Ubuntu 16.04

Download CIS Benchmark:

CIS Ubuntu Linux 16.04 LTS Benchmark - v1.0.0

Overview

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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored
Failure to comply with “Scored” recommendations will decrease the final benchmark score. Compliance with “Scored” recommendations will increase the final benchmark score.

Not scored
Failure to comply with “Not Scored” recommendations will not decrease the final benchmark score. Compliance with “Not Scored” recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

Level 1 - Server
Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for servers.

Level 2 - Server
This profile extends the “Level 1 - Server” profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers.

Level 1 - Workstation
Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for workstations.

Level 2 - Workstation
This profile extends the “Level 1 - Workstation” profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for workstations.

List of content

- 1 Initial setup
  - 1.1 Filesystem Configuration
    - 1.1.1 Disable unused filesystems
      - 1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Scored)
      - 1.1.1.2 Ensure mounting of freevxfs filesystems is disabled (Scored)
      - 1.1.1.3 Ensure mounting of jffs2 filesystems is disabled (Scored)
      - 1.1.1.4 Ensure mounting of hfs filesystems is disabled (Scored)
      - 1.1.1.5 Ensure mounting of hfsplus filesystems is disabled (Scored)
      - 1.1.1.6 Ensure mounting of squashfs filesystems is disabled (Scored)
      - 1.1.1.7 Ensure mounting of udf filesystems is disabled (Scored)
      - 1.1.1.8 Ensure mounting of FAT filesystems is disabled (Scored)
    - 1.1.2 Ensure separate partition exists for /tmp (Scored)
    - 1.1.3 Ensure nodev option set on /tmp partition (Scored)
    - 1.1.4 Ensure nosuid option set on /tmp partition (Scored)
    - 1.1.5 Ensure separate partition exists for /var (Scored)
    - 1.1.6 Ensure separate partition exists for /var/tmp (Scored)
    - 1.1.7 Ensure nodev option set on /var/tmp partition (Scored)
    - 1.1.8 Ensure nosuid option set on /var/tmp partition (Scored)
    - 1.1.9 Ensure noexec option set on /var/tmp partition (Scored)
    - 1.1.10 Ensure separate partition exists for /var/log (Scored)
    - 1.1.11 Ensure separate partition exists for /var/log/audit (Scored)
    - 1.1.12 Ensure separate partition exists for /home (Scored)
    - 1.1.13 Ensure nodev option set on /home partition (Scored)
    - 1.1.14 Ensure nodev option set on /dev/shm partition (Scored)
    - 1.1.15 Ensure nosuid option set on /dev/shm partition (Scored)
    - 1.1.16 Ensure noexec option set on /dev/shm partition (Scored)
    - 1.1.17 Ensure nodev option set on removable media partitions (Not Scored)

        - 1.1.18 Ensure nosuid option set on removable media partitions (Not Scored)
        - 1.1.19 Ensure noexec option set on removable media partitions (Not Scored)
        - 1.1.20 Ensure sticky bit is set on all world-writable directories (Scored)
        - 1.1.21 Disable Automounting (Scored)
    - 1.2 Configure Software Updates
        - 1.2.1 Ensure package manager repositories are configured (Not Scored)
        - 1.2.2 Ensure GPG keys are configured (Not Scored)
    - 1.3 Filesystem Integrity Checking
        - 1.3.1 Ensure AIDE is installed (Scored)
        - 1.3.2 Ensure filesystem integrity is regularly checked (Scored)
    - 1.4 Secure Boot Settings
        - 1.4.1 Ensure permissions on bootloader config are configured (Scored)
        - 1.4.2 Ensure bootloader password is set (Scored)
        - 1.4.3 Ensure authentication required for single user mode (Scored)
    - 1.5 Additional Process Hardening
        - 1.5.1 Ensure core dumps are restricted (Scored)
        - 1.5.2 Ensure XD/NX support is enabled (Not Scored)
        - 1.5.3 Ensure address space layout randomization (ASLR) is enabled (Scored)
        - 1.5.4 Ensure prelink is disabled (Scored)
    - 1.6 Mandatory Access Control
        - 1.6.1 Configure SELinux
            - 1.6.1.1 Ensure SELinux is not disabled in bootloader configuration (Scored)
            - 1.6.1.2 Ensure the SELinux state is enforcing (Scored)
            - 1.6.1.3 Ensure SELinux policy is configured (Scored)
            - 1.6.1.4 Ensure no unconfined daemons exist (Scored)
        - 1.6.2 Configure AppArmor
            - 1.6.2.1 Ensure AppArmor is not disabled in bootloader configuration (Scored)
            - 1.6.2.2 Ensure all AppArmor Profiles are enforcing (Scored)
        - 1.6.3 Ensure SELinux or AppArmor are installed (Not Scored)
    - 1.7 Warning Banners
        - 1.7.1 Command Line Warning Banners
            - 1.7.1.1 Ensure message of the day is configured properly (Scored)
            - 1.7.1.2 Ensure local login warning banner is configured properly (Not Scored)
            - 1.7.1.3 Ensure remote login warning banner is configured properly (Not Scored)
            - 1.7.1.4 Ensure permissions on /etc/motd are configured (Not Scored)
            - 1.7.1.5 Ensure permissions on /etc/issue are configured (Scored)
            - 1.7.1.6 Ensure permissions on /etc/issue.net are configured (Not Scored)
        - 1.7.2 Ensure GDM login banner is configured (Scored)
    - 1.8 Ensure updates, patches, and additional security software are installed (Not Scored)
- 2 Services
    - 2.1 inetd Services
        - 2.1.1 Ensure chargen services are not enabled (Scored)
        - 2.1.2 Ensure daytime services are not enabled (Scored)
        - 2.1.3 Ensure discard services are not enabled (Scored)
        - 2.1.4 Ensure echo services are not enabled (Scored)
        - 2.1.5 Ensure time services are not enabled (Scored)
        - 2.1.6 Ensure rsh server is not enabled (Scored)
        - 2.1.7 Ensure talk server is not enabled (Scored)
        - 2.1.8 Ensure telnet server is not enabled (Scored)
        - 2.1.9 Ensure tftp server is not enabled (Scored)

        - 2.1.10 Ensure xinetd is not enabled (Scored)
    - 2.2 Special Purpose Services
        - 2.2.1 Time Synchronization
            - 2.2.1.1 Ensure time synchronization is in use (Not Scored)
            - 2.2.1.2 Ensure ntp is configured (Scored)
            - 2.2.1.3 Ensure chrony is configured (Scored)
        - 2.2.2 Ensure X Window System is not installed (Scored)
        - 2.2.3 Ensure Avahi Server is not enabled (Scored)
        - 2.2.4 Ensure CUPS is not enabled (Scored)
        - 2.2.5 Ensure DHCP Server is not enabled (Scored)
        - 2.2.6 Ensure LDAP server is not enabled (Scored)
        - 2.2.7 Ensure NFS and RPC are not enabled (Scored)
        - 2.2.8 Ensure DNS Server is not enabled (Scored)
        - 2.2.9 Ensure FTP Server is not enabled (Scored)
        - 2.2.10 Ensure HTTP server is not enabled (Scored)
        - 2.2.11 Ensure IMAP and POP3 server is not enabled (Scored)
        - 2.2.12 Ensure Samba is not enabled (Scored)
        - 2.2.13 Ensure HTTP Proxy Server is not enabled (Scored)
        - 2.2.14 Ensure SNMP Server is not enabled (Scored)
        - 2.2.15 Ensure mail transfer agent is configured for local-only mode (Scored)
        - 2.2.16 Ensure rsync service is not enabled (Scored)
        - 2.2.17 Ensure NIS Server is not enabled (Scored)
    - 2.3 Service Clients
        - 2.3.1 Ensure NIS Client is not installed (Scored)
        - 2.3.2 Ensure rsh client is not installed (Scored)
        - 2.3.3 Ensure talk client is not installed (Scored)
        - 2.3.4 Ensure telnet client is not installed (Scored)
        - 2.3.5 Ensure LDAP client is not installed (Scored)
- 3 Network Configuration
    - 3.1 Network Parameters (Host Only)
        - 3.1.1 Ensure IP forwarding is disabled (Scored)
        - 3.1.2 Ensure packet redirect sending is disabled (Scored)
    - 3.2 Network Parameters (Host and Router)
        - 3.2.1 Ensure source routed packets are not accepted (Scored)
        - 3.2.2 Ensure ICMP redirects are not accepted (Scored)
        - 3.2.3 Ensure secure ICMP redirects are not accepted (Scored)
        - 3.2.4 Ensure suspicious packets are logged (Scored)
        - 3.2.5 Ensure broadcast ICMP requests are ignored (Scored)
        - 3.2.6 Ensure bogus ICMP responses are ignored (Scored)
        - 3.2.7 Ensure Reverse Path Filtering is enabled (Scored)
        - 3.2.8 Ensure TCP SYN Cookies is enabled (Scored)
    - 3.3 IPv6
        - 3.3.1 Ensure IPv6 router advertisements are not accepted (Not Scored)
        - 3.3.2 Ensure IPv6 redirects are not accepted (Not Scored)
        - 3.3.3 Ensure IPv6 is disabled (Not Scored)
    - 3.4 TCP Wrappers
        - 3.4.1 Ensure TCP Wrappers is installed (Scored)
        - 3.4.2 Ensure /etc/hosts.allow is configured (Scored)
        - 3.4.3 Ensure /etc/hosts.deny is configured (Scored)
        - 3.4.4 Ensure permissions on /etc/hosts.allow are configured (Scored)
        - 3.4.5 Ensure permissions on /etc/hosts.deny are 644 (Scored)

- 3.5 Uncommon Network Protocols
  - 3.5.1 Ensure DCCP is disabled (Not Scored)
  - 3.5.2 Ensure SCTP is disabled (Not Scored)
  - 3.5.3 Ensure RDS is disabled (Not Scored)
  - 3.5.4 Ensure TIPC is disabled (Not Scored)
- 3.6 Firewall Configuration
  - 3.6.1 Ensure iptables is installed (Scored)
  - 3.6.2 Ensure default deny firewall policy (Scored)
  - 3.6.3 Ensure loopback traffic is configured (Scored)
  - 3.6.4 Ensure outbound and established connections are configured (Not Scored)
  - 3.6.5 Ensure firewall rules exist for all open ports (Scored)
- 3.7 Ensure wireless interfaces are disabled (Not Scored)

- 4 Logging and Auditing
  - 4.1 Configure System Accounting (auditd)
    - 4.1.1 Configure Data Retention
      - 4.1.1.1 Ensure audit log storage size is configured (Not Scored)
      - 4.1.1.2 Ensure system is disabled when audit logs are full (Scored)
      - 4.1.1.3 Ensure audit logs are not automatically deleted (Scored)
    - 4.1.2 Ensure auditd service is enabled (Scored)
    - 4.1.3 Ensure auditing for processes that start prior to auditd is enabled (Scored)
    - 4.1.4 Ensure events that modify date and time information are collected (Scored)
    - 4.1.5 Ensure events that modify user/group information are collected (Scored)
    - 4.1.6 Ensure events that modify the system's network environment are collected (Scored)
    - 4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected (Scored)
    - 4.1.8 Ensure login and logout events are collected (Scored)
    - 4.1.9 Ensure session initiation information is collected (Scored)
    - 4.1.10 Ensure discretionary access control permission modification events are collected (Scored)
    - 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected (Scored)
    - 4.1.12 Ensure use of privileged commands is collected (Scored)
    - 4.1.13 Ensure successful file system mounts are collected (Scored)
    - 4.1.14 Ensure file deletion events by users are collected (Scored)
    - 4.1.15 Ensure changes to system administration scope (sudoers) is collected (Scored)
    - 4.1.16 Ensure system administrator actions (sudolog) are collected (Scored)
    - 4.1.17 Ensure kernel module loading and unloading is collected (Scored)
    - 4.1.18 Ensure the audit configuration is immutable (Scored)
  - 4.2 Configure Logging
    - 4.2.1 Configure rsyslog
      - 4.2.1.1 Ensure rsyslog Service is enabled (Scored)
      - 4.2.1.2 Ensure logging is configured (Not Scored)
      - 4.2.1.3 Ensure rsyslog default file permissions configured (Scored)
      - 4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host (Scored))
      - 4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)
    - 4.2.2 Configure syslog-ng
      - 4.2.2.1 Ensure syslog-ng service is enabled (Scored)
      - 4.2.2.2 Ensure logging is configured (Not Scored)

- 4.2.2.3 Ensure syslog-ng default file permissions configured (Scored)
- 4.2.2.4 Ensure syslog-ng is configured to send logs to a remote log host (Scored)
- 4.2.2.5 Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)

4.2.3 Ensure rsyslog or syslog-ng is installed (Scored)
4.2.4 Ensure permissions on all logfiles are configured (Scored)

4.3 Ensure logrotate is configured (Not Scored)

5 Access, Authentication and Authorization

5.1 Configure cron
5.1.1 Ensure cron daemon is enabled (Scored)
5.1.2 Ensure permissions on /etc/crontab are configured (Scored)
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Scored)
5.1.4 Ensure permissions on /etc/cron.daily are configured (Scored)
5.1.5 Ensure permissions on /etc/cron.weekly are configured (Scored)
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Scored)
5.1.7 Ensure permissions on /etc/cron.d are configured (Scored)
5.1.8 Ensure at/cron is restricted to authorized users (Scored)

5.2 SSH Server Configuration
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Scored)
5.2.2 Ensure SSH Protocol is set to 2 (Scored)
5.2.3 Ensure SSH LogLevel is set to INFO (Scored)
5.2.4 Ensure SSH X11 forwarding is disabled (Scored)
5.2.5 Ensure SSH MaxAuthTries is set to 4 or less (Scored)
5.2.6 Ensure SSH IgnoreRhosts is enabled (Scored)
5.2.7 Ensure SSH HostbasedAuthentication is disabled (Scored)
5.2.8 Ensure SSH root login is disabled (Scored)
5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Scored)
5.2.10 Ensure SSH PermitUserEnvironment is disabled (Scored)
5.2.11 Ensure only approved MAC algorithms are used (Scored)
5.2.12 Ensure SSH Idle Timeout Interval is configured (Scored)
5.2.13 Ensure SSH LoginGraceTime is set to one minute or less (Scored)
5.2.14 Ensure SSH access is limited (Scored)
5.2.15 Ensure SSH warning banner is configured (Scored)

5.3 Configure PAM
5.3.1 Ensure password creation requirements are configured (Scored)
5.3.2 Ensure lockout for failed password attempts is configured (Not Scored)
5.3.3 Ensure password reuse is limited (Scored)
5.3.4 Ensure password hashing algorithm is SHA-512 (Scored)

5.4 User Accounts and Environment
5.4.1 Set Shadow Password Suite Parameters
- 5.4.1.1 Ensure password expiration is 90 days or less (Scored)
- 5.4.1.2 Ensure minimum days between password changes is 7 or more (Scored)
- 5.4.1.3 Ensure password expiration warning days is 7 or more (Scored)
- 5.4.1.4 Ensure inactive password lock is 30 days or less (Scored)

5.4.2 Ensure system accounts are non-login (Scored)
5.4.3 Ensure default group for the root account is GID 0 (Scored)
5.4.4 Ensure default user umask is 027 or more restrictive (Scored)

5.5 Ensure root login is restricted to system console (Not Scored)
5.6 Ensure access to the su command is restricted (Scored)

- 6 System Maintenance
  - 6.1 System File Permissions
    - 6.1.1 Audit system file permissions (Not Scored)
    - 6.1.2 Ensure permissions on /etc/passwd are configured (Scored)
    - 6.1.3 Ensure permissions on /etc/shadow are configured (Scored)
    - 6.1.4 Ensure permissions on /etc/group are configured (Scored)
    - 6.1.5 Ensure permissions on /etc/shadow are configured (Scored)
    - 6.1.6 Ensure permissions on /etc/passwd- are configured (Scored)
    - 6.1.7 Ensure permissions on /etc/shadow- are configured (Scored)
    - 6.1.8 Ensure permissions on /etc/group- are configured (Scored)
    - 6.1.9 Ensure permissions on /etc/gshadow- are configured (Scored)
    - 6.1.10 Ensure no world writable files exist (Scored)
    - 6.1.11 Ensure no unowned files or directories exist (Scored)
    - 6.1.12 Ensure no ungrouped files or directories exist (Scored)
    - 6.1.13 Audit SUID executables (Not Scored)
    - 6.1.14 Audit SGID executables (Not Scored)
  - 6.2 User and Group Settings
    - 6.2.1 Ensure password fields are not empty (Scored)
    - 6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Scored)
    - 6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Scored)
    - 6.2.4 Ensure no legacy "+" entries exist in /etc/group (Scored)
    - 6.2.5 Ensure root is the only UID 0 account (Scored)
    - 6.2.6 Ensure root PATH Integrity (Scored)
    - 6.2.7 Ensure all users' home directories exist (Scored)
    - 6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Scored)
    - 6.2.9 Ensure users own their home directories (Scored)
    - 6.2.10 Ensure users' dot files are not group or world writable (Scored)
    - 6.2.11 Ensure no users have .forward files (Scored)
    - 6.2.12 Ensure no users have .netrc files (Scored)
    - 6.2.13 Ensure users' .netrc Files are not group or world accessible (Scored)
    - 6.2.14 Ensure no users have .rhosts files (Scored)
    - 6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Scored)
    - 6.2.16 Ensure no duplicate UIDs exist (Scored)
    - 6.2.17 Ensure no duplicate GIDs exist (Scored)
    - 6.2.18 Ensure no duplicate user names exist (Scored)
    - 6.2.19 Ensure no duplicate group names exist (Scored)
    - 6.2.20 Ensure shadow group is empty (Scored)