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	2024-09-20T20:58:18
Finished at	2024-09-20T20:58:38
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 6 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	92.393433	100.000000	92.39%

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 6x fail 4x notchecked		
▼ System Settings 3x fail 4x notchecked		
▼ Installing and Maintaining Software 1x fail		
▶ System and Software Integrity		

▼ **Disk Partitioning** 1x fail		
Ensure /tmp Located On Separate Partition	low	fail
▶ GNOME Desktop Environment		
▶ Sudo		
▼ **Account and Access Control** 1x fail		
▶ Warning Banners for System Accesses		
▶ Protect Accounts by Configuring PAM		
▼ **Protect Accounts by Restricting Password-Based Login** 1x fail		
▶ Set Account Expiration Parameters		
▶ Set Password Expiration Parameters		
▶ Verify Proper Storage and Existence of Password Hashes		
▼ **Restrict Root Logins** 1x 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	pass
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	pass
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		
▶ AppArmor		
▼ **GRUB2 bootloader configuration** 1x fail		
▼ **Non-UEFI GRUB2 bootloader configuration** 1x fail		
Verify /boot/grub/grub.cfg User Ownership	medium	pass
Verify /boot/grub/grub.cfg Permissions	medium	pass
Set Boot Loader Password in grub2	high	fail
▶ UEFI GRUB2 bootloader configuration		
▶ Configure Syslog		
▼ **Network Configuration and Firewalls** 4x notchecked		
▶ iptables and ip6tables		
▶ IPv6		
▶ Kernel Parameters Which Affect Networking		
▼ **nftables** 4x notchecked		
Install nftables Package	medium	pass
Verify nftables Service is Enabled	medium	pass
Ensure nftables Default Deny Firewall Policy	medium	notchecked
Ensure nftables Rules are Permanent	medium	pass
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)		
▶ File Permissions and Masks		
▼ **Services** 3x fail		
▶ Apport Service		
▶ Avahi Server		
▶ Cron and At Daemons		
▶ Deprecated services		

▸ DHCP		
▸ DNS Server		
▸ FTP Server		
▸ Web Server		
▸ IMAP and POP3 Server		
▸ LDAP		
▾ **Mail Server Software** 2x fail		
▾ **Configure SMTP For Mail Clients** 1x fail		
Disable Postfix Network Listening	medium	fail
Ensure Mail Transfer Agent is not Listening on any non-loopback Address	medium	fail
▸ NFS and RPC		
▸ Network Time Protocol		
▸ Obsolete Services		
▸ Proxy Server		
▸ Samba(SMB) Microsoft Windows File Sharing Server		
▸ SNMP Server		
▾ **SSH Server** 1x fail		
▾ **Configure OpenSSH Server if Necessary** 1x fail		
Set SSH Client Alive Count Max	medium	pass
Set SSH Client Alive Interval	medium	pass
Disable Host-Based Authentication	medium	pass
Disable SSH Access via Empty Passwords	high	pass
Disable SSH Support for .rhosts Files	medium	pass
Disable SSH Root Login	medium	pass
Disable X11 Forwarding	medium	pass
Do Not Allow SSH Environment Options	medium	pass
Enable PAM	medium	pass
Enable SSH Warning Banner	medium	pass
Limit Users' SSH Access	unknown	fail
Ensure SSH LoginGraceTime is configured	medium	pass
Set LogLevel to INFO	low	pass
Set SSH authentication attempt limit	medium	pass
Set SSH MaxSessions limit	medium	pass
Ensure SSH MaxStartups is configured	medium	pass
Use Only Strong Ciphers	medium	pass
Use Only Strong Key Exchange algorithms	medium	pass
Use Only Strong MACs	medium	pass
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	pass
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