Guide to the Secure Configuration of Ubuntu 20.04

with profile CIS Ubuntu 20.04 Level 1 Workstation Benchmark
— This baseline aligns to the Center for Internet Security
Ubuntu 20.04 LTS Benchmark, v1.0.0, released 07-21-2020.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide (https://www.open-scap.org/security-policies/scap-security-guide)
This guide presents a catalog of security-relevant configuration settings for Ubuntu 20.04. 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 (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	gn-VirtualBox
Benchmark URL	/home/gn/openscap/build/ssg-ubuntu2004-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU_20-04
Profile ID	xccdf_org.ssgproject.content_profile_cis_level1_workstation
Started at	2025-08-08T00:21:38

Finished at	2025-08-08T00:22:43
Performed by	gn

CPE Platforms

- cpe:/o:canonical:ubuntu_linux:20.04::~~lts~~~

Addresses

- IPv4 127.0.0.1
- IPv6 0:0:0:0:0:0:0:1
- MAC 00:00:00:00:00:00

Compliance and Scoring

The target system did not satisfy the conditions of 6 rules! Furthermore, the results of 19 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

204 passed 6 23 other

Severity of failed rules

0 1 low 4 medium 1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	84.614349	100.000000	84.61%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Ubuntu 20.04 6x fail 16x error 3x unknown 4x notchecked		
System Settings 6x fail 14x error 3x unknown 4x notchecked		
Installing and Maintaining Software 1x fail 3x error		

Title	Severity	Result
System and Software Integrity **1x error**		
Software Integrity Checking **1x error**		
Verify Integrity with AIDE **1x error**		
Install AIDE	medium	**pass**
Build and Test AIDE Database	medium	**pass**
Configure Periodic Execution of AIDE	medium	**error**
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 error**		
Install sudo Package	medium	**pass**
Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_pty	medium	**error**
Ensure Sudo Logfile Exists - sudo logfile	low	**error**
Account and Access Control **1x fail** **5x error** **2x unknown**		
Warning Banners for System Accesses **1x error**		
Implement a GUI Warning Banner		
Modify the System Login Banner	medium	**pass**
Modify the System Login Banner for Remote Connections	medium	**pass**
Modify the System Message of the Day Banner	medium	**error**
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**

Title	Severity	Result
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		
Protect Accounts by Restricting Password-Based Login 3x error		
Set Account Expiration Parameters		
Set Password Expiration Parameters 2x error		
Set Password Maximum Age	medium	pass
Set Password Minimum Age	medium	pass
Set Existing Passwords Maximum Age	medium	error
Set Existing Passwords Minimum Age	medium	error
Set Password Warning Age	medium	pass
Verify Proper Storage and Existence of Password Hashes		
Restrict Root Logins 1x error		
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	error
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

Title	Severity	Result
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 1x fail 1x error 2x unknown		
Ensure that No Dangerous Directories Exist in Root's Path 1x fail		
Ensure that Root's Path Does Not Include World or Group-Writable Directories	medium	fail
Ensure that Users Have Sensible Umask Values 2x unknown		
Ensure the Default Bash Umask is Set Correctly	medium	pass
Ensure the Default C Shell Umask is Set Correctly	medium	unknown
Ensure the Default Umask is Set Correctly in login.defs	medium	pass
Ensure the Default Umask is Set Correctly in /etc/profile	medium	unknown
Ensure the Default Umask is Set Correctly For Interactive Users	medium	pass
Set Interactive Session Timeout	medium	error
User Initialization Files Must Be Group-Owned By The Primary Group	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 unknown		
Ensure AppArmor is installed	medium	pass

Title	Severity	Result
All AppArmor Profiles are in enforce or complain mode	medium	unknown
Ensure AppArmor is enabled in the bootloader configuration	medium	pass
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		
Network Configuration and Firewalls **1x fail** **4x notchecked**		
iptables and ip6tables **4x notchecked**		
Inspect and Activate Default Rules **3x notchecked**		
Set Default ip6tables Policy for Incoming Packets	medium	notchecked
Set configuration for IPv6 loopback traffic	medium	notchecked
Set configuration for loopback traffic	medium	notchecked
Strengthen the Default Ruleset **1x notchecked**		
Set Default iptables Policy for Incoming Packets	medium	notchecked
Install iptables-persistent Package	medium	pass
Install iptables Package	medium	pass
Remove iptables-persistent Package	medium	notapplicable
IPv6		
Kernel Parameters Which Affect Networking		
nftables		
Uncomplicated Firewall (ufw) **1x fail**		
Install ufw Package	medium	fail

Title	Severity	Result
Remove ufw Package	medium	**pass**
Verify ufw Enabled	medium	**notapplicable**
Ensure ufw Default Deny Firewall Policy	medium	**notapplicable**
Set UFW Loopback Traffic	medium	**notapplicable**
File Permissions and Masks **1x fail** **6x error**		
Verify Permissions on Important Files and Directories **1x fail**		
Verify Permissions on Files with Local Account Information and Credentials		
Verify that All World-Writable Directories Have Sticky Bits Set	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 **6x error**		
Disable Mounting of cramfs	low	**error**
Disable Mounting of freevxfs	low	**error**
Disable Mounting of hfs	low	**error**
Disable Mounting of hfsplus	low	**error**
Disable Mounting of jffs2	low	**error**
Disable Mounting of udf	low	**error**
Restrict Partition Mount Options		
Restrict Programs from Dangerous Execution Patterns		
Services **2x error**		
Avahi Server		
Cron and At Daemons		

Title	Severity	Result
Deprecated services		
DHCP		
DNS Server		
FTP Server		
Web Server		
IMAP and POP3 Server		
LDAP		
Mail Server Software **1x error**		
Configure SMTP For Mail Clients **1x error**		
Disable Postfix Network Listening	medium	**error**
Ensure Mail Transfer Agent is not Listening on any non-loopback Address	medium	**pass**
NFS and RPC		
Network Time Protocol		
Obsolete Services		
Print Support		
Proxy Server		
Samba(SMB) Microsoft Windows File Sharing Server		
SNMP Server		
SSH Server **1x error**		
Configure OpenSSH Server if Necessary **1x error**		
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**

Title	Severity	Result
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	**error**
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 FIPS 140-2 Validated Ciphers	medium	**pass**
Use Only FIPS 140-2 Validated MACs	medium	**pass**
Use Only Strong Key Exchange algorithms	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**