Week 4 Homework Submission File: Linux Systems Administration

Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on /etc/shadow should allow only root read and write access.
    - Command to inspect permissions:

        ls -l /etc/shadow

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 2888 May 14 16:31 /etc/shadow
sysadmin@UbuntuDesktop:~$
```

    - Command to set permissions (if needed):

        Chmod 600 /etc/shadow

```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/shadow
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ ls -l /etc/shadow
-rw------- 1 root shadow 2888 May 14 16:31 /etc/shadow
```

2. Permissions on /etc/gshadow should allow only root read and write access.
    - Command to inspect permissions:

        ls -l /etc/gshadow

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw-r----- 1 root shadow 1076 May 14 16:31 /etc/gshadow
sysadmin@UbuntuDesktop:~$
```

    - Command to set permissions (if needed):

        Chmod 600 /etc/shadow

```
sysadmin@UbuntuDesktop:~$ sudo chmod 600 /etc/gshadow
sysadmin@UbuntuDesktop:~$ ls -l /etc/gshadow
-rw------- 1 root shadow 1076 May 14 16:31 /etc/gshadow
sysadmin@UbuntuDesktop:~$
```

3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
    - Command to inspect permissions:

      Ls -l /etc/group

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/group
-rw-r--r-- 1 root root 1303 May 14 16:31 /etc/group
sysadmin@UbuntuDesktop:~$
```

    - Command to set permissions (if needed):

4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
    - Command to inspect permissions:

      Ls -l /etc/passwd

```
sysadmin@UbuntuDesktop:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 3214 May 14 16:31 /etc/passwd
sysadmin@UbuntuDesktop:~$
```

    - Command to set permissions (if needed):

Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin.
    - Command to add each user account (include all five users):

Sudo adduser sam

Sudo adduser joe

Sudo adduser amy

Sudo adduser sara

Sudo adduser admin

```
sysadmin@UbuntuDesktop:~$ sudo adduser sara
```

2. Ensure that only the admin has general sudo access.
    - Command to add admin to the sudo group:

```
sysadmin@UbuntuDesktop:~$ sudo usermod -aG sudo admin
sysadmin@UbuntuDesktop:~$ groups admin
admin : admin sudo
```

Usermod -aG (a => append, G => groups)

Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.
    - Command to add group:

```
sysadmin@UbuntuDesktop:~$ sudo addgroup engineers
[sudo] password for sysadmin:
Adding group `engineers' (GID 1020) ...
Done.
```

2. Add users sam, joe, amy, and sara to the managed group.
    - Command to add users to engineers group (include all four users):

```
sysadmin@UbuntuDesktop:~$ sudo usermod -aG engineers sam
sysadmin@UbuntuDesktop:~$ groups sam
sam : sam engineers
sysadmin@UbuntuDesktop:~$ sudo usermod -aG engineers joe
sysadmin@UbuntuDesktop:~$ sudo usermod -aG engineers amy
sysadmin@UbuntuDesktop:~$ sudo usermod -aG engineers sara
sysadmin@UbuntuDesktop:~$ groups joe
joe : joe engineers
sysadmin@UbuntuDesktop:~$ groups amy
amy : amy engineers
sysadmin@UbuntuDesktop:~$ groups sara
sara : sara engineers
sysadmin@UbuntuDesktop:~$
```

3. Create a shared folder for this group at /home/engineers.
    - Command to create the shared folder:

```
sysadmin@UbuntuDesktop:~$ sudo mkdir -p /home/engineers
sysadmin@UbuntuDesktop:~$ ls -l /home/engineers/
total 0
```

4. Change ownership on the new engineers' shared folder to the engineers group.
    - Command to change ownership of engineer's shared folder to engineer group:

```
sysadmin@UbuntuDesktop:~$ sudo chgrp engineers /home/engineers/
sysadmin@UbuntuDesktop:~$ ls -l /home/engineers/
total 0
```

Step 4: Lynis Auditing

1. Command to install Lynis:

```
sysadmin@UbuntuDesktop:~$ sudo apt-get install lynis
[sudo] password for sysadmin:
Sorry, try again.
[sudo] password for sysadmin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
lynis is already the newest version (2.6.2-1).
The following packages were automatically installed and are no longer required:
  fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0 gir1.2-geocodeglib-1.0
  gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0
  gir1.2-unity-5.0 grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1
  libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1
  libetonyek-0.1-1 libevent-2.1-6 libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgee-0.8-2
  libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1
  liblirc-client0 libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1 libqqwing2v5 libraw16
  librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2
  libxmlsec1 libxmlsec1-nss lp-solve media-player-info python3-debconf python3-debian python3-mako
  python3-markupsafe syslinux syslinux-common syslinux-legacy update-notifier-common
  usb-creator-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 391 not upgraded.
sysadmin@UbuntuDesktop:~$
```

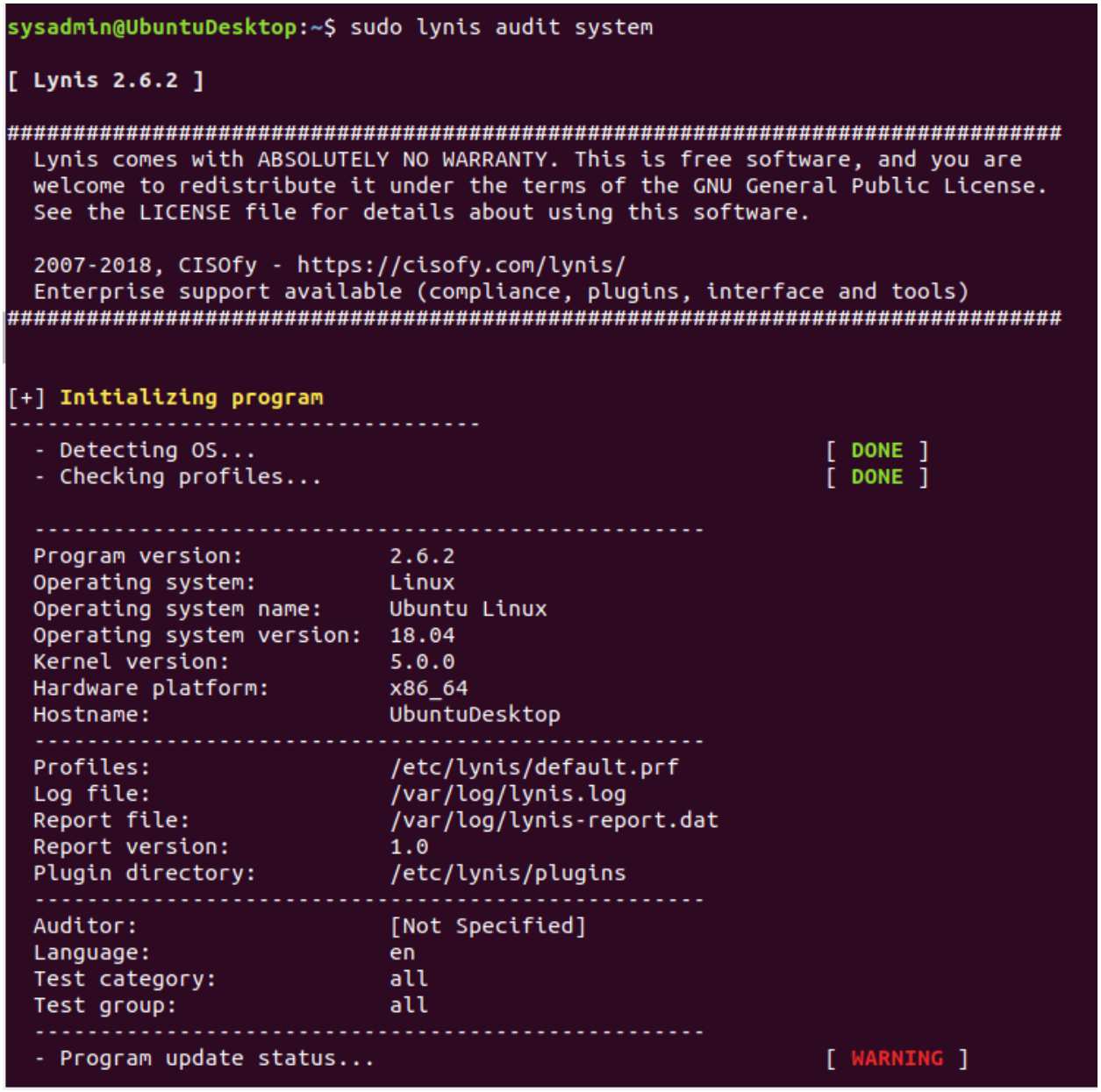
2. Command to see documentation and instructions:

    Man lynis

3. Command to run an audit:

Sudo lynis audit system

4. Provide a report from the Lynis output on what can be done to harden the system.
    - Screenshot of report output:



```
      ================================================================================
        Lynis update available
      ================================================================================

        Current version is more than 4 months old

        Current version : 262   Latest version : 306

        Please update to the latest version.
        New releases include additional features, bug fixes, tests, and baselines.

        Download the latest version:

        Packages (DEB/RPM) -  https://packages.cisofy.com
        Website (TAR)      -  https://cisofy.com/downloads/
        GitHub (source)    -  https://github.com/CISOfy/lynis

      ================================================================================


[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                    [ FOUND ]
    - Checking /sbin...                                   [ FOUND ]
    - Checking /usr/bin...                                [ FOUND ]
    - Checking /usr/sbin...                               [ FOUND ]
    - Checking /usr/local/bin...                          [ FOUND ]
    - Checking /usr/local/sbin...                         [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                     [ Not Installed ]
      - libpam-usb                                        [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                        [ Not Installed ]
    - apt-listchanges                                     [ Not Installed ]
    - checkrestart                                        [ Not Installed ]
```

```
    - needrestart                                          [ Not Installed ]
    - debsecan                                             [ Not Installed ]
    - debsums                                              [ Not Installed ]
    - fail2ban                                             [ Not Installed ]
]

[+] Boot and services
------------------------------------
  - Service Manager                                        [ systemd ]
  - Checking UEFI boot                                     [ DISABLED ]
  - Checking presence GRUB2                                [ FOUND ]
    - Checking for password protection                     [ WARNING ]
  - Check running services (systemctl)                     [ DONE ]
        Result: found 42 running services
  - Check enabled services at boot (systemctl)             [ DONE ]
        Result: found 67 enabled services
  - Check startup files (permissions)                      [ OK ]

[+] Kernel
------------------------------------
  - Checking default run level                             [ RUNLEVEL 5 ]
  - Checking CPU support (NX/PAE)
    CPU support: PAE and/or NoeXecute supported            [ FOUND ]
  - Checking kernel version and release                    [ DONE ]
  - Checking kernel type                                   [ DONE ]
  - Checking loaded kernel modules                         [ DONE ]
      Found 105 active modules
  - Checking Linux kernel configuration file               [ FOUND ]
  - Checking default I/O kernel scheduler                  [ NOT FOUND ]
  - Checking for available kernel update                   [ OK ]
  - Checking core dumps configuration                      [ DISABLED ]
    - Checking setuid core dumps configuration             [ PROTECTED ]
  - Check if reboot is needed                              [ NO ]

[+] Memory and Processes
------------------------------------
  - Checking /proc/meminfo                                 [ FOUND ]
  - Searching for dead/zombie processes                    [ OK ]
  - Searching for IO waiting processes                     [ OK ]

[+] Users, Groups and Authentication
------------------------------------
  - Administrator accounts                                 [ WARNING ]
  - Unique UIDs                                            [ WARNING ]
  - Consistency of group files (grpck)                     [ OK ]
  - Unique group IDs                                       [ OK ]
  - Unique group names                                     [ OK ]
  - Password file consistency                              [ SUGGESTION ]
  - Query system users (non daemons)                       [ DONE ]
  - NIS+ authentication support                            [ NOT ENABLED ]
```

```
  - Query system users (non daemons)                              [ DONE ]
  - NIS+ authentication support                                   [ NOT ENABLED ]
  - NIS authentication support                                    [ NOT ENABLED ]
  - sudoers file                                                  [ FOUND ]
    - Check sudoers file permissions                              [ OK ]
  - PAM password strength tools                                   [ SUGGESTION ]
  - PAM configuration files (pam.conf)                            [ FOUND ]
  - PAM configuration files (pam.d)                               [ FOUND ]
  - PAM modules                                                   [ FOUND ]
  - LDAP module in PAM                                            [ NOT FOUND ]
  - Accounts without expire date                                  [ OK ]
  - Accounts without password                                     [ OK ]
  - Checking user password aging (minimum)                        [ DISABLED ]
  - User password aging (maximum)                                 [ DISABLED ]
  - Checking expired passwords                                    [ OK ]
  - Checking Linux single user mode authentication                [ WARNING ]
  - Determining default umask
    - umask (/etc/profile)                                        [ NOT FOUND ]
    - umask (/etc/login.defs)                                     [ SUGGESTION ]
  - LDAP authentication support                                   [ NOT ENABLED ]
  - Logging failed login attempts                                 [ ENABLED ]

[+] Shells
------------------------------------
  - Checking shells from /etc/shells
    Result: found 4 shells (valid shells: 4).
    - Session timeout settings/tools                              [ NONE ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc                  [ NONE ]
    - Checking default umask in /etc/profile                      [ NONE ]

[+] File systems
------------------------------------
  - Checking mount points
    - Checking /home mount point                                  [ SUGGESTION ]
    - Checking /tmp mount point                                   [ SUGGESTION ]
    - Checking /var mount point                                   [ SUGGESTION ]
  - Query swap partitions (fstab)                                 [ OK ]
  - Testing swap partitions                                       [ OK ]
  - Checking for old files in /tmp                                [ OK ]
  - Checking /tmp sticky bit                                      [ OK ]
  - Checking /var/tmp sticky bit                                  [ OK ]
  - ACL support root file system                                  [ ENABLED ]
  - Mount options of /                                            [ NON DEFAULT ]
  - Checking Locate database                                      [ FOUND ]
  - Disable kernel support of some filesystems
    - Discovered kernel modules: cramfs freevxfs hfs hfsplus jffs2 udf

[+] USB Devices
------------------------------------
```

```
[+] USB Devices
------------------------------------
  - Checking usb-storage driver (modprobe config)            [ NOT DISABLED ]
  - Checking USB devices authorization                       [ ENABLED ]
  - Checking USBGuard                                        [ NOT FOUND ]

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)          [ DISABLED ]

[+] NFS
------------------------------------
  - Check running NFS daemon                                 [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                  [ FOUND ]
  - Searching DNS domain name                                [ UNKNOWN ]
  - Checking /etc/hosts
    - Checking /etc/hosts (duplicates)                       [ OK ]
    - Checking /etc/hosts (hostname)                         [ OK ]
    - Checking /etc/hosts (localhost)                        [ OK ]
    - Checking /etc/hosts (localhost to IP)                  [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                         [ FOUND ]
      - Querying package manager
    - Query unpurged packages                                [ FOUND ]
  - Checking security repository in sources.list file        [ OK ]
  - Checking APT package database                            [ OK ]
  - Checking vulnerable packages                             [ WARNING ]
  - Checking upgradeable packages                            [ SKIPPED ]
  - Checking package audit tool                              [ INSTALLED ]
    Found: apt-get

[+] Networking
------------------------------------
  - Checking IPv6 configuration                              [ ENABLED ]
      Configuration method                                   [ AUTO ]
      IPv6 only                                              [ NO ]
  - Checking configured nameservers
    - Testing nameservers
        Nameserver: 8.8.8.8                                  [ OK ]
        Nameserver: 127.0.0.53                               [ OK ]
    - Minimal of 2 responsive nameservers                    [ OK ]
  - Checking default gateway                                 [ DONE ]
  - Getting listening ports (TCP/UDP)                        [ DONE ]
```

```
  - Checking promiscuous interfaces                          [ OK ]
  - Checking waiting connections                             [ OK ]
  - Checking status DHCP client                              [ RUNNING ]
  - Checking for ARP monitoring software                     [ NOT FOUND ]

[+] Printers and Spools
-----------------------------------
  - Checking cups daemon                                     [ RUNNING ]
  - Checking CUPS configuration file                         [ OK ]
    - File permissions                                       [ WARNING ]
  - Checking CUPS addresses/sockets                          [ FOUND ]
  - Checking lp daemon                                       [ NOT RUNNING ]

[+] Software: e-mail and messaging
-----------------------------------
  - Postfix status                                           [ RUNNING ]
    - Postfix configuration                                  [ FOUND ]
      - Postfix banner                                       [ WARNING ]
  - Dovecot status                                           [ RUNNING ]

[+] Software: firewalls
-----------------------------------
  - Checking iptables kernel module                          [ FOUND ]
    - Checking iptables policies of chains                   [ FOUND ]
      - Checking chain INPUT (table: filter, policy )        [ other ]
    - Checking for empty ruleset                             [ OK ]
    - Checking for unused rules                              [ FOUND ]
  - Checking host based firewall                             [ ACTIVE ]

[+] Software: webserver
-----------------------------------
  - Checking Apache (binary /usr/sbin/apache2)               [ FOUND ]
      Info: Configuration file found (/etc/apache2/apache2.conf)
      Info: No virtual hosts found
    * Loadable modules                                       [ FOUND (114) ]
        - Found 114 loadable modules
          mod_evasive: anti-DoS/brute force                  [ NOT FOUND ]
          mod_reqtimeout/mod_qos                             [ FOUND ]
          ModSecurity: web application firewall              [ NOT FOUND ]
  - Checking nginx                                           [ NOT FOUND ]

[+] SSH Support
-----------------------------------
  - Checking running SSH daemon                              [ FOUND ]
    - Searching SSH configuration                            [ FOUND ]
    - SSH option: AllowTcpForwarding                         [ SUGGESTION ]
    - SSH option: ClientAliveCountMax                        [ SUGGESTION ]
    - SSH option: ClientAliveInterval                        [ OK ]
    - SSH option: Compression                                [ SUGGESTION ]
```

```
    - SSH option: ClientAliveInterval                    [ OK ]
    - SSH option: Compression                            [ SUGGESTION ]
    - SSH option: FingerprintHash                        [ OK ]
    - SSH option: GatewayPorts                           [ OK ]
    - SSH option: IgnoreRhosts                           [ OK ]
    - SSH option: LoginGraceTime                         [ OK ]
    - SSH option: LogLevel                               [ SUGGESTION ]
    - SSH option: MaxAuthTries                           [ SUGGESTION ]
    - SSH option: MaxSessions                            [ SUGGESTION ]
    - SSH option: PermitRootLogin                        [ SUGGESTION ]
    - SSH option: PermitUserEnvironment                  [ OK ]
    - SSH option: PermitTunnel                           [ OK ]
    - SSH option: Port                                   [ SUGGESTION ]
    - SSH option: PrintLastLog                           [ OK ]
    - SSH option: Protocol                               [ NOT FOUND ]
    - SSH option: StrictModes                            [ OK ]
    - SSH option: TCPKeepAlive                           [ SUGGESTION ]
    - SSH option: UseDNS                                 [ OK ]
    - SSH option: UsePrivilegeSeparation                 [ NOT FOUND ]
    - SSH option: VerifyReverseMapping                   [ NOT FOUND ]
    - SSH option: X11Forwarding                          [ SUGGESTION ]
    - SSH option: AllowAgentForwarding                   [ SUGGESTION ]
    - SSH option: AllowUsers                             [ NOT FOUND ]
    - SSH option: AllowGroups                            [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                         [ NOT FOUND ]

[+] Databases
------------------------------------
    No database engines found

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                           [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                         [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                        [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                    [ OK ]
    - Checking Syslog-NG status                          [ NOT FOUND ]
```

```
[+] Squid Support
------------------------------------
  - Checking running Squid daemon                          [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                      [ OK ]
    - Checking Syslog-NG status                            [ NOT FOUND ]
    - Checking systemd journal status                      [ FOUND ]
    - Checking Metalog status                              [ NOT FOUND ]
    - Checking RSyslog status                              [ FOUND ]
    - Checking RFC 3195 daemon status                      [ NOT FOUND ]
    - Checking minilogd instances                          [ NOT FOUND ]
  - Checking logrotate presence                            [ OK ]
  - Checking log directories (static list)                 [ DONE ]
  - Checking open log files                                [ DONE ]
  - Checking deleted files in use                          [ FILES FOUND ]

[+] Insecure services
------------------------------------
  - Checking inetd status                                  [ NOT ACTIVE ]

[+] Banners and identification
------------------------------------
  - /etc/issue                                             [ FOUND ]
    - /etc/issue contents                                  [ WEAK ]
  - /etc/issue.net                                         [ FOUND ]
    - /etc/issue.net contents                              [ WEAK ]

[+] Scheduled tasks
------------------------------------
  - Checking crontab/cronjob                               [ DONE ]

[+] Accounting
------------------------------------
  - Checking accounting information                        [ NOT FOUND ]
  - Checking sysstat accounting data                       [ NOT FOUND ]
  - Checking auditd                                        [ NOT FOUND ]

[+] Time and Synchronization
------------------------------------

[+] Cryptography
------------------------------------
  - Checking for expired SSL certificates [0/4]            [ NONE ]

[+] Virtualization
------------------------------------
```

```
[+] Containers
------------------------------------
    - Docker
      - Docker daemon                                    [ RUNNING ]
        - Docker info output (warnings)                  [ 1 ]
      - Containers
        - Total containers                               [ 0 ]
    - File permissions                                   [ OK ]

[+] Security frameworks
------------------------------------
  - Checking presence AppArmor                           [ FOUND ]
    - Checking AppArmor status                           [ ENABLED ]
  - Checking presence SELinux                            [ NOT FOUND ]
  - Checking presence grsecurity                         [ NOT FOUND ]
  - Checking for implemented MAC framework               [ OK ]

[+] Software: file integrity
------------------------------------
  - Checking file integrity tools
    - Tripwire                                           [ FOUND ]
  - Checking presence integrity tool                     [ FOUND ]

[+] Software: System tooling
------------------------------------
  - Checking automation tooling
    - Ansible artifact                                   [ FOUND ]
  - Automation tooling                                   [ FOUND ]
  - Checking for IDS/IPS tooling                         [ NONE ]

[+] Software: Malware
------------------------------------
  - Checking chkrootkit                                  [ FOUND ]

[+] File Permissions
------------------------------------
  - Starting file permissions check

[+] Home directories
------------------------------------
  - Checking shell history files                         [ OK ]

[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - fs.protected_hardlinks (exp: 1)                    [ OK ]
    - fs.protected_symlinks (exp: 1)                     [ OK ]
    - fs.suid_dumpable (exp: 0)                          [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                      [ DIFFERENT ]
```

```
[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - fs.protected_hardlinks (exp: 1)                          [ OK ]
    - fs.protected_symlinks (exp: 1)                           [ OK ]
    - fs.suid_dumpable (exp: 0)                                [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                            [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                             [ OK ]
    - kernel.dmesg_restrict (exp: 1)                           [ DIFFERENT ]
    - kernel.kptr_restrict (exp: 2)                            [ DIFFERENT ]
    - kernel.randomize_va_space (exp: 2)                       [ OK ]
    - kernel.sysrq (exp: 0)                                    [ DIFFERENT ]
    - kernel.yama.ptrace_scope (exp: 1 2 3)                    [ OK ]
    - net.ipv4.conf.all.accept_redirects (exp: 0)              [ OK ]
    - net.ipv4.conf.all.accept_source_route (exp: 0)           [ OK ]
    - net.ipv4.conf.all.bootp_relay (exp: 0)                   [ OK ]
    - net.ipv4.conf.all.forwarding (exp: 0)                    [ DIFFERENT ]
    - net.ipv4.conf.all.log_martians (exp: 1)                  [ DIFFERENT ]
    - net.ipv4.conf.all.mc_forwarding (exp: 0)                 [ OK ]
    - net.ipv4.conf.all.proxy_arp (exp: 0)                     [ OK ]
    - net.ipv4.conf.all.rp_filter (exp: 1)                     [ OK ]
    - net.ipv4.conf.all.send_redirects (exp: 0)                [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)          [ DIFFERENT ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)       [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)              [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)            [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)      [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                         [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                       [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)              [ DIFFERENT ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)           [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)          [ DIFFERENT ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)       [ OK ]

[+] Hardening
------------------------------------
    - Installed compiler(s)                                    [ FOUND ]
    - Installed malware scanner                                [ FOUND ]

[+] Custom Tests
------------------------------------
  - Running custom tests...                                    [ NONE ]

[+] Plugins (phase 2)
------------------------------------
```

```
-[ Lynis 2.6.2 Results ]-

Warnings (6):
----------------------------
! Version of Lynis is very old and should be updated [LYNIS]
    https://cisofy.com/controls/LYNIS/

! Multiple users with UID 0 found in passwd file [AUTH-9204]
    https://cisofy.com/controls/AUTH-9204/

! Multiple accounts found with same UID [AUTH-9208]
    https://cisofy.com/controls/AUTH-9208/

! No password set for single mode [AUTH-9308]
    https://cisofy.com/controls/AUTH-9308/

! Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

! Found some information disclosure in SMTP banner (OS or software name) [MAIL-8818]
    https://cisofy.com/controls/MAIL-8818/

Suggestions (52):
----------------------------
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [CUST-0280]
    https://your-domain.example.org/controls/CUST-0280/

* Install libpam-usb to enable multi-factor authentication for PAM sessions [CUST-0285]
    https://your-domain.example.org/controls/CUST-0285/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [CUST-0810]
    https://your-domain.example.org/controls/CUST-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [CUST-0811]
    https://your-domain.example.org/controls/CUST-0811/

* Install debian-goodies so that you can run checkrestart after upgrades to determine which services are using old versions of l
ibraries and need restarting. [CUST-0830]
    https://your-domain.example.org/controls/CUST-0830/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemon
s are using old versions of libraries and need restarting. [CUST-0831]
    https://your-domain.example.org/controls/CUST-0831/

* Install debsecan to generate lists of vulnerabilities which affect this installation. [CUST-0870]
    https://your-domain.example.org/controls/CUST-0870/

* Install debsums for the verification of installed package files against MD5 checksums. [CUST-0875]
```

```
  * Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
      https://cisofy.com/controls/DEB-0880/

  * Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOO
T-5122]
      https://cisofy.com/controls/BOOT-5122/

  * Run pwck manually and correct any errors in the password file [AUTH-9228]
      https://cisofy.com/controls/AUTH-9228/

  * Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
      https://cisofy.com/controls/AUTH-9262/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/controls/AUTH-9286/

  * Set password for single user mode to minimize physical access attack surface [AUTH-9308]
      https://cisofy.com/controls/AUTH-9308/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separated partition [FILE-6310]
      https://cisofy.com/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separated partition [FILE-6310]
      https://cisofy.com/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separated partition [FILE-6310]
      https://cisofy.com/controls/FILE-6310/

  * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [STRG-1840]
      https://cisofy.com/controls/STRG-1840/

  * Check DNS configuration for the dns domain name [NAME-4028]
      https://cisofy.com/controls/NAME-4028/

  * Purge old/removed packages (1 found) with aptitude purge or dpkg --purge command. This will cleanup old configuration files, c
ron jobs and startup scripts. [PKGS-7346]
      https://cisofy.com/controls/PKGS-7346/

  * Install debsums utility for the verification of packages with known good database. [PKGS-7370]
      https://cisofy.com/controls/PKGS-7370/

  * Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]
      https://cisofy.com/controls/PKGS-7392/
```

```
 * Install package apt-show-versions for patch management purposes [PKGS-7394]
     https://cisofy.com/controls/PKGS-7394/

 * Consider running ARP monitoring software (arpwatch,arpon) [NETW-3032]
     https://cisofy.com/controls/NETW-3032/

 * Access to CUPS configuration could be more strict. [PRNT-2307]
     https://cisofy.com/controls/PRNT-2307/

 * You are advised to hide the mail_name (option: smtpd_banner) from your postfix configuration. Use postconf -e or change your m
ain.cf file (/etc/postfix/main.cf) [MAIL-8818]
     https://cisofy.com/controls/MAIL-8818/

 * Disable the 'VRFY' command [MAIL-8820:disable_vrfy_command]
   - Details  : disable_vrfy_command=no
   - Solution : run postconf -e disable_vrfy_command=yes to change the value
     https://cisofy.com/controls/MAIL-8820/

 * Check iptables rules to see which rules are currently not used [FIRE-4513]
     https://cisofy.com/controls/FIRE-4513/

 * Install Apache mod_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]
     https://cisofy.com/controls/HTTP-6640/

 * Install Apache modsecurity to guard webserver against web application attacks [HTTP-6643]
     https://cisofy.com/controls/HTTP-6643/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : AllowTcpForwarding (YES --> NO)
     https://cisofy.com/controls/SSH-7408/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : ClientAliveCountMax (3 --> 2)
     https://cisofy.com/controls/SSH-7408/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : Compression (YES --> (DELAYED|NO))
     https://cisofy.com/controls/SSH-7408/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : LogLevel (INFO --> VERBOSE)
     https://cisofy.com/controls/SSH-7408/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : MaxAuthTries (6 --> 2)
     https://cisofy.com/controls/SSH-7408/

 * Consider hardening SSH configuration [SSH-7408]
   - Details  : MaxSessions (10 --> 2)
     https://cisofy.com/controls/SSH-7408/
```

```
  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (YES --> NO)
      https://cisofy.com/controls/SSH-7408/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/controls/LOGG-2190/

  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/controls/ACCT-9622/

  * Enable sysstat to collect accounting (no results) [ACCT-9626]
      https://cisofy.com/controls/ACCT-9626/

  * Enable auditd to collect audit information [ACCT-9628]
      https://cisofy.com/controls/ACCT-9628/

  * Run 'docker info' to see warnings applicable to Docker daemon [CONT-8104]
      https://cisofy.com/controls/CONT-8104/

  * One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
    - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
      https://cisofy.com/controls/KRNL-6000/

  * Harden compilers like restricting access to root user only [HRDN-7222]
      https://cisofy.com/controls/HRDN-7222/

  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 232
  Plugins enabled : 1
```

```
  Follow-up:
  ---------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

================================================================================

  Lynis security scan details:

  Hardening index : 56 [###########         ]
  Tests performed : 232
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [V]

  Lynis Modules:
  - Compliance Status      [?]
  - Security Audit         [V]
  - Vulnerability Scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

================================================================================
  Notice: Lynis update available
  Current version : 262    Latest version : 306
================================================================================

  Lynis 2.6.2

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

  2007-2018, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)

================================================================================

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

sysadmin@UbuntuDesktop:~$
```

Bonus

1. Command to install chkrootkit:

   Sudo apt-get install chkrootkit

```
sysadmin@UbuntuDesktop:~$ sudo apt-get install chkrootkit -y
[sudo] password for sysadmin:
Reading package lists... Done
Building dependency tree
Reading state information... Done
chkrootkit is already the newest version (0.52-1ubuntu0.1).
The following packages were automatically installed and are no longer required:
  fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0 gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0
  gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0 gir1.2-unity-5.0 grilo-plugins-0.3-base gstreamer1.0-gtk3
  libboost-date-time1.65.1 libboost-locale1.65.1 libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6
  libexiv2-14 libfreerdp-client2-2 libfreerdp2-2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4
  liblangtag-common liblangtag1 liblirc-client0 libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1 libqqwing2v5 libraw16
  librevenge-0.0-0 libsgutils2-2 libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxmlsec1 libxmlsec1-nss lp-solve
  media-player-info python3-debconf python3-debian python3-mako python3-markupsafe syslinux syslinux-common syslinux-legacy
  update-notifier-common usb-creator-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 483 not upgraded.
sysadmin@UbuntuDesktop:~$
```

2. Command to see documentation and instructions:

   man chkrootkit

```
chkrootkit(1)                                General Commands Manual                                chkrootkit(1)

NAME
       chkrootkit - Determine whether the system is infected with a rootkit

SYNOPSIS
       chkrootkit [OPTION]... [TESTNAME]...

DESCRIPTION
       chkrootkit  examines  certain  elements  of the target system and determines whether they have been tampered with. Some
       tools which chkrootkit applies while analyzing binaries and log files can be found at /usr/lib/chkrootkit.

OPTIONS
       -h     Print a short help message and exit.

       -V     Print version information and exit.

       -l     Print available tests.

       -d     Enter debug mode.

       -x     Enter expert mode.

       -e     Exclude known false positive files/dirs, quoted, space separated.

       -q     Enter quiet mode.

       -r dir Use dir as the root directory.

       -p dir1:dir2:dirN
              Specify the path for the external commands used by chkrootkit.

       -n     skip NFS mounted dirs

AUTHOR
       Manual page written by Yotam Rubin  <yotam@makif.omer.k12.il>  and  lantz  moore  <lmoore@debian.org>  for  the  Debian
       project. It may be used by others.

SEE ALSO
       strings(1)

                                                    10 January 2003                                chkrootkit(1)
```

3. Command to run expert mode:

   chkrootkit -x

4. Provide a report from the chrootkit output on what can be done to harden the system.
   - Screenshot of end of sample output:

```
.eh_frame
.init_array
.fini_array
.jcr
.data.rel.ro
.dynamic
.data
.bss
.gnu_debuglink
###
### Output of: /usr/bin/strings -a /bin/vdir
###
/lib64/ld-linux-x86-64.so.2
i~a/T
libselinux.so.1
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
_init
fgetfilecon
freecon
lgetfilecon
_fini
libc.so.6
fflush
strcpy
gmtime_r
__printf_chk
fnmatch
readdir
setlocale
mbrtowc
strncmp
optind
strrchr
fflush_unlocked
dcgettext
stpncpy
getpwuid
closedir
getgrgid
error
signal
mbstowcs
sigprocmask
__stack_chk_fail
__lxstat
iswprint
realloc
```

```
strlen
ungetc
sigemptyset
memset
localeconv
__errno_location
memcmp
mempcpy
unsetenv
_setjmp
__fprintf_chk
sigaddset
getgrnam
wcswidth
stdout
lseek
memcpy
fclose
strtoul
malloc
timegm
raise
mbsinit
tzset
__uflow
nl_langinfo
opendir
__ctype_b_loc
getenv
_obstack_allocated_p
optarg
__freading
stderr
wcwidth
ioctl
_obstack_begin_1
_obstack_newchunk
__snprintf_chk
readlink
fscanf
getopt_long
__fxstat
fileno
gethostname
_obstack_memory_used
getcwd
fwrite
gettimeofday
sigaction
```

```
[]A\A]A^A_
dev_ino_pop
sort_files
posix-
main
?pcdb-lswd
# Configuration file for dircolors, a utility to help you set the
# LS_COLORS environment variable used by GNU ls with the --color option.
# Copyright (C) 1996-2017 Free Software Foundation, Inc.
# Copying and distribution of this file, with or without modification,
# are permitted provided the copyright notice and this notice are preserved.
# The keywords COLOR, OPTIONS, and EIGHTBIT (honored by the
# slackware version of dircolors) are recognized but ignored.
# Below are TERM entries, which can be a glob patterns, to match
# against the TERM environment variable to determine if it is colorizable.
TERM Eterm
TERM ansi
TERM *color*
TERM con[0-9]*x[0-9]*
TERM cons25
TERM console
TERM cygwin
TERM dtterm
TERM gnome
TERM hurd
TERM jfbterm
TERM konsole
TERM kterm
TERM linux
TERM linux-c
TERM mlterm
TERM putty
TERM rxvt*
TERM screen*
TERM st
TERM terminator
TERM tmux*
TERM vt100
TERM xterm*
# Below are the color init strings for the basic file types. A color init
# string consists of one or more of the following numeric codes:
# Attribute codes:
# 00=none 01=bold 04=underscore 05=blink 07=reverse 08=concealed
# Text color codes:
# 30=black 31=red 32=green 33=yellow 34=blue 35=magenta 36=cyan 37=white
# Background color codes:
# 40=black 41=red 42=green 43=yellow 44=blue 45=magenta 46=cyan 47=white
```

```
.xcf 01;35
.xwd 01;35
.yuv 01;35
.cgm 01;35
.emf 01;35
# https://wiki.xiph.org/MIME_Types_and_File_Extensions
.ogv 01;35
.ogx 01;35
# audio formats
.aac 00;36
.au 00;36
.flac 00;36
.m4a 00;36
.mid 00;36
.midi 00;36
.mka 00;36
.mp3 00;36
.mpc 00;36
.ogg 00;36
.ra 00;36
.wav 00;36
# https://wiki.xiph.org/MIME_Types_and_File_Extensions
.oga 00;36
.opus 00;36
.spx 00;36
.xspf 00;36
%.*s%s%s
%%%02x
src/ls.c
sort_type != sort_version
 %lu
%*lu
]8;;file://%s%s%s
]8;;
%s %*s
%*s, %*s
 ->
error canonicalizing %s
cannot access %s
cannot read symbolic link %s
unlabeled
cannot open directory %s
reading directory %s
closing directory %s
total
vdir
test invocation
Multi-call invocation
sha224sum
```

```
34;42
30;42
30;41
slash
long-iso
cannot determine device and inode of %s
%s: not listing already-listed directory
Try '%s --help' for more information.
Usage: %s [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.
Mandatory arguments to long options are mandatory for short options too.
  -a, --all                  do not ignore entries starting with .
  -A, --almost-all           do not list implied . and ..
      --author               with -l, print the author of each file
  -b, --escape               print C-style escapes for nongraphic characters
      --block-size=SIZE      scale sizes by SIZE before printing them; e.g.,
                               '--block-size=M' prints sizes in units of
                               1,048,576 bytes; see SIZE format below
  -B, --ignore-backups       do not list implied entries ending with ~
  -c                         with -lt: sort by, and show, ctime (time of last
                               modification of file status information);
                               with -l: show ctime and sort by name;
                               otherwise: sort by ctime, newest first
  -C                         list entries by columns
      --color[=WHEN]         colorize the output; WHEN can be 'always' (default
                               if omitted), 'auto', or 'never'; more info below
  -d, --directory            list directories themselves, not their contents
  -D, --dired                generate output designed for Emacs' dired mode
  -f                         do not sort, enable -aU, disable -ls --color
  -F, --classify             append indicator (one of */=>@|) to entries
      --file-type            likewise, except do not append '*'
      --format=WORD          across -x, commas -m, horizontal -x, long -l,
                               single-column -1, verbose -l, vertical -C
      --full-time            like -l --time-style=full-iso
  -g                         like -l, but do not list owner
      --group-directories-first
                             group directories before files;
                               can be augmented with a --sort option, but any
                               use of --sort=none (-U) disables grouping
  -G, --no-group             in a long listing, don't print group names
  -h, --human-readable       with -l and/or -s, print human readable sizes
                               (e.g., 1K 234M 2G)
      --si                   likewise, but use powers of 1000 not 1024
  -H, --dereference-command-line
                             follow symbolic links listed on the command line
      --dereference-command-line-symlink-to-dir
                             follow each command line symbolic link
                               that points to a directory
```

```
                           follow symbolic links listed on the command line
    --dereference-command-line-symlink-to-dir
                           follow each command line symbolic link
                             that points to a directory
    --hide=PATTERN         do not list implied entries matching shell PATTERN
                             (overridden by -a or -A)
    --hyperlink[=WHEN]     hyperlink file names; WHEN can be 'always'
                             (default if omitted), 'auto', or 'never'
    --indicator-style=WORD  append indicator with style WORD to entry names:
                             none (default), slash (-p),
                             file-type (--file-type), classify (-F)
-i, --inode                print the index number of each file
-I, --ignore=PATTERN       do not list implied entries matching shell PATTERN
-k, --kibibytes            default to 1024-byte blocks for disk usage
-l                         use a long listing format
-L, --dereference          when showing file information for a symbolic
                             link, show information for the file the link
                             references rather than for the link itself
-m                         fill width with a comma separated list of entries
-n, --numeric-uid-gid      like -l, but list numeric user and group IDs
-N, --literal              print entry names without quoting
-o                         like -l, but do not list group information
-p, --indicator-style=slash
                           append / indicator to directories
-q, --hide-control-chars   print ? instead of nongraphic characters
    --show-control-chars   show nongraphic characters as-is (the default,
                             unless program is 'ls' and output is a terminal)
-Q, --quote-name           enclose entry names in double quotes
    --quoting-style=WORD   use quoting style WORD for entry names:
                             literal, locale, shell, shell-always,
                             shell-escape, shell-escape-always, c, escape
-r, --reverse              reverse order while sorting
-R, --recursive            list subdirectories recursively
-s, --size                 print the allocated size of each file, in blocks
-S                         sort by file size, largest first
    --sort=WORD            sort by WORD instead of name: none (-U), size (-S),
                             time (-t), version (-v), extension (-X)
    --time=WORD            with -l, show time as WORD instead of default
                             modification time: atime or access or use (-u);
                             ctime or status (-c); also use specified time
                             as sort key if --sort=time (newest first)
    --time-style=STYLE     with -l, show times using style STYLE:
                             full-iso, long-iso, iso, locale, or +FORMAT;
                             FORMAT is interpreted like in 'date'; if FORMAT
                             is FORMAT1<newline>FORMAT2, then FORMAT1 applies
                             to non-recent files and FORMAT2 to recent files;
                             if STYLE is prefixed with 'posix-', STYLE
                             takes effect only outside the POSIX locale
-t                         sort by modification time, newest first
```

```
      --version  output version information and exit
The SIZE argument is an integer and optional unit (example: 10K is 10*1024).
Units are K,M,G,T,P,E,Z,Y (powers of 1024) or KB,MB,... (powers of 1000).
Using color to distinguish file types is disabled both by default and
with --color=never.  With --color=auto, ls emits color codes only when
standard output is connected to a terminal.  The LS_COLORS environment
variable can change the settings.  Use the dircolors command to set it.
Exit status:
 0  if OK,
 1  if minor problems (e.g., cannot access subdirectory),
 2  if serious trouble (e.g., cannot access command-line argument).
http://www.gnu.org/software/coreutils/
Report %s translation bugs to <http://translationproject.org/team/>
Full documentation at: <%s%s>
or available locally via: info '(coreutils) %s%s'
ignoring invalid value of environment variable QUOTING_STYLE: %s
ignoring invalid width in environment variable COLUMNS: %s
ignoring invalid tab size in environment variable TABSIZE: %s
abcdfghiklmnopqrstuvw:xABCDFGHI:LNQRST:UXZ1
  - +FORMAT (e.g., +%H:%M) for a 'date'-style format
dev_ino_size <= obstack_object_size (&dev_ino_obstack)
//DIRED-OPTIONS// --quoting-style=%s
hash_get_n_entries (active_dir_set) == 0
unparsable value for LS_COLORS environment variable
dereference-command-line-symlink-to-dir
8.28
invalid argument %s for %s
ambiguous argument %s for %s
Valid arguments are:
  - %s
, %s
write error
system.posix_acl_access
system.posix_acl_default
POSIX
# entries:         %lu
# buckets:         %lu
max bucket length: %lu
# buckets used:    %lu (%.2f%%)
=fff?
Y@%.0Lf
%.1Lf
BLOCKSIZE
POSIXLY_CORRECT
eEgGkKmMpPtTyYzZ0
KMGTPEZY
%m/%d/%y
%Y-%m-%d
```

```
###
### Output of: /bin/ls -l /bin/vdir
###
-rwxr-xr-x 1 root root 133792 Jan 18  2018 /bin/vdir
###
### Output of: /usr/bin/strings -a /usr/bin/w
###
/lib64/ld-linux-x86-64.so.2
libprocps.so.6
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
escape_command
Hertz
tty_to_dev
readproctab
print_uptime
libc.so.6
__printf_chk
setlocale
strncmp
optind
dcgettext
inet_ntop
strncpy
__stack_chk_fail
putchar
_exit
program_invocation_name
strftime
strtol
getpwnam
strlen
setutent
__errno_location
utmpname
__fprintf_chk
```

```
ip-addr
help
version
 -h, --no-header     do not print header
 -u, --no-current    ignore current process username
 -s, --short         short format
 -f, --from          show remote hostname field
 -o, --old-style     old style output
 -i, --ip-addr       display IP address instead of hostname (if possible)
     --help     display this help and exit
 -V, --version  output version information and exit
User length environment PROCPS_USERLEN must be between 8 and %i, ignoring.
from length environment PROCPS_FROMLEN must be between 8 and %d, ignoring
  LOGIN@   IDLE   JCPU   PCPU WHAT
Y@write error
;*3$"
036111656c28ceb57d787db8d2350fa783516e.debug
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.data.rel.ro
.dynamic
.data
.bss
.gnu_debuglink
###
### Output of: /bin/ls -l /usr/bin/w
###
lrwxrwxrwx 1 root root 19 Nov 12  2019 /usr/bin/w -> /etc/alternatives/w
###
### Output of: /usr/bin/strings -a /usr/bin/write
###
```

```
.fini_array
.dynamic
.data
.bss
.gnu_debuglink
###
### Output of: /bin/ls -l /usr/bin/write
###
lrwxrwxrwx 1 root root 23 Nov 12  2019 /usr/bin/write -> /etc/alternatives/write
###
### Output of: /usr/bin/find /dev -type f
###
###
### Output of: /usr/bin/find /var/run/.tmp
###
/usr/bin/find: ‘/var/run/.tmp’: No such file or directory
###
### Output of: /usr/bin/find /usr/man/man1/lib/.lib
###
/usr/bin/find: ‘/usr/man/man1/lib/.lib’: No such file or directory
###
### Output of: /usr/bin/find /usr/man/man2/.man8
###
/usr/bin/find: ‘/usr/man/man2/.man8’: No such file or directory
###
### Output of: /usr/bin/find /usr/man/man1 -name '.. *'
###
/usr/bin/find: ‘/usr/man/man1’: No such file or directory
###
### Output of: /usr/bin/find /usr/share/locale/sk
###
/usr/share/locale/sk
/usr/share/locale/sk/LC_MESSAGES
/usr/share/locale/sk/LC_MESSAGES/debconf.mo
/usr/share/locale/sk/LC_MESSAGES/update-notifier.mo
/usr/share/locale/sk/LC_MESSAGES/xdg-user-dirs.mo
/usr/share/locale/sk/LC_MESSAGES/language-selector.mo
/usr/share/locale/sk/LC_MESSAGES/iso_3166-3.mo
/usr/share/locale/sk/LC_MESSAGES/iso_15924.mo
/usr/share/locale/sk/LC_MESSAGES/iso_3166-2.mo
/usr/share/locale/sk/LC_MESSAGES/iso_4217.mo
/usr/share/locale/sk/LC_MESSAGES/firewalld.mo
/usr/share/locale/sk/LC_MESSAGES/gettext-runtime.mo
/usr/share/locale/sk/LC_MESSAGES/libapt-pkg5.0.mo
/usr/share/locale/sk/LC_MESSAGES/xdg-desktop-portal.mo
/usr/share/locale/sk/LC_MESSAGES/iso_3166-1.mo
/usr/share/locale/sk/LC_MESSAGES/libapt-inst2.0.mo
/usr/share/locale/sk/LC_MESSAGES/gettext-tools.mo
/usr/share/locale/sk/LC_MESSAGES/iso_639.mo
```

```
/usr/share/locale/sk/LC_MESSAGES/menu-sections.mo
/usr/share/locale/sk/LC_MESSAGES/iso_3166.mo
/usr/share/locale/sk/LC_MESSAGES/iso_3166_2.mo
/usr/share/locale/sk/LC_MESSAGES/xdg-desktop-portal-gtk.mo
###
### Output of: /usr/bin/find /usr/lib/dy0
###
/usr/bin/find: ‘/usr/lib/dy0’: No such file or directory
###
### Output of: /usr/bin/find /tmp -name 982235016-gtkrc-429249277
###
###
### Output of: /usr/bin/find /var/spool/lp/admins/.lp/
###
/usr/bin/find: ‘/var/spool/lp/admins/.lp/’: No such file or directory
###
### Output of: /bin/ls /usr/bin/sourcemask 2> /dev/null
###
###
### Output of: /bin/ls /usr/bin/ras2xm 2> /dev/null
###
###
### Output of: /bin/ls /usr/sbin/in.telnet 2> /dev/null
###
###
### Output of: /bin/ls /sbin/vobiscum 2> /dev/null
###
###
### Output of: /bin/ls /usr/sbin/jcd 2> /dev/null
###
###
### Output of: /bin/ls /usr/sbin/atd2 2> /dev/null
###
###
### Output of: /bin/ls /usr/bin/.etc 2> /dev/null
###
###
### Output of: /bin/ls /usr/bin/xstat 2> /dev/null
###
###
### Output of: /bin/ls /etc/ld.so.hash 2> /dev/null
###
###
### Output of: /usr/bin/find /dev /usr /tmp     /lib /etc /var  -name tcp.log -o -name .linux-sniff -o -name sniff-l0g
-o -name core_ -o -wholename /usr/lib/in.httpd -o -wholename /usr/lib/in.pop3d
###
###
### Output of: /usr/bin/find /etc /sbin /usr/src/.puta /lib /usr/info -name ttyhash -o -name xlogin -o -name ldlib.tk -
o -name .t?rn
```

```
### Output of: /bin/netstat -an
###
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:52932         13.227.73.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:38346         142.250.188.4:443       TIME_WAIT
tcp        0      0 10.0.2.15:43634         142.250.141.154:443     ESTABLISHED
tcp        0      0 10.0.2.15:52928         13.227.73.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:58754         216.58.194.202:443      ESTABLISHED
tcp        0      0 10.0.2.15:39670         172.217.164.102:443     ESTABLISHED
tcp        0      0 10.0.2.15:35412         45.33.32.156:80         ESTABLISHED
tcp     1385      0 127.0.0.1:56060         127.0.1.1:139           CLOSE_WAIT
tcp        0      0 10.0.2.15:57422         172.217.164.98:443      ESTABLISHED
tcp        0      0 10.0.2.15:48356         172.217.5.98:443        ESTABLISHED
tcp        0      0 10.0.2.15:56678         23.215.102.32:443       TIME_WAIT
tcp        0      0 10.0.2.15:42350         54.208.141.248:443      ESTABLISHED
tcp        0      0 10.0.2.15:37204         34.120.5.221:443        TIME_WAIT
tcp        0      0 10.0.2.15:48488         172.217.5.98:443        ESTABLISHED
tcp        0      0 10.0.2.15:38130         74.125.203.94:443       ESTABLISHED
tcp        0      0 10.0.2.15:42354         54.208.141.248:443      TIME_WAIT
tcp        0      0 10.0.2.15:52926         13.227.73.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:34222         23.111.8.18:443         ESTABLISHED
tcp        0      0 10.0.2.15:58024         184.169.165.240:443     ESTABLISHED
tcp        0      0 10.0.2.15:41690         52.88.142.33:443        ESTABLISHED
tcp        0      0 10.0.2.15:37652         13.227.75.203:443       ESTABLISHED
tcp        0      0 10.0.2.15:39810         91.189.88.178:443       ESTABLISHED
tcp        0      0 10.0.2.15:40126         34.107.148.139:443      ESTABLISHED
tcp        0      0 10.0.2.15:36270         34.98.64.218:443        ESTABLISHED
tcp        0      0 10.0.2.15:35686         44.235.165.111:443      ESTABLISHED
tcp        0      0 10.0.2.15:58130         142.250.189.174:443     TIME_WAIT
tcp        0      1 10.0.2.15:43030         192.168.188.164:888     SYN_SENT
tcp        0      0 10.0.2.15:54840         147.75.38.124:443       TIME_WAIT
tcp        0      0 10.0.2.15:42114         142.250.189.161:443     ESTABLISHED
tcp        0      0 10.0.2.15:56292         151.101.26.132:443      TIME_WAIT
tcp        0      0 10.0.2.15:45558         44.235.148.11:443       ESTABLISHED
tcp        0      0 10.0.2.15:43996         8.39.36.144:443         TIME_WAIT
tcp        0      0 10.0.2.15:52958         13.227.73.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:48416         172.217.5.98:443        ESTABLISHED
```

```
tcp        0      0 10.0.2.15:55074         137.116.89.182:443      TIME_WAIT
tcp        0      0 10.0.2.15:54498         34.120.237.76:443       TIME_WAIT
tcp        0      0 10.0.2.15:42080         142.250.189.161:443     ESTABLISHED
tcp        0      0 10.0.2.15:34726         216.58.194.174:443      TIME_WAIT
tcp        0      0 10.0.2.15:50418         23.73.129.207:443       ESTABLISHED
tcp        0      0 10.0.2.15:60486         13.227.73.104:443       ESTABLISHED
tcp        0      0 10.0.2.15:49890         130.211.9.179:443       ESTABLISHED
tcp        0      0 10.0.2.15:54828         147.75.38.124:443       ESTABLISHED
tcp        0      0 10.0.2.15:44572         52.89.116.6:443         ESTABLISHED
tcp        0      0 10.0.2.15:43928         34.223.150.237:443      ESTABLISHED
tcp        0      0 10.0.2.15:44308         45.33.32.156:80         ESTABLISHED
tcp        0      0 10.0.2.15:56390         204.237.133.116:443     ESTABLISHED
tcp        0      0 127.0.0.1:56106         127.0.1.1:139           ESTABLISHED
tcp        0      0 10.0.2.15:52956         13.227.73.26:443        ESTABLISHED
tcp        0      0 10.0.2.15:39460         35.190.7.190:443        ESTABLISHED
tcp        0      0 10.0.2.15:58700         216.58.194.202:443      ESTABLISHED
tcp     1389      0 127.0.0.1:56058         127.0.1.1:139           CLOSE_WAIT
tcp        0      0 10.0.2.15:58128         142.250.189.174:443     ESTABLISHED
tcp        0      0 10.0.2.15:37738         13.227.73.13:443        TIME_WAIT
tcp        0      0 10.0.2.15:36202         13.227.73.41:443        TIME_WAIT
tcp        0      0 10.0.2.15:46222         96.16.172.70:443        TIME_WAIT
tcp        0      0 10.0.2.15:57430         172.217.164.98:443      ESTABLISHED
tcp        0      0 10.0.2.15:36648         172.217.5.97:443        ESTABLISHED
tcp        0      0 127.0.1.1:139           127.0.0.1:56106         ESTABLISHED
tcp        0      0 10.0.2.15:52456         142.250.72.206:443      ESTABLISHED
tcp        0      0 10.0.2.15:36502         216.58.194.194:443      ESTABLISHED
tcp        0      0 10.0.2.15:47966         172.217.6.67:443        ESTABLISHED
tcp6       0      0 :::993                  :::*                    LISTEN
tcp6       0      0 :::995                  :::*                    LISTEN
tcp6       0      0 :::139                  :::*                    LISTEN
tcp6       0      0 :::110                  :::*                    LISTEN
tcp6       0      0 :::143                  :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
tcp6       0      0 :::25                   :::*                    LISTEN
tcp6       0      0 :::445                  :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:68              0.0.0.0:*
udp        0      0 172.17.255.255:137      0.0.0.0:*
udp        0      0 172.17.0.1:137          0.0.0.0:*
udp        0      0 10.0.2.255:137          0.0.0.0:*
udp        0      0 10.0.2.15:137           0.0.0.0:*
udp        0      0 0.0.0.0:137             0.0.0.0:*
udp        0      0 172.17.255.255:138      0.0.0.0:*
udp        0      0 172.17.0.1:138          0.0.0.0:*
udp        0      0 10.0.2.255:138          0.0.0.0:*
udp        0      0 10.0.2.15:138           0.0.0.0:*
udp        0      0 0.0.0.0:138             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
```

```
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     38248    @/tmp/dbus-SruE2XqLu7
unix  2      [ ACC ]     STREAM     LISTENING     32772    @/tmp/.ICE-unix/2006
unix  2      [ ]         DGRAM                    13500    /run/systemd/journal/syslog
unix  2      [ ACC ]     STREAM     LISTENING     13508    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    37914    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    30684    /run/user/121/systemd/notify
unix  9      [ ]         DGRAM                    13510    /run/systemd/journal/socket
unix  2      [ ACC ]     SEQPACKET  LISTENING     13498    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     37917    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     30687    /run/user/121/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     37921    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     30691    /run/user/121/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     37922    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     30692    /run/user/121/gnupg/S.gpg-agent.ssh
unix  34     [ ]         DGRAM                    13515    /run/systemd/journal/dev-log
unix  2      [ ACC ]     STREAM     LISTENING     37923    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     37924    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     30693    /run/user/121/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     13518    /run/systemd/fsck.progress
unix  2      [ ACC ]     STREAM     LISTENING     37925    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     30694    /run/user/121/bus
unix  2      [ ACC ]     STREAM     LISTENING     37926    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     30695    /run/user/121/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     30696    /run/user/121/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     37935    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     30697    /run/user/121/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     38356    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     33015    /run/user/121/wayland-0
unix  2      [ ACC ]     STREAM     LISTENING     37287    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     38468    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     37209    @/tmp/.ICE-unix/2613
unix  2      [ ACC ]     STREAM     LISTENING     37028    @/tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    27006    /var/lib/samba/private/msg.sock/1182
unix  2      [ ACC ]     STREAM     LISTENING     256431   /run/user/1000/speech-dispatcher/speechd.sock
unix  2      [ ACC ]     STREAM     LISTENING     37029    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     38166    /tmp/ssh-noE42nw62Nvq/agent.2613
unix  2      [ ACC ]     STREAM     LISTENING     24584    /run/NetworkManager/private-dhcp
unix  2      [ ACC ]     STREAM     LISTENING     37210    /tmp/.ICE-unix/2613
unix  2      [ ACC ]     STREAM     LISTENING     29264    /var/run/docker/libnetwork/6c7feb748bac.sock
unix  2      [ ACC ]     STREAM     LISTENING     1643723  /run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     32773    /tmp/.ICE-unix/2006
unix  2      [ ACC ]     STREAM     LISTENING     32972    /tmp/.X11-unix/X1024
unix  2      [ ACC ]     STREAM     LISTENING     22245    /run/containerd/containerd.sock.ttrpc
```

```
unix  2      [ ACC ]     STREAM     LISTENING     1643723  /run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     32773    /tmp/.ICE-unix/2006
unix  2      [ ACC ]     STREAM     LISTENING     32972    /tmp/.X11-unix/X1024
unix  2      [ ACC ]     STREAM     LISTENING     22245    /run/containerd/containerd.sock.ttrpc
unix  2      [ ACC ]     STREAM     LISTENING     22246    /run/containerd/containerd.sock
unix  2      [ ACC ]     STREAM     LISTENING     16979    /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     30610    @/tmp/dbus-v4txN8kU
unix  2      [ ACC ]     STREAM     LISTENING     16981    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     16983    /run/acpid.socket
unix  2      [ ]         DGRAM                    25774    /var/lib/samba/private/msg.sock/1047
unix  2      [ ACC ]     STREAM     LISTENING     32458    @/tmp/dbus-idOsCeoE
unix  2      [ ACC ]     STREAM     LISTENING     37939    @/tmp/dbus-kJDlnXlN
unix  2      [ ACC ]     STREAM     LISTENING     16985    /run/snapd.socket
unix  2      [ ACC ]     STREAM     LISTENING     17404    @irqbalance522.sock
unix  2      [ ACC ]     STREAM     LISTENING     16987    /run/snapd-snap.socket
unix  2      [ ACC ]     STREAM     LISTENING     25799    /var/run/samba/nmbd/unexpected
unix  2      [ ACC ]     STREAM     LISTENING     37938    @/tmp/dbus-pa4xfhES
unix  2      [ ACC ]     STREAM     LISTENING     27343    public/cleanup
unix  2      [ ACC ]     STREAM     LISTENING     25431    /var/run/dovecot/ssl-params
unix  2      [ ACC ]     STREAM     LISTENING     25432    /var/run/dovecot/login/ssl-params
unix  2      [ ACC ]     STREAM     LISTENING     16991    /var/run/docker.sock
unix  2      [ ACC ]     STREAM     LISTENING     25433    /var/run/dovecot/replicator
unix  2      [ ACC ]     STREAM     LISTENING     25434    /var/run/dovecot/replication-notify
unix  2      [ ACC ]     STREAM     LISTENING     16993    /run/avahi-daemon/socket
unix  2      [ ACC ]     STREAM     LISTENING     27346    public/qmgr
unix  2      [ ACC ]     STREAM     LISTENING     25435    /var/run/dovecot/login/pop3
unix  2      [ ACC ]     STREAM     LISTENING     27350    private/tlsmgr
unix  2      [ ACC ]     STREAM     LISTENING     25443    /var/run/dovecot/log-errors
unix  2      [ ACC ]     STREAM     LISTENING     27353    private/rewrite
unix  2      [ ACC ]     STREAM     LISTENING     25444    /var/run/dovecot/ipc
unix  2      [ ACC ]     STREAM     LISTENING     27356    private/bounce
unix  2      [ ACC ]     STREAM     LISTENING     25445    /var/run/dovecot/login/ipc-proxy
unix  2      [ ACC ]     STREAM     LISTENING     27359    private/defer
unix  2      [ ACC ]     STREAM     LISTENING     25446    /var/run/dovecot/indexer-worker
unix  2      [ ACC ]     STREAM     LISTENING     27362    private/trace
unix  2      [ ACC ]     STREAM     LISTENING     25447    /var/run/dovecot/indexer
unix  2      [ ACC ]     STREAM     LISTENING     27365    private/verify
unix  2      [ ACC ]     STREAM     LISTENING     25448    /var/run/dovecot/login/imap
unix  2      [ ACC ]     STREAM     LISTENING     27368    public/flush
unix  2      [ ACC ]     STREAM     LISTENING     25449    /var/run/dovecot/imap-master
unix  2      [ ACC ]     STREAM     LISTENING     27371    private/proxymap
unix  2      [ ACC ]     STREAM     LISTENING     25450    /var/run/dovecot/imap-urlauth-worker
unix  2      [ ACC ]     STREAM     LISTENING     27374    private/proxywrite
unix  2      [ ACC ]     STREAM     LISTENING     27339    public/pickup
unix  2      [ ACC ]     STREAM     LISTENING     25451    /var/run/dovecot/token-login/imap-urlauth
unix  2      [ ACC ]     STREAM     LISTENING     27377    private/smtp
unix  2      [ ACC ]     STREAM     LISTENING     25452    /var/run/dovecot/imap-urlauth
unix  2      [ ACC ]     STREAM     LISTENING     27380    private/relay
unix  2      [ ]         DGRAM                    27037    /var/lib/samba/private/msg.sock/1333
```

```
unix  2      [ ACC ]     STREAM     LISTENING     27383    public/showq
unix  2      [ ACC ]     STREAM     LISTENING     25458    /var/run/dovecot/doveadm-server
unix  2      [ ACC ]     STREAM     LISTENING     27386    private/error
unix  2      [ ACC ]     STREAM     LISTENING     25459    /var/run/dovecot/dns-client
unix  2      [ ACC ]     STREAM     LISTENING     27389    private/retry
unix  2      [ ]         DGRAM                    26583    /var/lib/samba/private/msg.sock/1354
unix  2      [ ACC ]     STREAM     LISTENING     25460    /var/run/dovecot/director-admin
unix  2      [ ACC ]     STREAM     LISTENING     27392    private/discard
unix  2      [ ACC ]     STREAM     LISTENING     25461    /var/run/dovecot/director-userdb
unix  2      [ ACC ]     STREAM     LISTENING     27395    private/local
unix  2      [ ACC ]     STREAM     LISTENING     25462    /var/run/dovecot/dict
unix  2      [ ]         DGRAM                    236706   /var/lib/samba/private/msg.sock/8814
unix  2      [ ACC ]     STREAM     LISTENING     27398    private/virtual
unix  2      [ ACC ]     STREAM     LISTENING     25463    /var/run/dovecot/dict-async
unix  2      [ ACC ]     STREAM     LISTENING     27401    private/lmtp
unix  2      [ ACC ]     STREAM     LISTENING     25464    /var/run/dovecot/config
unix  2      [ ACC ]     STREAM     LISTENING     27404    private/anvil
unix  2      [ ACC ]     STREAM     LISTENING     25465    /var/run/dovecot/login/login
unix  2      [ ACC ]     STREAM     LISTENING     27407    private/scache
unix  2      [ ACC ]     STREAM     LISTENING     25466    /var/run/dovecot/token-login/tokenlogin
unix  2      [ ACC ]     STREAM     LISTENING     27410    private/maildrop
unix  2      [ ACC ]     STREAM     LISTENING     25467    /var/run/dovecot/auth-login
unix  2      [ ACC ]     STREAM     LISTENING     27413    private/uucp
unix  2      [ ACC ]     STREAM     LISTENING     25468    /var/run/dovecot/auth-client
unix  2      [ ACC ]     STREAM     LISTENING     27416    private/ifmail
unix  2      [ ACC ]     STREAM     LISTENING     27419    private/bsmtp
unix  2      [ ACC ]     STREAM     LISTENING     25469    /var/run/dovecot/auth-userdb
unix  2      [ ACC ]     STREAM     LISTENING     27422    private/scalemail-backend
unix  2      [ ACC ]     STREAM     LISTENING     25470    /var/run/dovecot/auth-master
unix  2      [ ACC ]     STREAM     LISTENING     27425    private/mailman
unix  2      [ ACC ]     STREAM     LISTENING     25471    /var/run/dovecot/auth-worker
unix  2      [ ACC ]     STREAM     LISTENING     25472    /var/run/dovecot/anvil
unix  2      [ ACC ]     STREAM     LISTENING     38522    @/tmp/dbus-PKlNAY9d
unix  2      [ ACC ]     STREAM     LISTENING     25473    /var/run/dovecot/anvil-auth-penalty
unix  2      [ ACC ]     STREAM     LISTENING     25474    /var/run/dovecot/master
unix  2      [ ]         DGRAM                    27202    @0000c
unix  2      [ ACC ]     STREAM     LISTENING     30613    @/tmp/dbus-8uh0ceIN
unix  2      [ ACC ]     STREAM     LISTENING     25430    /var/run/dovecot/stats
unix  2      [ ]         DGRAM                    27036    /var/lib/samba/private/msg.sock/1331
unix  2      [ ACC ]     STREAM     LISTENING     30611    @/tmp/dbus-t94kyS5W
unix  2      [ ACC ]     STREAM     LISTENING     32971    @/tmp/.X11-unix/X1024
unix  2      [ ACC ]     STREAM     LISTENING     27788    /var/run/docker/metrics.sock
unix  2      [ ]         DGRAM                    20137    /var/spool/postfix/dev/log
unix  3      [ ]         DGRAM                    13485    /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     31981    @/tmp/dbus-AmNDuYejSX
unix  2      [ ACC ]     STREAM     LISTENING     30612    @/tmp/dbus-kOW73Cm7
unix  2      [ ACC ]     STREAM     LISTENING     13488    /run/systemd/private
unix  3      [ ]         STREAM     CONNECTED     1214779
unix  3      [ ]         STREAM     CONNECTED     41464
```

```
unix  3      [ ]         STREAM     CONNECTED     37656    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33455
unix  3      [ ]         STREAM     CONNECTED     19007
unix  3      [ ]         STREAM     CONNECTED     41385
unix  3      [ ]         STREAM     CONNECTED     40395
unix  3      [ ]         STREAM     CONNECTED     40821
unix  3      [ ]         DGRAM                    30685
unix  3      [ ]         STREAM     CONNECTED     249022
unix  3      [ ]         STREAM     CONNECTED     41009    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39779    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     39735
unix  3      [ ]         STREAM     CONNECTED     38789
unix  3      [ ]         STREAM     CONNECTED     37071    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     35728
unix  3      [ ]         STREAM     CONNECTED     31823
unix  3      [ ]         STREAM     CONNECTED     27400
unix  3      [ ]         STREAM     CONNECTED     1335150
unix  3      [ ]         STREAM     CONNECTED     1170563  @/dbus-vfs-daemon/socket-VRAWYSoT
unix  3      [ ]         STREAM     CONNECTED     39398
unix  3      [ ]         STREAM     CONNECTED     37677
unix  3      [ ]         STREAM     CONNECTED     33433    @/tmp/.X11-unix/X1024
unix  3      [ ]         STREAM     CONNECTED     1171933  @/dbus-vfs-daemon/socket-Nen1qpBt
unix  3      [ ]         STREAM     CONNECTED     40536
unix  3      [ ]         STREAM     CONNECTED     40410    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     37962
unix  3      [ ]         STREAM     CONNECTED     40814
unix  3      [ ]         STREAM     CONNECTED     40580
unix  3      [ ]         STREAM     CONNECTED     39768    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     40240
unix  3      [ ]         STREAM     CONNECTED     38432    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     37066
unix  2      [ ]         DGRAM                    31816
unix  3      [ ]         STREAM     CONNECTED     31531    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     27397
unix  3      [ ]         STREAM     CONNECTED     263979
unix  3      [ ]         STREAM     CONNECTED     39374
unix  3      [ ]         STREAM     CONNECTED     37652
unix  3      [ ]         STREAM     CONNECTED     33432
unix  3      [ ]         STREAM     CONNECTED     19198
unix  2      [ ]         DGRAM                    1181913
unix  3      [ ]         STREAM     CONNECTED     40529
unix  3      [ ]         STREAM     CONNECTED     40396    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     37005    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     41452
unix  3      [ ]         STREAM     CONNECTED     41263    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     39889    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     39736    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39438    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     38435    @/tmp/.X11-unix/X0
```

```
unix  3      [ ]         STREAM     CONNECTED     40403    @/tmp/dbus-SruE2XqLu7
unix  3      [ ]         STREAM     CONNECTED     37961
unix  3      [ ]         STREAM     CONNECTED     20725
unix  3      [ ]         STREAM     CONNECTED     41451
unix  3      [ ]         STREAM     CONNECTED     41345    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     31826    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     40658
unix  3      [ ]         STREAM     CONNECTED     40421    @/tmp/.ICE-unix/2613
unix  3      [ ]         STREAM     CONNECTED     40168
unix  3      [ ]         STREAM     CONNECTED     37346
unix  3      [ ]         STREAM     CONNECTED     37069
unix  3      [ ]         STREAM     CONNECTED     35729    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     31862
unix  3      [ ]         STREAM     CONNECTED     27411
unix  3      [ ]         STREAM     CONNECTED     1911230
unix  3      [ ]         STREAM     CONNECTED     1366470
unix  3      [ ]         STREAM     CONNECTED     40082
unix  3      [ ]         STREAM     CONNECTED     39347    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33461
unix  2      [ ]         DGRAM                    19205
unix  3      [ ]         STREAM     CONNECTED     39811    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     40405    @/tmp/dbus-SruE2XqLu7
unix  3      [ ]         STREAM     CONNECTED     37936
unix  3      [ ]         DGRAM                    30686
unix  3      [ ]         STREAM     CONNECTED     40657
unix  3      [ ]         STREAM     CONNECTED     39761    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39617
unix  3      [ ]         STREAM     CONNECTED     38314    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    36947
unix  3      [ ]         STREAM     CONNECTED     31866
unix  3      [ ]         STREAM     CONNECTED     27408
unix  3      [ ]         STREAM     CONNECTED     1336572
unix  3      [ ]         STREAM     CONNECTED     39346
unix  3      [ ]         STREAM     CONNECTED     39106    /run/user/1000/pulse/native
unix  3      [ ]         STREAM     CONNECTED     33465    @/tmp/.X11-unix/X1024
unix  3      [ ]         STREAM     CONNECTED     40555
unix  3      [ ]         STREAM     CONNECTED     40404
unix  3      [ ]         DGRAM                    37915
unix  3      [ ]         STREAM     CONNECTED     41450
unix  3      [ ]         STREAM     CONNECTED     40852
unix  3      [ ]         STREAM     CONNECTED     41032    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     40600
unix  3      [ ]         STREAM     CONNECTED     39516
unix  3      [ ]         STREAM     CONNECTED     37523
unix  3      [ ]         STREAM     CONNECTED     38315    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     32771    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     31533
unix  3      [ ]         STREAM     CONNECTED     27399
unix  3      [ ]         STREAM     CONNECTED     1357433
```

```
unix  3      [ ]         STREAM     CONNECTED     39882
unix  3      [ ]         STREAM     CONNECTED     37963    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20726    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19465    /var/run/dbus/system_bus_socket
unix  3      [ ]         SEQPACKET  CONNECTED     41449
unix  3      [ ]         STREAM     CONNECTED     40839
unix  2      [ ]         DGRAM                    30668
unix  3      [ ]         STREAM     CONNECTED     41011    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     39683
unix  3      [ ]         STREAM     CONNECTED     40401    @/tmp/dbus-SruE2XqLu7
unix  3      [ ]         STREAM     CONNECTED     37326
unix  3      [ ]         STREAM     CONNECTED     31844
unix  3      [ ]         STREAM     CONNECTED     1911229
unix  3      [ ]         STREAM     CONNECTED     1336856
unix  3      [ ]         STREAM     CONNECTED     39410
unix  3      [ ]         STREAM     CONNECTED     37660
unix  3      [ ]         STREAM     CONNECTED     33483    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     24097
unix  3      [ ]         STREAM     CONNECTED     263989
unix  3      [ ]         SEQPACKET  CONNECTED     41392
unix  3      [ ]         STREAM     CONNECTED     40423
unix  3      [ ]         DGRAM                    37916
unix  3      [ ]         STREAM     CONNECTED     27804    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18458
unix  3      [ ]         STREAM     CONNECTED     41453
unix  3      [ ]         STREAM     CONNECTED     40840    @/tmp/dbus-PKlNAY9d
unix  3      [ ]         STREAM     CONNECTED     31769
unix  3      [ ]         STREAM     CONNECTED     40619
unix  3      [ ]         STREAM     CONNECTED     39760
unix  3      [ ]         STREAM     CONNECTED     40400    @/tmp/dbus-SruE2XqLu7
unix  3      [ ]         STREAM     CONNECTED     37344
unix  3      [ ]         STREAM     CONNECTED     37072    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     31863
unix  3      [ ]         STREAM     CONNECTED     31528
unix  3      [ ]         STREAM     CONNECTED     1366469
unix  3      [ ]         STREAM     CONNECTED     1170871
unix  3      [ ]         STREAM     CONNECTED     40111    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     37679
unix  3      [ ]         STREAM     CONNECTED     33475    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     27293    /run/containerd/containerd.sock
unix  3      [ ]         STREAM     CONNECTED     24844    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     263988
unix  2      [ ]         DGRAM                    40474
unix  3      [ ]         STREAM     CONNECTED     40420
unix  3      [ ]         STREAM     CONNECTED     40822    @/tmp/.ICE-unix/2613
unix  3      [ ]         STREAM     CONNECTED     40656
unix  3      [ ]         STREAM     CONNECTED     39759    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39616
unix  3      [ ]         STREAM     CONNECTED     37272
```

```
/usr/bin/find: ‘/usr/src/.puta’: No such file or directory
/usr/bin/find: ‘/usr/info’: No such file or directory
###
### Output of: /usr/bin/find /lib /usr/lib /usr/local/lib -name libproc.a
###
###
### Output of: /usr/bin/find /dev/.lib/lib -name 1i0n.sh
2> /dev/null
###
###
### Output of: /usr/bin/find /dev -name ptyxx
###
###
### Output of: /usr/bin/find /usr/doc -name '... '
###
/usr/bin/find: ‘/usr/doc’: No such file or directory
###
### Output of: /usr/bin/find /usr/lib -name '.ark*'
###
###
### Output of: /usr/bin/find /bin -name rtty -o -name squit
###
###
### Output of: /usr/bin/find /sbin -name pback
###
###
### Output of: /usr/bin/find /usr/man/man3 -name psid 2> /dev/null
###
###
### Output of: /usr/bin/find /proc -name kset 2> /dev/null
###
###
### Output of: /usr/bin/find /usr/src/linux/modules -name autod.o -o -name soundx.o 2> /dev/null
###
###
### Output of: /usr/bin/find /usr/bin -name gib -o -name ct -o -name snick -o -name kfl
###
###
### Output of: /usr/bin/find /bin /usr/bin -name kr4p -o -name n3tstat -o -name chsh2
###
###
### Output of: /usr/bin/find /etc/rc.d/rsha
###
/usr/bin/find: ‘/etc/rc.d/rsha’: No such file or directory
###
### Output of: /usr/bin/find /etc/rc.d/arch/alpha/lib/.lib /usr/src/linux/arch/alpha/lib/.lib/
###
/usr/bin/find: ‘/etc/rc.d/arch/alpha/lib/.lib’: No such file or directory
/usr/bin/find: ‘/usr/src/linux/arch/alpha/lib/.lib/’: No such file or directory
```

```
unix  3      [ ]         STREAM     CONNECTED     37660
unix  3      [ ]         STREAM     CONNECTED     33483    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     24097
unix  3      [ ]         STREAM     CONNECTED     263989
unix  3      [ ]         SEQPACKET  CONNECTED     41392
unix  3      [ ]         STREAM     CONNECTED     40423
unix  3      [ ]         DGRAM                    37916
unix  3      [ ]         STREAM     CONNECTED     27804    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     18458
unix  3      [ ]         STREAM     CONNECTED     41453
unix  3      [ ]         STREAM     CONNECTED     40840    @/tmp/dbus-PKlNAY9d
unix  3      [ ]         STREAM     CONNECTED     31769
unix  3      [ ]         STREAM     CONNECTED     40619
unix  3      [ ]         STREAM     CONNECTED     39760
unix  3      [ ]         STREAM     CONNECTED     40400    @/tmp/dbus-SruE2XqLu7
unix  3      [ ]         STREAM     CONNECTED     37344
unix  3      [ ]         STREAM     CONNECTED     37072    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     31863
unix  3      [ ]         STREAM     CONNECTED     31528
unix  3      [ ]         STREAM     CONNECTED     1366469
unix  3      [ ]         STREAM     CONNECTED     1170871
unix  3      [ ]         STREAM     CONNECTED     40111    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     37679
unix  3      [ ]         STREAM     CONNECTED     33475    /run/user/121/bus
unix  3      [ ]         STREAM     CONNECTED     27293    /run/containerd/containerd.sock
unix  3      [ ]         STREAM     CONNECTED     24844    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     263988
unix  2      [ ]         DGRAM                    40474
unix  3      [ ]         STREAM     CONNECTED     40420
unix  3      [ ]         STREAM     CONNECTED     40822    @/tmp/.ICE-unix/2613
unix  3      [ ]         STREAM     CONNECTED     40656
unix  3      [ ]         STREAM     CONNECTED     39759    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39616
unix  3      [ ]         STREAM     CONNECTED     37272
unix  3      [ ]         STREAM     CONNECTED     31927
unix  3      [ ]         STREAM     CONNECTED     30617    @/tmp/dbus-kOW73Cm7
unix  3      [ ]         STREAM     CONNECTED     1336573
unix  3      [ ]         STREAM     CONNECTED     1170875
unix  3      [ ]         STREAM     CONNECTED     39400    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     37680    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33482
unix  3      [ ]         STREAM     CONNECTED     41395
unix  3      [ ]         STREAM     CONNECTED     40402
unix  3      [ ]         SEQPACKET  CONNECTED     41448
unix  3      [ ]         STREAM     CONNECTED     31732    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    40602
unix  3      [ ]         STREAM     CONNECTED     40556
unix  3      [ ]         STREAM     CONNECTED     40261
unix  3      [ ]         STREAM     CONNECTED     37327    /run/user/1000/bus
```

```
unix  3      [ ]         STREAM     CONNECTED     33715    @/tmp/dbus-AmNDuYejSX
unix  3      [ ]         STREAM     CONNECTED     34172    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     33401
unix  3      [ ]         STREAM     CONNECTED     19670
unix  3      [ ]         STREAM     CONNECTED     1214769
unix  3      [ ]         SEQPACKET  CONNECTED     1201529
unix  3      [ ]         DGRAM                    13487
unix  3      [ ]         STREAM     CONNECTED     37630
unix  3      [ ]         STREAM     CONNECTED     37311    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     36859
unix  3      [ ]         STREAM     CONNECTED     24946    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20251
unix  2      [ ]         DGRAM                    20123
unix  3      [ ]         STREAM     CONNECTED     19463
unix  3      [ ]         STREAM     CONNECTED     1310170
unix  2      [ ]         SEQPACKET  CONNECTED     303001
unix  3      [ ]         STREAM     CONNECTED     49024
unix  3      [ ]         STREAM     CONNECTED     41033
unix  2      [ ]         DGRAM                    39566
unix  3      [ ]         STREAM     CONNECTED     40264
unix  3      [ ]         STREAM     CONNECTED     38218
unix  3      [ ]         STREAM     CONNECTED     33924
unix  3      [ ]         STREAM     CONNECTED     31731
unix  3      [ ]         STREAM     CONNECTED     27355
unix  3      [ ]         STREAM     CONNECTED     1215496
unix  3      [ ]         STREAM     CONNECTED     39807    @/tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    34464
unix  2      [ ]         DGRAM                    34364
unix  3      [ ]         STREAM     CONNECTED     34171
unix  3      [ ]         STREAM     CONNECTED     33380
unix  2      [ ]         DGRAM                    27556
unix  3      [ ]         STREAM     CONNECTED     1214768
unix  3      [ ]         STREAM     CONNECTED     1201520
unix  2      [ ]         DGRAM                    31691
unix  3      [ ]         STREAM     CONNECTED     1643732  /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     38387    /var/run/dbus/system_bus_socket
unix  2      [ ]         STREAM     CONNECTED     268605   @/tmp/dbus-mBcSPmyJ
unix  3      [ ]         STREAM     CONNECTED     49025    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     39887    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     39588
unix  3      [ ]         STREAM     CONNECTED     40262
unix  3      [ ]         STREAM     CONNECTED     38224    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     33968    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     31841    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     1310185
unix  3      [ ]         STREAM     CONNECTED     1306581
unix  3      [ ]         STREAM     CONNECTED     230825
unix  3      [ ]         STREAM     CONNECTED     39868
unix  2      [ ]         DGRAM                    34376
```

```
EXE 12003: /usr/lib/firefox/firefox
CWD 12077: /proc/9766/fdinfo
EXE 12077: /usr/lib/firefox/firefox
CWD 12594: /
EXE 12594: /usr/sbin/cups-browsed
CWD 12604: /
EXE 12604: /usr/sbin/cups-browsed
CWD 12806: /proc/903/fdinfo
EXE 12806: /usr/lib/firefox/firefox
CWD 12807: /proc/903/fdinfo
EXE 12807: /usr/lib/firefox/firefox
CWD 12963: /proc/3552/fdinfo
EXE 12963: /usr/lib/firefox/firefox
CWD 12964: /proc/3552/fdinfo
EXE 12964: /usr/lib/firefox/firefox
CWD 12967: /proc/3552/fdinfo
EXE 12967: /usr/lib/firefox/firefox
CWD 12968: /proc/3552/fdinfo
EXE 12968: /usr/lib/firefox/firefox
CWD 13610: /proc/3419/fdinfo
EXE 13610: /usr/lib/firefox/firefox
CWD 13611: /proc/3419/fdinfo
EXE 13611: /usr/lib/firefox/firefox
CWD 13851: /proc/1078/fdinfo
EXE 13851: /usr/lib/firefox/firefox
CWD 13853: /proc/1078/fdinfo
EXE 13853: /usr/lib/firefox/firefox
CWD 25851: /home/sysadmin
EXE 25851: /usr/lib/firefox/firefox
CWD 25908: /home/sysadmin
EXE 25908: /usr/lib/firefox/firefox
CWD 25909: /home/sysadmin
EXE 25909: /usr/lib/firefox/firefox
CWD 25927: /home/sysadmin
EXE 25927: /usr/lib/firefox/firefox
CWD 25952: /home/sysadmin
EXE 25952: /usr/lib/firefox/firefox
CWD 26185: /proc/903/fdinfo
EXE 26185: /usr/lib/firefox/firefox
CWD 26204: /proc/10304/fdinfo
EXE 26204: /usr/lib/firefox/firefox
CWD 26226: /proc/9766/fdinfo
EXE 26226: /usr/lib/firefox/firefox
CWD 26798: /home/sysadmin
EXE 26798: /usr/lib/firefox/firefox
CWD 26799: /home/sysadmin
EXE 26799: /usr/lib/firefox/firefox
not found
###
```

```
EXE 10314: /usr/lib/firefox/firefox
CWD 10315: /proc/10304/fdinfo
EXE 10315: /usr/lib/firefox/firefox
CWD 10316: /proc/10304/fdinfo
EXE 10316: /usr/lib/firefox/firefox
CWD 10317: /proc/10304/fdinfo
EXE 10317: /usr/lib/firefox/firefox
CWD 10319: /proc/10304/fdinfo
EXE 10319: /usr/lib/firefox/firefox
CWD 10320: /proc/10304/fdinfo
EXE 10320: /usr/lib/firefox/firefox
CWD 10321: /proc/10304/fdinfo
EXE 10321: /usr/lib/firefox/firefox
CWD 10322: /proc/10304/fdinfo
EXE 10322: /usr/lib/firefox/firefox
CWD 10323: /proc/10304/fdinfo
EXE 10323: /usr/lib/firefox/firefox
CWD 10324: /proc/10304/fdinfo
EXE 10324: /usr/lib/firefox/firefox
CWD 10636: /proc/9766/fdinfo
EXE 10636: /usr/lib/firefox/firefox
CWD 10637: /proc/9766/fdinfo
EXE 10637: /usr/lib/firefox/firefox
CWD 10639: /proc/9766/fdinfo
EXE 10639: /usr/lib/firefox/firefox
CWD 10640: /proc/9766/fdinfo
EXE 10640: /usr/lib/firefox/firefox
CWD 10641: /proc/9766/fdinfo
EXE 10641: /usr/lib/firefox/firefox
CWD 11212: /proc/10304/fdinfo
EXE 11212: /usr/lib/firefox/firefox
CWD 11229: /proc/10304/fdinfo
EXE 11229: /usr/lib/firefox/firefox
CWD 11230: /proc/10304/fdinfo
EXE 11230: /usr/lib/firefox/firefox
CWD 11990: /proc/9766/fdinfo
EXE 11990: /usr/lib/firefox/firefox
CWD 11997: /proc/9766/fdinfo
EXE 11997: /usr/lib/firefox/firefox
CWD 11998: /home/sysadmin
EXE 11998: /usr/lib/firefox/firefox
CWD 11999: /home/sysadmin
EXE 11999: /usr/lib/firefox/firefox
CWD 12000: /proc/9766/fdinfo
EXE 12000: /usr/lib/firefox/firefox
CWD 12001: /proc/9766/fdinfo
EXE 12001: /usr/lib/firefox/firefox
CWD 12002: /proc/9766/fdinfo
EXE 12002: /usr/lib/firefox/firefox
```

```
EXE  7301: /usr/lib/firefox/firefox
CWD  7302: /proc/1078/fdinfo
EXE  7302: /usr/lib/firefox/firefox
CWD  7459: /home/sysadmin
EXE  7459: /usr/lib/firefox/firefox
CWD  7461: /proc/7458/fdinfo
EXE  7461: /usr/lib/firefox/firefox
CWD  7462: /proc/7458/fdinfo
EXE  7462: /usr/lib/firefox/firefox
CWD  7463: /proc/7458/fdinfo
EXE  7463: /usr/lib/firefox/firefox
CWD  7464: /proc/7458/fdinfo
EXE  7464: /usr/lib/firefox/firefox
CWD  7465: /proc/7458/fdinfo
EXE  7465: /usr/lib/firefox/firefox
CWD  7466: /proc/7458/fdinfo
EXE  7466: /usr/lib/firefox/firefox
CWD  7467: /proc/7458/fdinfo
EXE  7467: /usr/lib/firefox/firefox
CWD  7468: /proc/7458/fdinfo
EXE  7468: /usr/lib/firefox/firefox
CWD  7469: /proc/7458/fdinfo
EXE  7469: /usr/lib/firefox/firefox
CWD  7470: /proc/7458/fdinfo
EXE  7470: /usr/lib/firefox/firefox
CWD  7471: /proc/7458/fdinfo
EXE  7471: /usr/lib/firefox/firefox
CWD  7472: /proc/7458/fdinfo
EXE  7472: /usr/lib/firefox/firefox
CWD  7473: /proc/7458/fdinfo
EXE  7473: /usr/lib/firefox/firefox
CWD  7474: /proc/7458/fdinfo
EXE  7474: /usr/lib/firefox/firefox
CWD  7475: /proc/7458/fdinfo
EXE  7475: /usr/lib/firefox/firefox
CWD  7476: /proc/7458/fdinfo
EXE  7476: /usr/lib/firefox/firefox
CWD  7477: /proc/7458/fdinfo
EXE  7477: /usr/lib/firefox/firefox
CWD  7478: /proc/7458/fdinfo
EXE  7478: /usr/lib/firefox/firefox
CWD  7486: /proc/7484/fdinfo
EXE  7486: /usr/lib/firefox/firefox
CWD  7487: /home/sysadmin
EXE  7487: /usr/lib/firefox/firefox
CWD  7488: /proc/7484/fdinfo
EXE  7488: /usr/lib/firefox/firefox
CWD  7489: /proc/7484/fdinfo
EXE  7489: /usr/lib/firefox/firefox
```

```
###
### Output of: ./chklastlog  -f /var/log/wtmp -l /var/log/lastlog
###
 The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! gdm          2051 tty1   /usr/bin/Xwayland :1024 -rootless -terminate -accessx -core -listen 4 -listen 5 -displayfd 6
! gdm          2001 tty1   /usr/lib/gdm3/gdm-wayland-session gnome-session --autostart /usr/share/gdm/greeter/autostart
! gdm          2006 tty1   /usr/lib/gnome-session/gnome-session-binary --autostart /usr/share/gdm/greeter/autostart
! gdm          2013 tty1   /usr/bin/gnome-shell
! gdm          2158 tty1   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! gdm          2159 tty1   /usr/lib/gnome-settings-daemon/gsd-clipboard
! gdm          2161 tty1   /usr/lib/gnome-settings-daemon/gsd-color
! gdm          2163 tty1   /usr/lib/gnome-settings-daemon/gsd-datetime
! gdm          2167 tty1   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! gdm          2181 tty1   /usr/lib/gnome-settings-daemon/gsd-keyboard
! gdm          2183 tty1   /usr/lib/gnome-settings-daemon/gsd-media-keys
! gdm          2189 tty1   /usr/lib/gnome-settings-daemon/gsd-mouse
! gdm          2190 tty1   /usr/lib/gnome-settings-daemon/gsd-power
! gdm          2192 tty1   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! gdm          2195 tty1   /usr/lib/gnome-settings-daemon/gsd-rfkill
! gdm          2199 tty1   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! gdm          2201 tty1   /usr/lib/gnome-settings-daemon/gsd-sharing
! gdm          2202 tty1   /usr/lib/gnome-settings-daemon/gsd-smartcard
! gdm          2206 tty1   /usr/lib/gnome-settings-daemon/gsd-sound
! gdm          2217 tty1   /usr/lib/gnome-settings-daemon/gsd-wacom
! gdm          2155 tty1   /usr/lib/gnome-settings-daemon/gsd-xsettings
! gdm          2103 tty1   ibus-daemon --xim --panel disable
! gdm          2107 tty1   /usr/lib/ibus/ibus-dconf
! gdm          2280 tty1   /usr/lib/ibus/ibus-engine-simple
! gdm          2109 tty1   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin      899 tty2   /usr/lib/firefox/firefox -contentproc -childID 16 -isForBrowser -prefsLen 12416 -prefMapSize
 176343 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appd
ir /usr/lib/firefox/browser 3315 true tab
! sysadmin     1077 tty2   /usr/lib/firefox/firefox -contentproc -childID 19 -isForBrowser -prefsLen 12416 -prefMapSize
 176343 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appd
ir /usr/lib/firefox/browser 3315 true tab
! sysadmin     3418 tty2   /usr/lib/firefox/firefox -contentproc -childID 2 -isForBrowser -prefsLen 1 -prefMapSize 1763
43 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appdir /u
sr/lib/firefox/browser 3315 true tab
! sysadmin     3551 tty2   /usr/lib/firefox/firefox -contentproc -childID 5 -isForBrowser -prefsLen 9422 -prefMapSize 1
76343 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appdir
 /usr/lib/firefox/browser 3315 true tab
! sysadmin     7457 tty2   /usr/lib/firefox/firefox -contentproc -childID 23 -isForBrowser -prefsLen 12450 -prefMapSize
 176343 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appd
ir /usr/lib/firefox/browser 3315 true tab
! sysadmin     7483 tty2   /usr/lib/firefox/firefox -contentproc -childID 24 -isForBrowser -prefsLen 12450 -prefMapSize
 176343 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appd
ir /usr/lib/firefox/browser 3315 true tab
```

```
! sysadmin     3395 tty2   /usr/lib/firefox/firefox -contentproc -childID 1 -isForBrowser -prefsLen 1 -prefMapSize 1763
43 -parentBuildID 20190718161435 -greomni /usr/lib/firefox/omni.ja -appomni /usr/lib/firefox/browser/omni.ja -appdir /u
sr/lib/firefox/browser 3315 true tab
! sysadmin     2587 tty2   /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -no
reset -keeptty -verbose 3
! sysadmin     3315 tty2   /usr/lib/firefox/firefox -new-window
! sysadmin     2582 tty2   /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session -
-session=ubuntu
! sysadmin     2613 tty2   /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
! sysadmin     2785 tty2   /usr/bin/gnome-shell
! sysadmin     3575 tty2   /usr/bin/gnome-software --gapplication-service
! sysadmin     3053 tty2   /usr/lib/gnome-settings-daemon/gsd-a11y-settings
! sysadmin     3057 tty2   /usr/lib/gnome-settings-daemon/gsd-clipboard
! sysadmin     3051 tty2   /usr/lib/gnome-settings-daemon/gsd-color
! sysadmin     3061 tty2   /usr/lib/gnome-settings-daemon/gsd-datetime
! sysadmin     3122 tty2   /usr/lib/gnome-disk-utility/gsd-disk-utility-notify
! sysadmin     3063 tty2   /usr/lib/gnome-settings-daemon/gsd-housekeeping
! sysadmin     3064 tty2   /usr/lib/gnome-settings-daemon/gsd-keyboard
! sysadmin     3067 tty2   /usr/lib/gnome-settings-daemon/gsd-media-keys
! sysadmin     3017 tty2   /usr/lib/gnome-settings-daemon/gsd-mouse
! sysadmin     3018 tty2   /usr/lib/gnome-settings-daemon/gsd-power
! sysadmin     3022 tty2   /usr/lib/gnome-settings-daemon/gsd-print-notifications
! sysadmin     3107 tty2   /usr/lib/gnome-settings-daemon/gsd-printer
! sysadmin     3024 tty2   /usr/lib/gnome-settings-daemon/gsd-rfkill
! sysadmin     3026 tty2   /usr/lib/gnome-settings-daemon/gsd-screensaver-proxy
! sysadmin     3028 tty2   /usr/lib/gnome-settings-daemon/gsd-sharing
! sysadmin     3030 tty2   /usr/lib/gnome-settings-daemon/gsd-smartcard
! sysadmin     3033 tty2   /usr/lib/gnome-settings-daemon/gsd-sound
! sysadmin     3037 tty2   /usr/lib/gnome-settings-daemon/gsd-wacom
! sysadmin     3042 tty2   /usr/lib/gnome-settings-daemon/gsd-xsettings
! sysadmin     2860 tty2   ibus-daemon --xim --panel disable
! sysadmin     2864 tty2   /usr/lib/ibus/ibus-dconf
! sysadmin     3206 tty2   /usr/lib/ibus/ibus-engine-simple
! sysadmin     2866 tty2   /usr/lib/ibus/ibus-x11 --kill-daemon
! sysadmin     3120 tty2   nautilus-desktop
! sysadmin    10016 tty2   /usr/lib/speech-dispatcher-modules/sd_dummy /etc/speech-dispatcher/modules/dummy.conf
! sysadmin    10008 tty2   /usr/lib/speech-dispatcher-modules/sd_espeak-ng /etc/speech-dispatcher/modules/espeak-ng.con
f
! sysadmin    10005 tty2   /usr/lib/speech-dispatcher-modules/sd_generic /etc/speech-dispatcher/modules/generic.conf
! root        26498 pts/0  /bin/sh /usr/sbin/chkrootkit -x
! root        26934 pts/0  ./chkutmp
! root        26936 pts/0  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        26935 pts/0  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        26497 pts/0  sudo chkrootkit -x
! sysadmin      709 pts/0  bash
! sysadmin     7970 pts/1  bash
chkutmp: nothing deleted
not tested
sysadmin@UbuntuDesktop:~$
```