

Guide to the Secure Configuration of Ubuntu 20.04

with profile CIS Ubuntu 20.04 Level 2 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 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_level2_workstation
Started at	2025-07-20T11:56:39

Finished at	2025-07-20T11:59:33
Performed by	gn

CPE Platforms

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

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.1.14
- IPv6 0:0:0:0:0:0:1
- IPv6 fd17:625c:f037:a801:1a4d:32d6:d507:5b29
- IPv6 fd17:625c:f037:a801:d566:bfaa:ac43:2113
- IPv6 fe80:0:0:0:a655:43b5:2972:e162
- MAC 00:00:00:00:00:00
- MAC 08:00:27:47:ED:FA

Compliance and Scoring

The target system did not satisfy the conditions of 104 rules! Furthermore, the results of 6 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

134 passed

104 failed

9

Severity of failed rules

6 other

16 low

80 medium

2

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	40.078323	100.000000	40.08%

Rule Overview

Title	Severity			Result
<div> <div>Guide to the Secure Configuration of Ubuntu 20.04</div> <div>104x fail</div> <div>5x error</div> <div>1x unknown</div> <div>3x notchecked</div> </div>				
<div> <div>System Settings</div> <div>87x fail</div> <div>5x error</div> <div>1x unknown</div> <div>3x notchecked</div> </div>				

Title	Severity	Result
Installing and Maintaining Software 11x fail 2x error		
System and Software Integrity 3x fail		
Software Integrity Checking 3x fail		
Verify Integrity with AIDE 3x fail		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure Periodic Execution of AIDE	medium	fail
Package "prelink" Must not be Installed	medium	pass
Disk Partitioning 6x fail		
Ensure /home Located On Separate Partition	low	fail
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
Ensure /var/tmp Located On Separate Partition	medium	fail
GNOME Desktop Environment 2x fail		
Configure GNOME Login Screen 1x fail		
Disable the GNOME3 Login User List	medium	fail
Configure GNOME3 DConf User Profile	high	fail
Sudo 2x error		
Install sudo Package	medium	pass
Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_ptty	medium	error
Ensure Sudo Logfile Exists - sudo logfile	low	error
Account and Access Control 26x fail 3x error		
Warning Banners for System Accesses 4x fail		
Implement a GUI Warning Banner 2x fail		

Title	Severity	Result
Enable GNOME3 Login Warning Banner	medium	fail
Set the GNOME3 Login Warning Banner Text	medium	fail
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 10x fail		
Set Lockouts for Failed Password Attempts 2x fail		
Limit Password Reuse	medium	fail
Set Deny 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

Title	Severity	Result
Ensure PAM Enforces Password Requirements - Minimum Different Categories	medium	<u>fail</u>
Ensure PAM Enforces Password Requirements - Minimum Length	medium	<u>fail</u>
Ensure PAM Enforces Password Requirements - Minimum Special Characters	medium	<u>fail</u>
Ensure PAM Enforces Password Requirements - Authentication Retry Prompts Permitted Per-Session	medium	<u>fail</u>
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	medium	<u>fail</u>
Install pam_pwquality Package	medium	<u>fail</u>
Protect Accounts by Restricting Password-Based Login 5x fail 3x error		
Set Account Expiration Parameters 1x fail		
Set Account Expiration Following Inactivity	medium	<u>fail</u>
Ensure All Accounts on the System Have Unique Names	medium	<u>pass</u>
Ensure shadow Group is Empty	medium	<u>pass</u>
Set Password Expiration Parameters 2x fail 2x error		
Set Password Maximum Age	medium	<u>fail</u>
Set Password Minimum Age	medium	<u>fail</u>
Set Existing Passwords Maximum Age	medium	<u>error</u>
Set Existing Passwords Minimum Age	medium	<u>error</u>
Set Password Warning Age	medium	<u>pass</u>
Verify Proper Storage and Existence of Password Hashes		
Restrict Root Logins 2x fail 1x error		
Verify Only Root Has UID 0	high	<u>pass</u>
Verify Root Has A Primary GID 0	high	<u>pass</u>
Ensure the Group Used by pam_wheel.so Module Exists on System and is Empty	medium	<u>fail</u>

Title	Severity	Result
Ensure Authentication Required for Single User Mode	medium	<u>error</u>
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	<u>pass</u>
Enforce Usage of pam_wheel with Group Parameter for su Authentication	medium	<u>fail</u>
Ensure All Accounts on the System Have Unique User IDs	medium	<u>pass</u>
Ensure All Groups on the System Have Unique Group ID	medium	<u>pass</u>
Ensure All Groups on the System Have Unique Group Names	medium	<u>pass</u>
Secure Session Configuration Files for Login Accounts 7x fail		
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	<u>fail</u>
Ensure that Users Have Sensible Umask Values 4x fail		
Ensure the Default Bash Umask is Set Correctly	medium	<u>fail</u>
Ensure the Default C Shell Umask is Set Correctly	medium	<u>fail</u>
Ensure the Default Umask is Set Correctly in login.defs	medium	<u>fail</u>
Ensure the Default Umask is Set Correctly in /etc/profile	medium	<u>fail</u>
Ensure the Default Umask is Set Correctly For Interactive Users	medium	<u>pass</u>
Set Interactive Session Timeout	medium	<u>fail</u>
User Initialization Files Must Be Group-Owned By The Primary Group	medium	<u>pass</u>
User Initialization Files Must Be Owned By the Primary User	medium	<u>pass</u>
All Interactive Users Home Directories Must Exist	medium	<u>pass</u>

Title	Severity	Result
All Interactive User Home Directories Must Be Group-Owned By The Primary Group	medium	<u>pass</u>
All Interactive User Home Directories Must Be Owned By The Primary User	medium	<u>pass</u>
All Interactive User Home Directories Must Have mode 0750 Or Less Permissive	medium	<u>fail</u>
AppArmor 1x fail 1x unknown 1x notchecked		
Ensure AppArmor is installed	medium	<u>pass</u>
Enforce all AppArmor Profiles	medium	<u>notchecked</u>
All AppArmor Profiles are in enforce or complain mode	medium	<u>unknown</u>
Ensure AppArmor is enabled in the bootloader configuration	medium	<u>fail</u>
GRUB2 bootloader configuration 2x fail		
Non-UEFI GRUB2 bootloader configuration 2x fail		
Verify /boot/grub/grub.cfg User Ownership	medium	<u>pass</u>
Verify /boot/grub/grub.cfg Permissions	medium	<u>fail</u>
Set Boot Loader Password in grub2	high	<u>fail</u>
UEFI GRUB2 bootloader configuration		
Configure Syslog 4x fail		
systemd-journald 3x fail		
Ensure journald is configured to compress large log files	medium	<u>fail</u>
Ensure journald is configured to send logs to rsyslog	medium	<u>fail</u>
Ensure journald is configured to write log files to persistent disk	medium	<u>fail</u>
Rsyslog Logs Sent To Remote Host 1x fail		
Ensure Logs Sent To Remote Host	medium	<u>fail</u>
Ensure rsyslog is Installed	medium	<u>pass</u>
Enable rsyslog Service	medium	<u>pass</u>

Title	Severity	Result
Ensure rsyslog Default File Permissions Configured	medium	<u>pass</u>
Network Configuration and Firewalls 29x fail 2x notchecked		
iptables and ip6tables 1x fail		
Inspect and Activate Default Rules		
Strengthen the Default Ruleset		
Install iptables-persistent Package	medium	<u>fail</u>
Install iptables Package	medium	<u>notapplicable</u>
Remove iptables-persistent Package	medium	<u>pass</u>
IPv6 7x fail		
Configure IPv6 Settings if Necessary 7x fail		
Configure Accepting Router Advertisements on All IPv6 Interfaces	medium	<u>fail</u>
Disable Accepting ICMP Redirects for All IPv6 Interfaces	medium	<u>fail</u>
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv6 Interfaces	medium	<u>fail</u>
Disable Kernel Parameter for IPv6 Forwarding	medium	<u>fail</u>
Disable Accepting Router Advertisements on all IPv6 Interfaces by Default	medium	<u>fail</u>
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv6 Interfaces	medium	<u>fail</u>
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv6 Interfaces by Default	medium	<u>fail</u>
Kernel Parameters Which Affect Networking 16x fail		
Network Related Kernel Runtime Parameters for Hosts and Routers 13x fail		
Disable Accepting ICMP Redirects for All IPv4 Interfaces	medium	<u>fail</u>
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv4 Interfaces	medium	<u>fail</u>
Enable Kernel Parameter to Log Martian Packets on all IPv4 Interfaces	unknown	<u>fail</u>

Title	Severity	Result
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	fail
Enable Kernel Parameter 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		
Uncomplicated Firewall (ufw) 1x fail 2x notchecked		
Install ufw Package	medium	pass
Remove ufw Package	medium	fail
Verify ufw Enabled	medium	pass

Title	Severity	Result
Ensure ufw Default Deny Firewall Policy	medium	<u>notchecked</u>
Set UFW Loopback Traffic	medium	<u>notchecked</u>
Uncommon Network Protocols 4x fail		
Disable DCCP Support	medium	<u>fail</u>
Disable RDS Support	low	<u>fail</u>
Disable SCTP Support	medium	<u>fail</u>
Disable TIPC Support	low	<u>fail</u>
Wireless Networking		
File Permissions and Masks 14x fail		
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	<u>pass</u>
Ensure No World-Writable Files Exist	medium	<u>pass</u>
Ensure All Files Are Owned by a Group	medium	<u>pass</u>
Ensure All Files Are Owned by a User	medium	<u>pass</u>
Verify permissions of log files	medium	<u>fail</u>
Restrict Dynamic Mounting and Unmounting of Filesystems 7x fail		
Disable the Automounter	medium	<u>notapplicable</u>
Disable Mounting of cramfs	low	<u>fail</u>
Disable Mounting of freevxfs	low	<u>fail</u>
Disable Mounting of hfs	low	<u>fail</u>
Disable Mounting of hfsplus	low	<u>fail</u>
Disable Mounting of jffs2	low	<u>fail</u>
Disable Mounting of udf	low	<u>fail</u>
Disable Modprobe Loading of USB Storage Driver	medium	<u>fail</u>
Restrict Partition Mount Options 3x fail		

Title	Severity	Result
Add nodev Option to /dev/shm	medium	<u>fail</u>
Add noexec Option to /dev/shm	medium	<u>fail</u>
Add nosuid Option to /dev/shm	medium	<u>fail</u>
Add nodev Option to /home	unknown	<u>notapplicable</u>
Add nodev Option to /tmp	medium	<u>notapplicable</u>
Add noexec Option to /tmp	medium	<u>notapplicable</u>
Add nosuid Option to /tmp	medium	<u>notapplicable</u>
Add nodev Option to /var/tmp	medium	<u>notapplicable</u>
Add noexec Option to /var/tmp	medium	<u>notapplicable</u>
Add nosuid Option to /var/tmp	medium	<u>notapplicable</u>
Restrict Programs from Dangerous Execution Patterns 3x fail		
Disable Core Dumps 2x fail		
Disable Core Dumps for All Users	medium	<u>fail</u>
Disable Core Dumps for SUID programs	medium	<u>fail</u>
Enable ExecShield 1x fail		
Enable Randomized Layout of Virtual Address Space	medium	<u>fail</u>
Services 14x fail		
Avahi Server 2x fail		
Disable Avahi Server if Possible 2x fail		
Uninstall avahi Server Package	medium	<u>fail</u>
Disable Avahi Server Software	medium	<u>fail</u>
Cron and At Daemons 6x fail		
Restrict at and cron to Authorized Users if Necessary		
Enable cron Service	medium	<u>pass</u>
Verify Group Who Owns cron.d	medium	<u>pass</u>
Verify Group Who Owns cron.daily	medium	<u>pass</u>

Title	Severity	Result
Verify Group Who Owns cron.hourly	medium	<u>pass</u>
Verify Group Who Owns cron.monthly	medium	<u>pass</u>
Verify Group Who Owns cron.weekly	medium	<u>pass</u>
Verify Group Who Owns Crontab	medium	<u>pass</u>
Verify Owner on cron.d	medium	<u>pass</u>
Verify Owner on cron.daily	medium	<u>pass</u>
Verify Owner on cron.hourly	medium	<u>pass</u>
Verify Owner on cron.monthly	medium	<u>pass</u>
Verify Owner on cron.weekly	medium	<u>pass</u>
Verify Owner on crontab	medium	<u>pass</u>
Verify Permissions on cron.d	medium	<u>fail</u>
Verify Permissions on cron.daily	medium	<u>fail</u>
Verify Permissions on cron.hourly	medium	<u>fail</u>
Verify Permissions on cron.monthly	medium	<u>fail</u>
Verify Permissions on cron.weekly	medium	<u>fail</u>
Verify Permissions on crontab	medium	<u>fail</u>
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		
The Chrony package is installed	medium	<u>fail</u>

Title	Severity	Result
The Chronyd service is enabled	medium	<u>notapplicable</u>
Enable the NTP Daemon	high	<u>notapplicable</u>
Enable systemd_timesyncd Service	high	<u>pass</u>
A remote time server for Chrony is configured	medium	<u>notapplicable</u>
Ensure that chronyd is running under chrony user account	medium	<u>notapplicable</u>
Configure server restrictions for ntpd	medium	<u>notapplicable</u>
Configure ntpd To Run As ntp User	medium	<u>notapplicable</u>
Obsolete Services 2x fail		
Xinetd		
Rlogin, Rsh, and Rexec		
Chat/Messaging Services		
Telnet 1x fail		
Remove telnet Clients	low	<u>fail</u>
Uninstall rsync Package	medium	<u>fail</u>
Print Support 2x fail		
Uninstall CUPS Package	unknown	<u>fail</u>
Disable the CUPS Service	unknown	<u>fail</u>
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	<u>pass</u>
Set SSH Client Alive Interval	medium	<u>pass</u>
Disable Host-Based Authentication	medium	<u>pass</u>
Disable SSH Access via Empty Passwords	high	<u>pass</u>

Title	Severity	Result
Disable SSH Support for .rhosts Files	medium	<u>pass</u>
Disable SSH Root Login	medium	<u>pass</u>
Disable SSH TCP Forwarding	medium	<u>pass</u>
Disable X11 Forwarding	medium	<u>pass</u>
Do Not Allow SSH Environment Options	medium	<u>pass</u>
Enable PAM	medium	<u>pass</u>
Enable SSH Warning Banner	medium	<u>pass</u>
Limit Users' SSH Access	unknown	<u>fail</u>
Ensure SSH LoginGraceTime is configured	medium	<u>pass</u>
Set LogLevel to INFO	low	<u>pass</u>
Set SSH authentication attempt limit	medium	<u>pass</u>
Set SSH MaxSessions limit	medium	<u>pass</u>
Ensure SSH MaxStartups is configured	medium	<u>pass</u>
Use Only FIPS 140-2 Validated Ciphers	medium	<u>pass</u>
Use Only FIPS 140-2 Validated MACs	medium	<u>pass</u>
Use Only Strong Key Exchange algorithms	medium	<u>pass</u>
Verify Group Who Owns SSH Server config file	medium	<u>pass</u>
Verify Owner on SSH Server config file	medium	<u>pass</u>
Verify Permissions on SSH Server config file	medium	<u>pass</u>
Verify Permissions on SSH Server Private *_key Key Files	medium	<u>pass</u>
Verify Permissions on SSH Server Public *.pub Key Files	medium	<u>pass</u>
System Accounting with auditd 3x fail		
Configure auditd Rules for Comprehensive Auditing		
Configure auditd Data Retention		
Ensure the audit Subsystem is Installed	medium	<u>fail</u>

Title	Severity	Result
Enable auditd Service	medium	<u>notapplicable</u>
Enable Auditing for Processes Which Start Prior to the Audit Daemon	low	<u>fail</u>
Extend Audit Backlog Limit for the Audit Daemon	low	<u>fail</u>

Red Hat and Red Hat Enterprise Linux are either registered trademarks or trademarks of Red Hat, Inc. in the United States and other countries. All other names are registered trademarks or trademarks of their respective companies.

Generated using OpenSCAP (<http://open-scap.org>) 1.2.16