OpenSCAP Evaluation Report

Guide to the Secure Configuration of Ubuntu 22.04

with profile CIS Ubuntu 22.04 Level 1 Workstation Benchmark

— This baseline aligns to the Center for Internet Security
Ubuntu 22.04 LTS Benchmark, v1.0.0, released 08-30-2022.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide
This guide presents a catalog of security-relevant configuration settings for Ubuntu 22.04. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	pkrvmatcq79t5rz
Benchmark URL	./scap-security-guide-0.1.74/ssg-ubuntu2204-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU_22-04
Profile ID	xccdf_org.ssgproject.content_profile_cis_level1_workstation
Started at	2024-09-20T20:50:22
Finished at	2024-09-20T20:50:55
Performed by	packer

CPE Platforms

- cpe:/o:canonical:ubuntu_linux:22.04::~~lts~~~

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.0.4
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:222:48ff:fe5b:ce0a
- MAC 00:00:00:00:00:00
- MAC 00:22:48:5B:CE:0A

Compliance and Scoring

The target system did not satisfy the conditions of 101 rules! Please review rule results and consider applying remediation.

Rule results

Severity of failed rules

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	66.365211	100.000000	66.37%

Rule Overview

- [x] pass
- [x] fail
- [x] notchecked
- [x] fixed
- [x] error
- [x] notapplicable
- [x] informational
- [x] unknown

Search through XCCDF rules — Search

Group rules by: Default

Title	Severity	Result
▾ Guide to the Secure Configuration of Ubuntu 22.04 101x fail 7x notchecked		
▾ System Settings 72x fail 7x notchecked		
▾ Installing and Maintaining Software 7x fail		
▾ System and Software Integrity 4x fail		

▼ **Software Integrity Checking** 4x fail		
▼ **Verify Integrity with AIDE** 4x fail		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure AIDE to Verify the Audit Tools	medium	fail
Configure Periodic Execution of AIDE	medium	fail
Package "prelink" Must not be Installed	medium	pass
▼ **Disk Partitioning** 1x fail		
Ensure /tmp Located On Separate Partition	low	fail
▶ GNOME Desktop Environment		
▼ **Sudo** 2x fail		
Install sudo Package	medium	pass
Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_pty	medium	pass
Ensure Sudo Logfile Exists - sudo logfile	low	fail
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	medium	pass
Require Re-Authentication When Using the sudo Command	medium	fail
▼ **Account and Access Control** 25x fail		
▼ **Warning Banners for System Accesses** 2x fail		
▶ Implement a GUI Warning Banner		
Modify the System Login Banner	medium	fail
Modify the System Login Banner for Remote Connections	medium	fail
Modify the System Message of the Day Banner	medium	pass
Verify Group Ownership of System Login Banner	medium	pass
Verify Group Ownership of System Login Banner for Remote Connections	medium	pass
Verify Group Ownership of Message of the Day Banner	medium	pass
Verify ownership of System Login Banner	medium	pass
Verify ownership of System Login Banner for Remote Connections	medium	pass
Verify ownership of Message of the Day Banner	medium	pass
Verify permissions on System Login Banner	medium	pass
Verify permissions on System Login Banner for Remote Connections	medium	pass
Verify permissions on Message of the Day Banner	medium	pass
▼ **Protect Accounts by Configuring PAM** 13x fail		
▼ **Set Lockouts for Failed Password Attempts** 4x fail		
Limit Password Reuse	medium	fail
Lock Accounts After Failed Password Attempts	medium	fail
Set Interval For Counting Failed Password Attempts	medium	fail
Set Lockout Time for Failed Password Attempts	medium	fail
▼ **Set Password Quality Requirements** 7x fail		
▼ **Set Password Quality Requirements with pam_pwquality** 7x fail		
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Different Categories	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Length	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Special Characters	medium	fail
Ensure PAM Enforces Password Requirements - Authentication Retry Prompts Permitted Per-Session	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	medium	fail
▼ **Set Password Hashing Algorithm** 1x fail		
Set Password Hashing Algorithm in /etc/login.defs	medium	fail
Install pam_pwquality Package	medium	fail

▼ **Protect Accounts by Restricting Password-Based Login** 6x fail		
▼ **Set Account Expiration Parameters** 1x fail		
Set Account Expiration Following Inactivity	medium	fail
Ensure All Accounts on the System Have Unique Names	medium	pass
Ensure shadow Group is Empty	medium	pass
▼ **Set Password Expiration Parameters** 2x fail		
Set Password Maximum Age	medium	fail
Set Password Minimum Age	medium	fail
Set Existing Passwords Maximum Age	medium	pass
Set Existing Passwords Minimum Age	medium	pass
Set Password Warning Age	medium	pass
▶ Verify Proper Storage and Existence of Password Hashes		
▼ **Restrict Root Logins** 3x fail		
Verify Only Root Has UID 0	high	pass
Verify Root Has A Primary GID 0	high	pass
Ensure the Group Used by pam_wheel.so Module Exists on System and is Empty	medium	fail
Ensure Authentication Required for Single User Mode	medium	fail
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	pass
Enforce Usage of pam_wheel with Group Parameter for su Authentication	medium	fail
Ensure All Accounts on the System Have Unique User IDs	medium	pass
Ensure All Groups on the System Have Unique Group ID	medium	pass
Ensure All Groups on the System Have Unique Group Names	medium	pass
▼ **Secure Session Configuration Files for Login Accounts** 4x fail		
▶ Ensure that No Dangerous Directories Exist in Root's Path		
▼ **Ensure that Users Have Sensible Umask Values** 3x fail		
Ensure the Default Bash Umask is Set Correctly	medium	fail
Ensure the Default Umask is Set Correctly in login.defs	medium	fail
Ensure the Default Umask is Set Correctly in /etc/profile	medium	fail
Ensure the Default Umask is Set Correctly For Interactive Users	medium	pass
Set Interactive Session Timeout	medium	fail
User Initialization Files Must Be Group-Owned By The Primary Group	medium	pass
User Initialization Files Must Not Run World-Writable Programs	medium	pass
User Initialization Files Must Be Owned By the Primary User	medium	pass
All Interactive Users Home Directories Must Exist	medium	pass
All Interactive User Home Directories Must Be Group-Owned By The Primary Group	medium	pass
All Interactive User Home Directories Must Be Owned By The Primary User	medium	pass
All Interactive User Home Directories Must Have mode 0750 Or Less Permissive	medium	pass
▼ **AppArmor** 1x fail		
Ensure AppArmor is installed	medium	pass
All AppArmor Profiles are in enforce or complain mode	medium	pass
Ensure AppArmor is enabled in the bootloader configuration	medium	fail
▼ **GRUB2 bootloader configuration** 2x fail		
▼ **Non-UEFI GRUB2 bootloader configuration** 2x fail		
Verify /boot/grub/grub.cfg User Ownership	medium	pass
Verify /boot/grub/grub.cfg Permissions	medium	fail
Set Boot Loader Password in grub2	high	fail
▶ UEFI GRUB2 bootloader configuration		
▼ **Configure Syslog** 4x fail		
▼ **systemd-journald** 3x fail		
Install systemd-journal-remote Package	medium	fail

Enable systemd-journald Service	medium	pass
Ensure journald is configured to compress large log files	medium	fail
Ensure journald is configured to write log files to persistent disk	medium	fail
Disable systemd-journal-remote Socket	medium	pass
▸ Configure rsyslogd to Accept Remote Messages If Acting as a Log Server		
▾ **Rsyslog Logs Sent To Remote Host** 1x fail		
Ensure Logs Sent To Remote Host	medium	fail
Ensure rsyslog is Installed	medium	pass
Enable rsyslog Service	medium	pass
Ensure rsyslog Default File Permissions Configured	medium	pass
▾ **Network Configuration and Firewalls** 25x fail 7x notchecked		
▸ iptables and ip6tables		
▾ **IPv6** 7x fail		
▾ **Configure IPv6 Settings if Necessary** 7x fail		
Configure Accepting Router Advertisements on All IPv6 Interfaces	medium	fail
Disable Accepting ICMP Redirects for All IPv6 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv6 Interfaces	medium	fail
Disable Kernel Parameter for IPv6 Forwarding	medium	fail
Disable Accepting Router Advertisements on all IPv6 Interfaces by Default	medium	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv6 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv6 Interfaces by Default	medium	fail
▾ **Kernel Parameters Which Affect Networking** 15x fail		
▾ **Network Related Kernel Runtime Parameters for Hosts and Routers** 12x fail		
Disable Accepting ICMP Redirects for All IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv4 Interfaces	medium	fail
Enable Kernel Parameter to Log Martian Packets on all IPv4 Interfaces	unknown	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Secure ICMP Redirects on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv4 Interfaces by Default	medium	pass
Enable Kernel Paremeter to Log Martian Packets on all IPv4 Interfaces by Default	unknown	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces by Default	medium	fail
Configure Kernel Parameter for Accepting Secure Redirects By Default	medium	fail
Enable Kernel Parameter to Ignore ICMP Broadcast Echo Requests on IPv4 Interfaces	medium	fail
Enable Kernel Parameter to Ignore Bogus ICMP Error Responses on IPv4 Interfaces	unknown	fail
Enable Kernel Parameter to Use TCP Syncookies on Network Interfaces	medium	fail
▾ **Network Parameters for Hosts Only** 3x fail		
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces by Default	medium	fail
Disable Kernel Parameter for IP Forwarding on IPv4 Interfaces	medium	fail
▾ **nftables** 2x fail 4x notchecked		
Install nftables Package	medium	notapplicable
Verify nftables Service is Enabled	medium	fail
Ensure nftables Default Deny Firewall Policy	medium	notchecked
Ensure nftables Rules are Permanent	medium	fail
Ensure Base Chains Exist for Nftables	medium	notchecked
Set nftables Configuration for Loopback Traffic	medium	notchecked
Ensure a Table Exists for Nftables	medium	notchecked
▾ **Uncomplicated Firewall (ufw)** 1x fail 3x notchecked		

Remove ufw Package	medium	fail
Verify ufw Enabled	medium	pass
Ensure ufw Default Deny Firewall Policy	medium	notchecked
Set UFW Loopback Traffic	medium	notchecked
Ensure ufw Firewall Rules Exist for All Open Ports	medium	notchecked
File Permissions and Masks 8x fail		
Verify Permissions on Important Files and Directories 1x fail		
Verify Permissions on Files with Local Account Information and Credentials		
Verify File Permissions Within Some Important Directories		
Verify Permissions on /etc/audit/auditd.conf	medium	pass
Verify Permissions on /etc/audit/rules.d/*.rules	medium	pass
Ensure No World-Writable Files Exist	medium	pass
Ensure All Files Are Owned by a Group	medium	pass
Ensure All Files Are Owned by a User	medium	pass
Verify permissions of log files	medium	fail
Restrict Dynamic Mounting and Unmounting of Filesystems 1x fail		
Disable Mounting of cramfs	low	fail
Restrict Partition Mount Options 3x fail		
Add nodev Option to /dev/shm	medium	fail
Add noexec Option to /dev/shm	medium	fail
Add nosuid Option to /dev/shm	medium	fail
Add nodev Option to /home	unknown	notapplicable
Add nosuid Option to /home	medium	notapplicable
Add nodev Option to /tmp	medium	notapplicable
Add noexec Option to /tmp	medium	notapplicable
Add nosuid Option to /tmp	medium	notapplicable
Add nodev Option to /var/log/audit	medium	notapplicable
Add noexec Option to /var/log/audit	medium	notapplicable
Add nosuid Option to /var/log/audit	medium	notapplicable
Add nodev Option to /var/log	medium	notapplicable
Add noexec Option to /var/log	medium	notapplicable
Add nosuid Option to /var/log	medium	notapplicable
Add nodev Option to /var	medium	notapplicable
Add nosuid Option to /var	medium	notapplicable
Add nodev Option to /var/tmp	medium	notapplicable
Add noexec Option to /var/tmp	medium	notapplicable
Add nosuid Option to /var/tmp	medium	notapplicable
Restrict Programs from Dangerous Execution Patterns 3x fail		
Disable Core Dumps 2x fail		
Disable Core Dumps for All Users	medium	fail
Disable Core Dumps for SUID programs	medium	fail
Enable ExecShield 1x fail		
Enable Randomized Layout of Virtual Address Space	medium	fail
Services 29x fail		
Apport Service 1x fail		
Disable Apport Service	unknown	fail
Avahi Server		
Cron and At Daemons 6x fail		
Restrict at and cron to Authorized Users if Necessary		

Enable cron Service	medium	pass
Verify Group Who Owns cron.d	medium	pass
Verify Group Who Owns cron.daily	medium	pass
Verify Group Who Owns cron.hourly	medium	pass
Verify Group Who Owns cron.monthly	medium	pass
Verify Group Who Owns cron.weekly	medium	pass
Verify Group Who Owns Crontab	medium	pass
Verify Owner on cron.d	medium	pass
Verify Owner on cron.daily	medium	pass
Verify Owner on cron.hourly	medium	pass
Verify Owner on cron.monthly	medium	pass
Verify Owner on cron.weekly	medium	pass
Verify Owner on crontab	medium	pass
Verify Permissions on cron.d	medium	fail
Verify Permissions on cron.daily	medium	fail
Verify Permissions on cron.hourly	medium	fail
Verify Permissions on cron.monthly	medium	fail
Verify Permissions on cron.weekly	medium	fail
Verify Permissions on crontab	medium	fail
▶ Deprecated services		
▶ DHCP		
▶ DNS Server		
▶ FTP Server		
▶ Web Server		
▶ IMAP and POP3 Server		
▶ LDAP		
▶ Mail Server Software		
▶ NFS and RPC		
▼ **Network Time Protocol** 1x fail		
Install the systemd_timesyncd Service	high	fail
The Chronyd service is enabled	medium	pass
Enable the NTP Daemon	high	notapplicable
Enable systemd_timesyncd Service	high	notapplicable
Ensure that chronyd is running under chrony user account	medium	pass
Configure server restrictions for ntpd	medium	notapplicable
Configure ntpd To Run As ntp User	medium	notapplicable
▼ **Obsolete Services** 2x fail		
▶ Rlogin, Rsh, and Rexec		
▶ Chat/Messaging Services		
▼ **Telnet** 1x fail		
Remove telnet Clients	low	fail
Uninstall rsync Package	medium	fail
▶ Proxy Server		
▶ Samba(SMB) Microsoft Windows File Sharing Server		
▶ SNMP Server		
▼ **SSH Server** 19x fail		
▼ **Configure OpenSSH Server if Necessary** 18x fail		
Set SSH Client Alive Count Max	medium	fail
Set SSH Client Alive Interval	medium	fail
Disable Host-Based Authentication	medium	fail

Disable SSH Access via Empty Passwords	high	fail
Disable SSH Support for .rhosts Files	medium	fail
Disable SSH Root Login	medium	fail
Disable X11 Forwarding	medium	fail
Do Not Allow SSH Environment Options	medium	fail
Enable PAM	medium	pass
Enable SSH Warning Banner	medium	fail
Limit Users' SSH Access	unknown	fail
Ensure SSH LoginGraceTime is configured	medium	fail
Set LogLevel to INFO	low	fail
Set SSH authentication attempt limit	medium	fail
Set SSH MaxSessions limit	medium	fail
Ensure SSH MaxStartups is configured	medium	fail
Use Only Strong Ciphers	medium	fail
Use Only Strong Key Exchange algorithms	medium	fail
Use Only Strong MACs	medium	fail
Verify Group Who Owns SSH Server config file	medium	pass
Verify Owner on SSH Server config file	medium	pass
Verify Permissions on SSH Server config file	medium	fail
Verify Permissions on SSH Server Private *_key Key Files	medium	pass
Verify Permissions on SSH Server Public *.pub Key Files	medium	pass
▶ System Accounting with auditd		

Show all result details