmod u-x,go-wx /etc/passwd-
  chown root:root /etc/shadow-
  chown root:shadow /etc/shadow-
  chmod o-rwx,g-rw /etc/shadow-
  chown root:root /etc/group-
  chmod u-x,go-wx /etc/group-
  chown root:root /etc/gshadow-
  chown root:shadow /etc/gshadow-
  chmod o-rwx,g-rw /etc/gshadow-
- lock root
  usermod -s /bin/false root
  usermod -L root
  usermod -g 0 root
- lock root to physical consoles
  gedit /etc/securetty
    - remove entries for any consoles that are not in a physically secure location
- Secure lightdm.conf
    - This varies depending on the display manager, yours may be gdm (gnome display manager) or lightdm, do the steps accordingly

  gedit /etc/lightdm/lightdm.conf
  allow-guest=true => allow-guest=false
  autologin-user=[user] => autologin-user=
- Secure custom.conf
  gedit /etc/gdm/custom.conf
  AutomaticLoginEnable=true => AutomaticLoginEnable=false
  AutomaticLogin=[user] => AutomaticLogin=
- Secure gdm-password file

gedit /etc/pam.d/gdm-password
auth sufficient pam_succeed_if.so user ingroup nopasswdlogin => DELETE LINE

groups

- Create groups specified in README:
  groupadd [group]
- Delete groups not in the README:
  groupdel [group]
- Add users to groups especially administrators to the sudo and wheel group:
  usermod -aG [group] [user]
- Remove users from groups especially unauthorized administrations from the sudo group:
  gpasswd -d [user] [group]
- /etc/group:
  wheel:x:10:root,<user list>

configure sudo

gedit visudo:
Defaults requiretty
Defaults use_pty
Defaults lecture="always"
Defaults log_input,log_output
Defaults passwd_tries=3
Defaults passwd_timeout=1
gedit /etc/pam.d/su:
auth required pam_wheel.so

---

3. Networking

Firewall

apt install ufw iptables -y
ufw enable
ufw default deny incoming
ufw logging verbose
gedit /etc/default/ufw
IPV6=no => IPV6=yes

- Allow or deny connections for critical services or backdoors:
  ufw [allow/deny] [program/port/ip address]

Backdoors

apt install nmap -y && nmap -sVf -p- 127.0.0.1 && apt purge nmap -y
lsof -i -n -p

netstat -tulpn

dns

- Remove non default entries in /etc/hosts

hosts files

gedit /etc/hosts.allow

- Remove suspicious entries

gedit /etc/hosts.deny:

ALL: ALL

---

4. Security Auditing

Unauthorized services

service --status-all

- remove bad services

systemctl disable [service] && systemctl stop [service]

Critical Serivces

OpenSSH Server

apt install openssh-server -y

service ssh enable

service ssh start

chown root:root /etc/ssh/sshd_config

chmod og-rwx /etc/ssh/sshd_config

- Secure sshd_config file

gedit /etc/ssh/sshd_config:

#KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

#Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

UsePrivilegeSeparation sandbox

Subsystem sftp internal-sftp -f AUTHPRIV -l INFO

AllowTcpForwarding no

AllowStreamLocalForwarding no

GatewayPorts no
PermitTunnel no
UseDNS no
Compression no
TCPKeepAlive no
AllowAgentForwarding no
PermitRootLogin no
Port 8808
ForwardX11 no
Protocol 2
LogLevel INFO # Verbose
X11Forwarding no
MaxAuthTries 2
IgnoreRhosts yes
HostbasedAuthentication no
PermitEmptyPasswords no
PermitUserEnvironment no
ClientAliveInterval 300
ClientAliveCountMax 0
LoginGraceTime 60
Banner /etc/issue.net
ListenAddress 0.0.0.0
MaxSessions 2
MaxStartups 2
PasswordAuthentication yes/no ???????
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
service sshd restart
sshd -T
ufw allow 8808
systemctl reload sshd

mySQL

apt install mysql-server -y
mysql_secure_installation
service mysql enable
service mysql start

- Secure mysqld.cnf file

/etc/mysql/mysql.conf.d/mysqld.cnf
bind-address = 127.0.0.1
user = mysql
port = 1542

```
local_infile = 0
symbolic-links = 0
default_password_lifetime = 90
service mysql restart
```

Apache

```
apt install apache2
service apache2 start
service apache2 enable
ufw allow "Apache Full"
apt install libapache2-mod-security2
mv /etc/modsecurity/modsecurity.conf-recommended
/etc/modsecurity/modsecurity.conf
useradd -r -s /bin/false apache
groupadd apache
useradd -G apache apache
chown -R apache:apache /opt/apache
chmod -R 750 /etc/apache2/*
/etc/apache2/apache2.conf
ServerTokens Prod
ServerSignature Off
FileETag None
User apache
Group apache
TraceEnable off
Timeout 60
Header always append X-Frame-Options SAMEORIGIN
Header set X-XSS-Protection "1; mode=block"
<Directory />
Options –Indexes -Includes
AllowOverride None
</Directory>
<LimitExcept GET POST HEAD>
deny from all
</LimitExcept>
# $EDITOR httpsd.conf
<Directory /opt/apache/htdocs>
Options None
</Directory>
<Directory />
Options -Indexes
AllowOverride None
</Directory>
service apache2 restart
```

postfix

- Secure main.cf

  gedit /etc/postfix/main.cf

  inet_interfaces = loopback-only

---

5. cron

- systemctl enable cron

  rm /etc/cron.deny

  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

  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# systemctl enable cron

  rm /etc/cron.deny

  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

  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
```

---

6. mounting

```
mount -o remountcnoexec /dev/shm
mount -o remount,nosuid /dev/shm1
mount -o remount,nodev /dev/shm
```

Secure fstab

```
gedit /etc/fstab
none /run/shm tmpfs defaults,ro 0 0
```

---

7. Kernel

Secure sysctl.conf

```
gedit /etc/sysctl.conf
fs.protected_hardlinks=1
fs.protected_symlinks=1
fs.suid_dumpable=0
kernel.exec-shield=1
kernel.randomize_va_space=2
net.ipv4.ip_forward=0
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.all.accept_source_route=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.all.secure_redirects=0
net.ipv6.conf.all.accept_ra=0
net.ipv4.conf.default.secure_redirects=0
net.ipv4.conf.default.send_redirects=0
net.ipv4.conf.default.log_martians=1
net.ipv4.conf.default.rp_filter=1
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.icmp_ignore_bogus_error_messages=1
net.ipv4.icmp_ignore_bogus_error_responses=1
```

```
net.ipv4.tcp_syncookies=1
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.all.disable_ipv6 = 1 # Careful! This disables IPv6
net.ipv6.conf.default.accept_ra=0
net.ipv6.conf.default.accept_redirects=0
```

Secure limits.conf

```
gedit /etc/security/limits.conf
* hard core 0
```

Secure CIS.conf

```
gedit /etc/modprobe.d/CIS.conf
install dccp /bin/true
install sctp /bin/true
install rds /bin/true
install tipc /bin/true
```

Secure host.conf

```
gedit /etc/host.conf
order bind,hosts
multi on
nospoof on
```

Secure resolv.conf

```
gedit /etc/resolv.conf
make server 8.8.8.8
/etc/rc.local:
exit 0
```

---

8. File permisions

Check permissions for

- /etc/gshadow
- /etc/passwd
- /etc/group
- /etc/shadow
- /etc/hosts
- /etc/hosts.deny
- /etc/hosts.allow

---

9. Audit

no world writable files

```
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -perm -0002
```

no unowned files or directories

```
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser
#df --local -P | awk {'if (NR!=1) print $6'} | xargs -r '{}' find '{}' -xdev -nogroup
```

no unowned files or directories

```
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nogroup
```

SUID executable

```
df --local -P | awk {'if (NR!=1)print $6'} | xargs -I '{}' find '{}' -xdev -type f -perm -4000
#df --local -P | awk {'if (NR!=1) print $6'} | xargs -r '{}' find '{}' -xdev -type f -perm -4000
```

SGID executables

```
df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type f -perm -2000
```

---

10. Miscellaneous

```
snap refresh
apt install rsyslog -y
systemctl enable rsyslog
```

Secure rsyslog.conf

```
gedit /etc/rsyslog.conf:
```

- Remove anything that sends logs to a domain

```
apt purge xinetd openbsd-inetd inetutils-inetd -y
apt install tcpd -y
apt install apparmor -y
aa-enforce /etc/apparmor.d/*
```

---

11. CIS documents

/etc/modprobe.d/CIS.conf:

- install cramfs /bin/true
- install freevxfs /bin/true
- install jffs2 /bin/true
- install hfs /bin/true
- install hfsplus /bin/true
- install udf /bin/true
- rmmod udf
- rmmod hfsplus
- rmmod hfs
- rmmod jffs2
- rmmod freevxfs
- rmmod cramfs
-
- echo "file systems on separate partitians /tmp /var /var/tmp /var/log /var/log/audit /home"
- echo "edit the fstab to do the following options"
- mount -o remount,nodev /tmp
- mount -o remount,nosuid /tmp
- mount -o remount,nodev /var/tmp
- mount -o remount,nosuid /var/tmp
- mount -o remount,noexec /var/tmp
- mount -o remount,nodev /home
- mount -o remount,nodev /dev/shm
- mount -o remount,nosuid /dev/shm
- mount -o remount,noexec /dev/shm
- echo "edit fstab to have nodev, nosuid, noexec, for all removable media pertitians"
- df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -perm -0002 2>/dev/null | xargs chmod a+t
- systemctl disable autofs
- systemctl stop autofs
- apt-cache policy
- apt-key list
- apt-get install aide aide-common
- aideinit
- crontab -u root -e:
- 0 5 * * * /usr/bin/aide --config /etc/aide/aide.conf --check
- chown root:root /boot/grub/grub.cfg
- chmod og-rwx /boot/grub/grub.cfg
- grub-mkpasswd-pbkdf2
- /etc/grub.d/00_header
- cat <<EOFset superusers="<username>"password_pbkdf2 <username> <encrypted-password>EOF

- update-grub
- passwd root
- /etc/security/limits.conf or /etc/security/limits.d/*
- # hard core 0
- /etc/sysctl.conf or /etc/sysctl.d/*
- fs.suid_dumpable = 0
- kernel.randomize_va_space = 2
- sysctl -w kernel.randomize_va_space=2
- sysctl -w fs.suid_dumpable=0
- echo "sysctl -p"
- echo "Ensure XD/NX support is enabled"
- prelink -ua
- apt-get remove prelink

SELINUX!!!!!!!

- **/etc/default/grub:**
  - remove all => selinux=0 enforcing=0
  - GRUB_CMDLINE_LINUX_DEFAULT="quiet"
  - GRUB_CMDLINE_LINUX=""
  - update-grub
- **/etc/selinux/config:**
  - SELINUX=enforcing
  - SELINUXTYPE=ubuntu
  - ps -eZ | egrep "initrc" | egrep -vw "tr|ps|egrep|bash|awk" | tr ':' ' ' | awk '{ print $NF }'
  - echo "investigate unconfied daemons"

APPARMOR

- **/etc/default/grub:**
  - remove all => apparmor=0 from CMDLINE_LINUX parameters
  - GRUB_CMDLINE_LINUX_DEFAULT="quiet"
  - GRUB_CMDLINE_LINUX=""
  - update-grub
  - apparmor_status
  - aa-enforce /etc/apparmor.d/*
  - apt-get install selinux
  - apt-get install apparmor
- **/etc/motd:**
  - remove => \m \r \s \v
  - 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
- **/etc/dconf/profile/gdm:**
    - user-db:user
    - system-db:gdm
    - file-db:/usr/share/gdm/greeter-dconf-defaults
- **/etc/dconf/db/gdm.d/01-banner-message:**
    - [org/gnome/login-screen]
    - banner-message-enable=true
    - banner-message-text='Authorized uses only. All activity may be monitored and reported.'
    - dconf update
- **/etc/inetd.conf or /etc/inetd.d/*:**
    - remove anything starting with chargen | daytime | discard | echo | time | shell, login, exec | talk, ntalk | telnet | tftp |
- **/etc/xinetd.conf and /etc/xinetd.d/*:**
    - disable = yes on all chargen | daytime | discard | echo | time | rsh, rloging, rexec | talk | telnet | tftp |
    - systemctl disable xinetd
    - apt-get remove openbsd-inetd
    - apt-get install ntp
    - apt-get install chrony
    - systemctl enable ntp
    - systemctl enable chrony
- **/etc/ntp.conf:**
    - estrict -4 default kod nomodify notrap nopeer noquery
    - restrict -6 default kod nomodify notrap nopeer noquery
    - server <remote-server>
- **/etc/init.d/ntp:**
    - RUNASUSER=ntp
- **/etc/chrony/chrony.conf:**
    - server <remote-server>
    - apt-get remove xserver-xorg* # Be very careful
    - systemctl disable avahi-daemon #remove?????
    - systemctl disable cups # remove cups? configuring printing?
    - systemctl disable isc-dhcp-server
    - systemctl disable isc-dhcp-server6
    - systemctl disable slapd
    - systemctl disable nfs-server
    - systemctl disable rpcbind
    - systemctl disable bind9

    - systemctl disable vsftpd
    - systemctl disable apache2
    - systemctl disable dovecot
    - systemctl disable smbd
    - systemctl disable squid
    - systemctl disable snmpd
    - /etc/postfix/main.cf
    - RECIVING MAIL section =>
    - inet_interfaces = loopback-only
    - systemctl restart postfix
    - systemctl disable rsync
    - systemctl disable nis
    - apt-get remove nis
    - apt-get remove rsh-client rsh-redone-client
    - apt-get remove talk
    - apt-get remove telnet
    - apt-get remove ldap-utils
- **/etc/sysctl.conf or /etc/sysctl.d/*:**
    - net.ipv4.ip_forward = 0
    - net.ipv4.conf.all.send_redirects = 0
    - net.ipv4.conf.default.send_redirects = 0
    - net.ipv4.conf.all.accept_source_route = 0
    - net.ipv4.conf.default.accept_source_route = 0
    - net.ipv4.conf.all.accept_redirects = 0
    - net.ipv4.conf.default.accept_redirects = 0
    - net.ipv4.conf.all.secure_redirects = 0
    - net.ipv4.conf.default.secure_redirects = 0
    - net.ipv4.conf.all.log_martians = 1
    - net.ipv4.conf.default.log_martians = 1
    - net.ipv4.icmp_echo_ignore_broadcasts = 1
    - net.ipv4.icmp_ignore_bogus_error_responses = 1
    - net.ipv4.conf.all.rp_filter = 1
    - net.ipv4.conf.default.rp_filter = 1
    - net.ipv4.tcp_syncookies = 1
    - net.ipv6.conf.all.accept_ra = 0
    - net.ipv6.conf.default.accept_ra = 0
    - net.ipv6.conf.all.accept_redirects = 0
    - net.ipv6.conf.default.accept_redirects = 0
    - sysctl -w net.ipv4.ip_forward=0
    - sysctl -w net.ipv4.route.flush=1
    - sysctl -w net.ipv4.conf.all.send_redirects=0
    - sysctl -w net.ipv4.conf.default.send_redirects=0
    - sysctl -w net.ipv4.route.flush=1
    - sysctl -w net.ipv4.conf.all.accept_source_route=0

- sysctl -w net.ipv4.conf.default.accept_source_route=0
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.conf.all.accept_redirects=0
- sysctl -w net.ipv4.conf.default.accept_redirects=0
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.conf.all.secure_redirects=0# sysctl -w net.ipv4.conf.default.secure_redirects=0# sysctl -w net.ipv4.route.flush=1sysctl -w net.ipv4.conf.all.secure_redirects=0
- sysctl -w net.ipv4.conf.default.secure_redirects=0
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.conf.all.log_martians=1
- sysctl -w net.ipv4.conf.default.log_martians=1
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.conf.all.rp_filter=1
- sysctl -w net.ipv4.conf.default.rp_filter=1
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv4.tcp_syncookies=1
- sysctl -w net.ipv4.route.flush=1
- sysctl -w net.ipv6.conf.all.accept_ra=0
- sysctl -w net.ipv6.conf.default.accept_ra=0
- sysctl -w net.ipv6.route.flush=1
- sysctl -w net.ipv6.conf.all.accept_redirects=0
- sysctl -w net.ipv6.conf.default.accept_redirects=0
- sysctl -w net.ipv6.route.flush=1

- **/etc/default/grub:**
  - add => ipv6.disable=1 to GRUB_CMDLINE_LINUX
  - GRUB_CMDLINE_LINUX="ipv6.disable=1"
  - update-grub
  - apt-get install tcpd
  - #echo "ALL: <net>/<mask>, <net>/<mask>, ..." >/etc/hosts.allow
  - echo "ALL: ALL" >> /etc/hosts.deny
  - chown root:root /etc/hosts.allow
  - chmod 644 /etc/hosts.allow
  - chown root:root /etc/hosts.deny
  - chmod 644 /etc/hosts.deny
  - /etc/modprobe.d/CIS.conf:
  - install dccp /bin/true
  - install sctp /bin/true
  - install rds /bin/true

    - install tipc /bin/true
    - apt-get install iptables
    - iptables -F
    - iptables -P INPUT DROP
    - iptables -P OUTPUT DROP
    - iptables -P FORWARD DROP
    - iptables -A INPUT -i lo -j ACCEPT
    - iptables -A OUTPUT -o lo -j ACCEPT
    - iptables -A INPUT -s 127.0.0.0/8 -j DROP
    - iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
    - iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
    - iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
    - iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
    - iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
    - iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
    - ####iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
    - ####ip link set <interface> down

- **/etc/audit/auditd.conf:**
    - max_log_file = 100000000000
    - space_left_action = email
    - action_mail_acct = root
    - admin_space_left_action = halt
    - max_log_file_action = keep_logs
    - systemctl enable auditd
    - /etc/default/grub:
    - add => GRUB_CMDLINE_LINUX="audit=1"
    - update-grub
- **/etc/audit/audit.rules:**
    - if 32:
    - -a always,exit -F arch=b32-S adjtimex -S settimeofday -S stime -k time-change
    - -a always,exit -F arch=b32 -S clock_settime -k time-change
    - -w /etc/localtime -p wa -k time-change
    - if 64:
    - -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
    - -a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
    - -a always,exit -F arch=b64 -S clock_settime -k time-change
    - -a always,exit -F arch=b32 -S clock_settime -k time-change

- -w /etc/localtime -p wa -k time-change

- -w /etc/group -p wa -k identity
- -w /etc/passwd -p wa -k identity
- -w /etc/gshadow -p wa -k identity
- -w /etc/shadow -p wa -k identity
- -w /etc/security/opasswd -p wa -k identity

- if 32:
- -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
- -w /etc/issue -p wa -k system-locale
- -w /etc/issue.net -p wa -k system-locale
- -w /etc/hosts -p wa -k system-locale
- -w /etc/sysconfig/network -p wa -k system-locale

- if 64:
- -a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
- -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale
- -w /etc/issue -p wa -k system-locale
- -w /etc/issue.net -p wa -k system-locale
- -w /etc/hosts -p wa -k system-locale
- -w /etc/sysconfig/network -p wa -k system-locale

- **SELinux:**
  - -w /etc/selinux/ -p wa -k MAC-policy
  - -w /usr/share/selinux/ -p wa -k MAC-policy
-
- **AppArmor:**
  - -w /etc/apparmor/ -pwa -k MAC-policy
  - -w /etc/apparmor.d/ -p wa -k MAC-policy

  - -w /var/log/faillog -p wa -k logins
  - -w /var/log/lastlog -p wa -k logins
  - -w /var/log/tallylog -p wa -k logins

  - -w /var/run/utmp -p wa -k session
  - -w /var/log/wtmp -p wa -k logins
  - -w /var/log/btmp -p wa -k logins

  - if 32:

- -a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b32 -S setxattr-S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

- if 64:
- -a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
- -a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

- if 32:
- -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
- -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

- if 64:
- -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
- -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
- -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
- -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

    - 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" }

- if 32:
- -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

- if 64:
- -a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
- -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

- if 32:
- -a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

- if 64:
- -a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete
- -a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete

- -w /etc/sudoers -p wa -k scope
- -w /etc/sudoers.d/ -p wa -k scope

- -w /var/log/sudo.log -p wa -k actions

- if 32:
- -w /sbin/insmod -p x -k modules
- -w /sbin/rmmod -p x -k modules
- -w /sbin/modprobe -p x -k modules
- -a always,exit -F arch=b32 -S init_module -S delete_module -k modules

- if 64:
- -w /sbin/insmod -p x -k modules
- -w /sbin/rmmod -p x -k modules
- -w /sbin/modprobe -p x -k modules
- -a always,exit -F arch=b64 -S init_module -S delete_module -k modules

- -e 2

- #### LOOOOGOOGOGOINGNGNG

- if rsyslog::::::::::::::
- systemctl enable rsyslog
- /etc/rsyslog.conf or /etc/rsyslog.d/*.conf:
- $FileCreateMode 0640
- if log host, if not comment out:
- $ModLoad imtcp
- $InputTCPServerRun 514
- edit as needed:
- *.* @@loghost.example.com
- *.emerg :omusrmsg:*
- mail.* -/var/log/mail
- mail.info -/var/log/mail.info
- mail.warning -/var/log/mail.warn
- mail.err /var/log/mail.err
- news.crit -/var/log/news/news.crit
- news.err -/var/log/news/news.err
- news.notice -/var/log/news/news.notice
- *.=warning;*.=err -/var/log/warn
- *.crit /var/log/warn
- *.*;mail.none;news.none -/var/log/messages
- local0,local1.* -/var/log/localmessages
- local2,local3.* -/var/log/localmessages
- local4,local5.* -/var/log/localmessages
- local6,local7.* -/var/log/localmessages
-
- pkill -HUP rsyslogd
-
-
- if syslog-ng::::::::::::::::::::
- update-rc.d syslog-ng enable
-
- /etc/syslog-ng/syslog-ng.conf:
- options { chain_hostnames(off); flush_lines(0); perm(0640); stats_freq(3600);threaded(yes); };
-
- if host:
- source net{ tcp(); };
- destination remote { file("/var/log/remote/${FULLHOST}-log"); };
- log { source(net); destination(remote); };
- else: remove
-
-
- if needs to send to destination:
- destination logserver { tcp("logfile.example.com" port(514)); };

- log { source(src); destination(logserver); }
- configure as appropriate:
- log { source(src); source(chroots); filter(f_console); destination(console); };
- log { source(src); source(chroots); filter(f_console); destination(xconsole); };
- log { source(src); source(chroots); filter(f_newscrit); destination(newscrit); };
- log { source(src); source(chroots); filter(f_newserr); destination(newserr); };
- log { source(src); source(chroots); filter(f_newsnotice); destination(newsnotice); };
- log { source(src); source(chroots); filter(f_mailinfo); destination(mailinfo); };
- log { source(src); source(chroots); filter(f_mailwarn); destination(mailwarn); };
- log { source(src); source(chroots); filter(f_mailerr); destination(mailerr); };
-
- log { source(src); source(chroots); filter(f_mail); destination(mail); };
- log { source(src); source(chroots); filter(f_acpid); destination(acpid); flags(final); };
- log { source(src); source(chroots); filter(f_acpid_full); destination(devnull); flags(final); };
- log { source(src); source(chroots); filter(f_acpid_old); destination(acpid); flags(final); };
- log { source(src); source(chroots); filter(f_netmgm); destination(netmgm); flags(final); };
- log { source(src); source(chroots); filter(f_local); destination(localmessages); };
- log { source(src); source(chroots); filter(f_messages); destination(messages); };
- log { source(src); source(chroots); filter(f_iptables); destination(firewall); };
- log { source(src); source(chroots); filter(f_warn); destination(warn); };
-
- pkill -HUP syslog-ng
-
- apt-get install rsyslog
- apt-get install syslog-ng
-
- chmod -R g-wx,o-rwx /var/log/*
-
- /etc/logrotate.conf => make sure logs rotate set maxage to longer than should remain on system
-
-
-
-
- systemctl enable cron
- 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
- rm /etc/cron.deny
- 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
-
-
-
- systemctl reload auditd
-
-
-
-
-
-
- dpkg --verify > <filename> > correct discripancies found and return the audit until output is clean or rist is mitigated or accepted
- Code MeaningS File size differs.M File mode differs (includes permissions and file type).
- 5 The MD5 checksum differs.
- D The major and minor version numbers differ on a device file.
- L A mismatch occurs in a link.
- U The file ownership differs.
- G The file group owner differs.
- T The file time (mtime) differs.
-
- apt list --installed | cut -d/ -f1 | dpkg --verify