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	2025-07-20T11:53:16

Finished at	2025-07-20T11:56:35
Performed by	gn

CPE Platforms

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

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.1.14
- IPv6 0:0:0:0:0:0:0:1
- 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 90 rules! Furthermore, the results of 6 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

132 passed 90 failed 8

Severity of failed rules

5 8 low 75 medium 2

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	59.980213	100.000000	59.98%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Ubuntu 20.04 **90x fail** **5x error** **1x unknown** **2x notchecked**		
System Settings **77x fail** **5x error** **1x unknown** **2x notchecked**		

Title	Severity	Result
Installing and Maintaining Software **6x 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 **1x fail**		
Ensure /tmp Located On Separate Partition	low	**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_pty	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**		
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**

Title	Severity	Result
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**
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**

Title	Severity	Result
Ensure PAM Enforces Password Requirements - Authentication Retry Prompts Permitted Per-Session	medium	**fail**
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	medium	**fail**
Install pam_pwquality Package	medium	**fail**
Protect Accounts by Restricting Password-Based Login **5x fail** **3x error**		
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** **2x error**		
Set Password Maximum Age	medium	**fail**
Set Password Minimum Age	medium	**fail**
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 **2x fail** **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	**fail**
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	**fail**

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 **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	**fail**
Ensure that Users Have Sensible Umask Values **4x fail**		
Ensure the Default Bash Umask is Set Correctly	medium	**fail**
Ensure the Default C Shell 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 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	**fail**

Title	Severity	Result
AppArmor 1x fail 1x unknown		
Ensure AppArmor is installed	medium	**pass**
All AppArmor Profiles are in enforce or complain mode	medium	**unknown**
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		
Ensure journald is configured to compress large log files	medium	**fail**
Ensure journald is configured to send logs to rsyslog	medium	**fail**
Ensure journald is configured to write log files to persistent disk	medium	**fail**
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 2x notchecked		
iptables and ip6tables 1x fail		
Inspect and Activate Default Rules		
Strengthen the Default Ruleset		
Install iptables-persistent Package	medium	**fail**

Title	Severity	Result
Install iptables Package	medium	**notapplicable**
Remove iptables-persistent Package	medium	**pass**
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 **16x fail**		
Network Related Kernel Runtime Parameters for Hosts and Routers **13x 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**

Title	Severity	Result
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv4 Interfaces by Default	medium	**fail**
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		
Uncomplicated Firewall (ufw) **1x fail** **2x notchecked**		
Install ufw Package	medium	**pass**
Remove ufw Package	medium	**fail**
Verify ufw Enabled	medium	**pass**
Ensure ufw Default Deny Firewall Policy	medium	**notchecked**
Set UFW Loopback Traffic	medium	**notchecked**
File Permissions and Masks **13x fail**		
Verify Permissions on Important Files and Directories **1x fail**		
Verify Permissions on Files with Local Account Information and Credentials		

Title	Severity	Result
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 fail**		
Disable Mounting of cramfs	low	**fail**
Disable Mounting of freevxfs	low	**fail**
Disable Mounting of hfs	low	**fail**
Disable Mounting of hfsplus	low	**fail**
Disable Mounting of jffs2	low	**fail**
Disable Mounting of udf	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 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/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**

Title	Severity	Result
Disable Core Dumps for SUID programs	medium	**fail**
Enable ExecShield **1x fail**		
Enable Randomized Layout of Virtual Address Space	medium	**fail**
Services **13x fail**		
Avahi Server **2x fail**		
Disable Avahi Server if Possible **2x fail**		
Uninstall avahi Server Package	medium	**fail**
Disable Avahi Server Software	medium	**fail**
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**

Title	Severity	Result
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**		
The Chrony package is installed	medium	**fail**
The Chronyd service is enabled	medium	**notapplicable**
Enable the NTP Daemon	high	**notapplicable**
Enable systemd_timesyncd Service	high	**pass**
A remote time server for Chrony is configured	medium	**notapplicable**
Ensure that chronyd is running under chrony user account	medium	**notapplicable**
Configure server restrictions for ntpd	medium	**notapplicable**
Configure ntpd To Run As ntp User	medium	**notapplicable**
Obsolete Services **2x fail**		
Xinetd		
Rlogin, Rsh, and Rexec		
Chat/Messaging Services		
Telnet **1x fail**		

Title	Severity	Result
Remove telnet Clients	low	**fail**
Uninstall rsync Package	medium	**fail**
Print Support **1x fail**		
Uninstall CUPS Package	unknown	**fail**
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 FIPS 140-2 Validated Ciphers	medium	**pass**
Use Only FIPS 140-2 Validated MACs	medium	**pass**

Title	Severity	Result
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**

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