



LibreOffice Conf.
Asia
UbuCon Asia 2023



Surakarta | October, 8th 2023



UBUNTU SECURITY BEST PRACTICE

LERN HOW TO IMPLEMENT SECURITY ON LINUX

Yusuf Hadiwinata Sutandar
yusuf@biznetgio.com

<https://www.biznetgio.com>
<https://louca.id>



Yusuf Hadiwinata S.

Linux Geek, Opensource Enthusiast, Security Hobbies

RHCT, RHCSAv5-v7, RHCEv5-v7, RHCVA, RHCI, RHCX, RHCSA-RHOS, RHCJA, CEI, CEH, CHFI, CND, EDRP, CCNA, MCTCNA, Security+, Network+, VCA, vExpert 2017-2018

Vice President Operation & Services – PT Biznet Gio Nusantara





CYBER SECURITY 101

An Introduction about Cyber Security
Perimeter in general

1

2

LINUX SECURITY

Learn more about security Principal on
Linux Operating System

HARDENING

Deep dive learn about security
implementation on Ubuntu Operating System

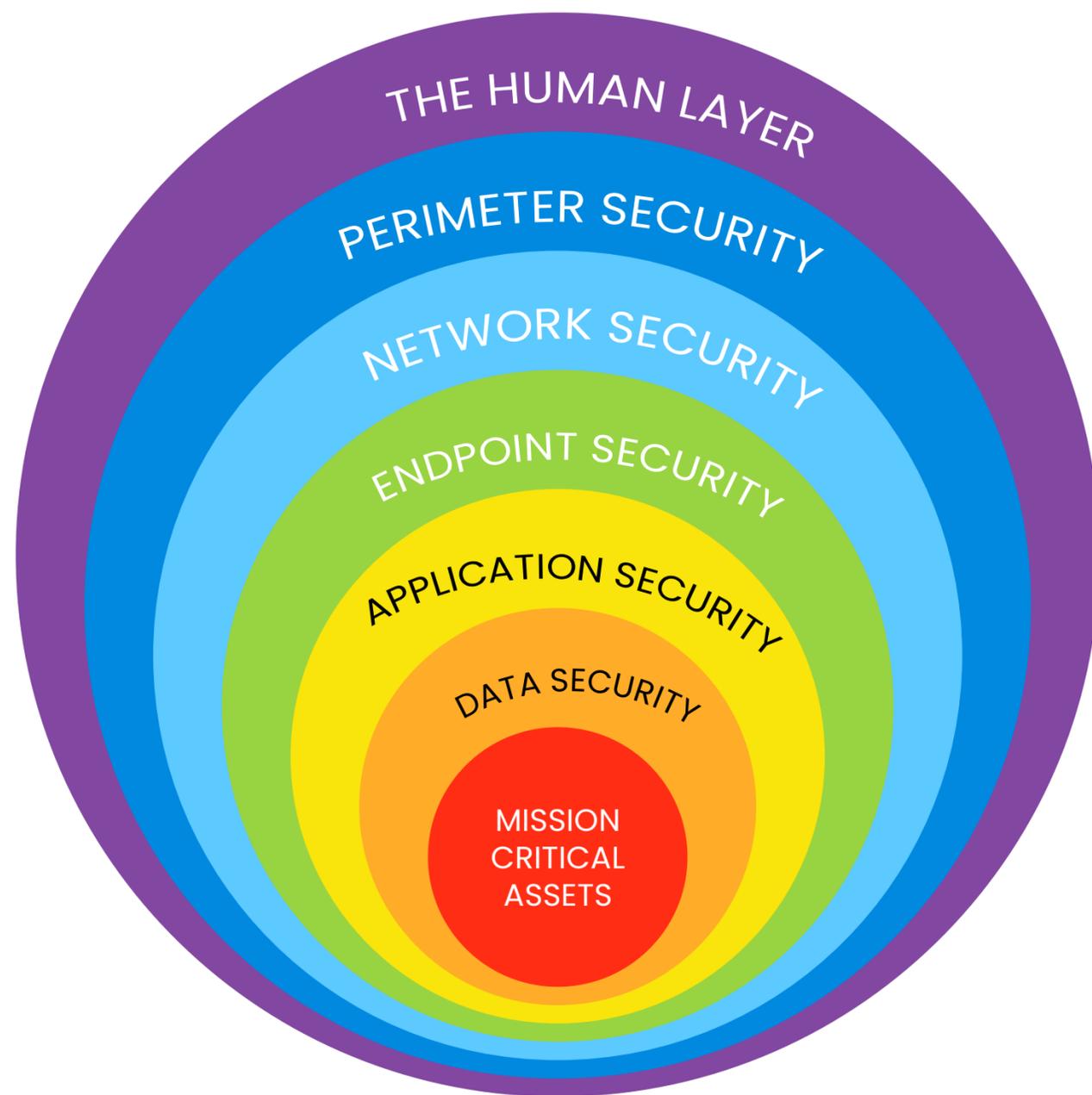
3

4

Q & A

Ask a question and win merchandize
from Biznet Gio

CYBER SECURITY 101



1

Human Layer: Training

2

Perimeter: Firewalls, Spamfilters,
Intrusion Detection / Prevention

3

Network: Secure Design & Topology,
VLANs, Multi-Layer Firewalls/Switchers

4

Endpoint: Anti-virus, Software Firewalls,
Breach Detection Agents

5

Application: Patching, Updates

6

Data: Encryption at rest and in motion

7

Mission Critical: Backups, Response and
Recovery Plans

1

Human Layer: Training

Security awareness training is a **strategy used by IT and security professionals** to prevent and mitigate user risk. These programs are designed **to help users and employees understand the role** they play in helping to combat information security breaches.

Ex: Certified Secure Computer User (CSCU)

PHISHING BERKEDOK HADIAH

Media yang sering digunakan

- SMS
- Telepon
- Aplikasi chat

Tahapan phishing berkedok hadiah

INVESTIGATE Penjahat siber menginvestigasi calon korban dan membuat cerita undian berhadiah palsu yang diputarbalikkan faktanya

Penjahat siber menghubungi korban dan mendesak untuk segera klaim hadiah dengan memberikan data pribadi (nomor kartu ATM, PIN, OTP) pada website atau form

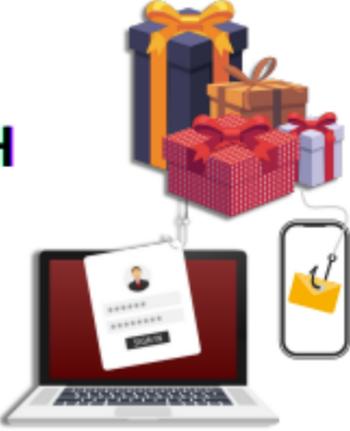
HOOK

Setelah data pribadi didapatkan, maka penjahat siber segera membobol rekening atau dompet digital milik korban

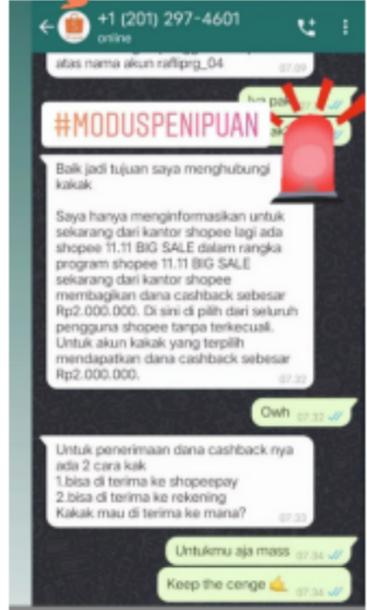
PLAY

Setelah itu, penjahat siber mengakhiri komunikasi dengan cara yang natural, sehingga korban tidak curiga

EXIT



Nomor negara Amerika Serikat, tepatnya New Jersey



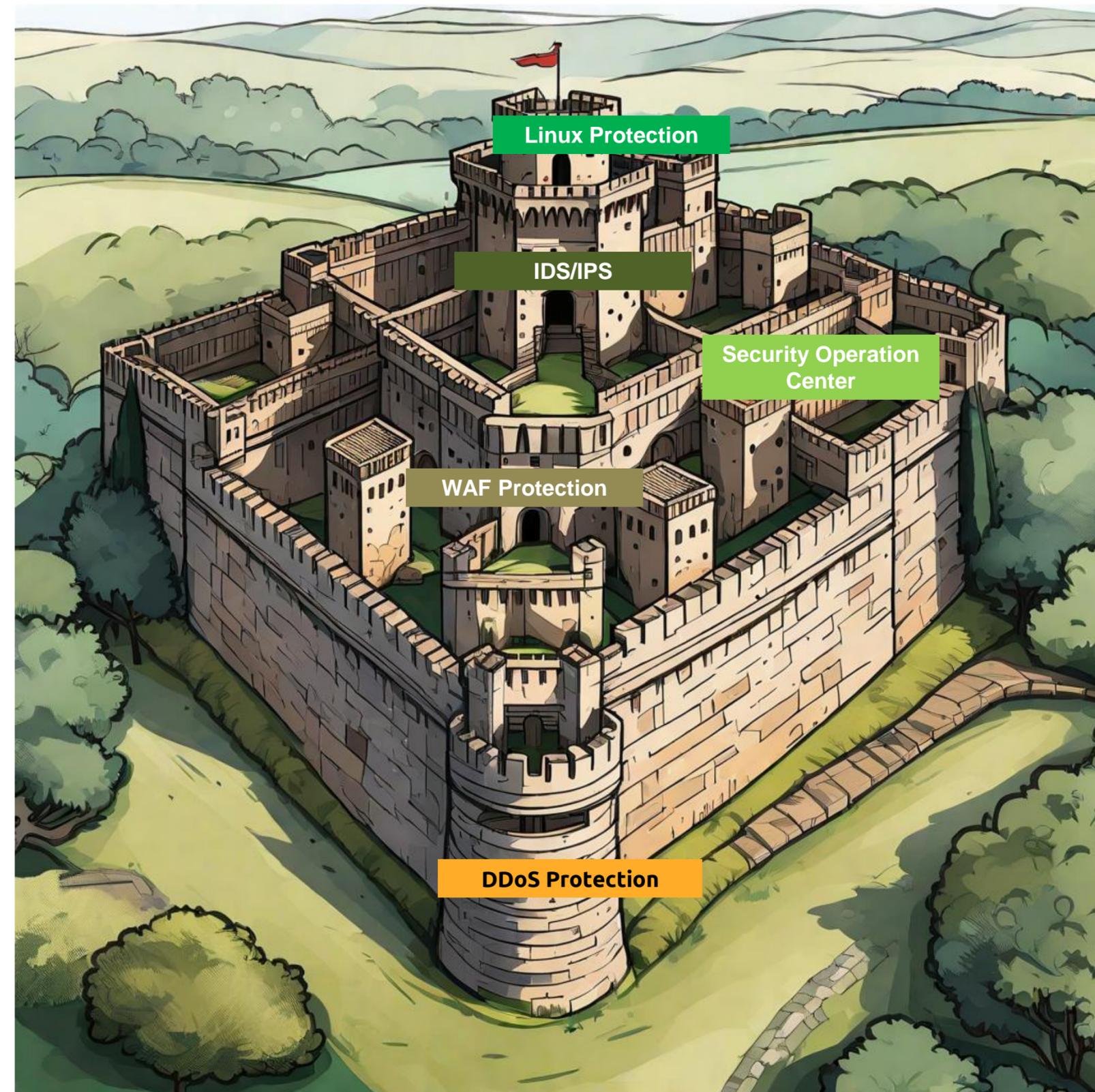
Sumber gambar:
<https://medantalk.com/modus-penipuan-pesanan-whatsapp-mengatasnamakan-shopee-biasanya-dimiring-iming-hadiah-nanti/>

Pencegahan

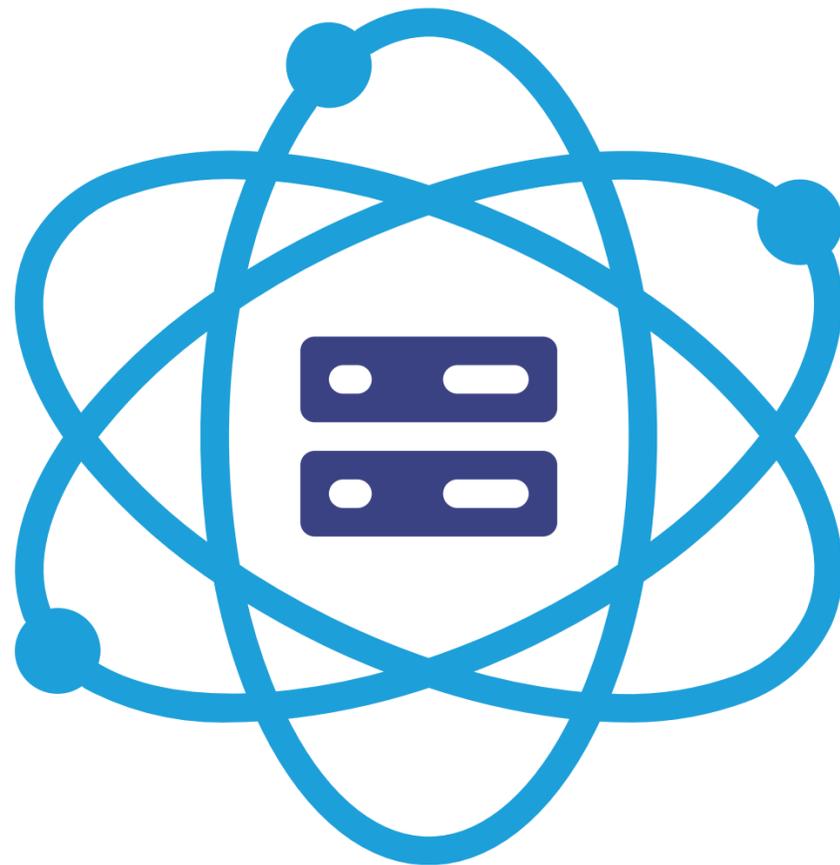
1. Jika Anda tidak pernah mengikuti undian, maka secara logika Anda tidak akan memenangkan undian apapun. Jika Anda menerima informasi memenangkan undian, maka informasi tersebut adalah informasi yang tidak benar.
2. Jika Anda ragu-ragu, hubungi pihak yang resmi melalui kontak yang resmi.

2 Perimeter: Firewalls, Spamfilter, Intrusion Detection/Prevention, WAF, etc

The perimeter layer stops most attackers.
It stops the spam, the petty thief, the automatic scanning tools ran by anonymous curious cats



LINUX SECURITY



Know your system(s)

The first principle is about knowing what your system is supposed to do.

What is its primary role, what software packages does it need and who needs access?

Security Measures:

- Password policy
- Proper software patch management
- Configuration management
- Documentation

LINUX SECURITY

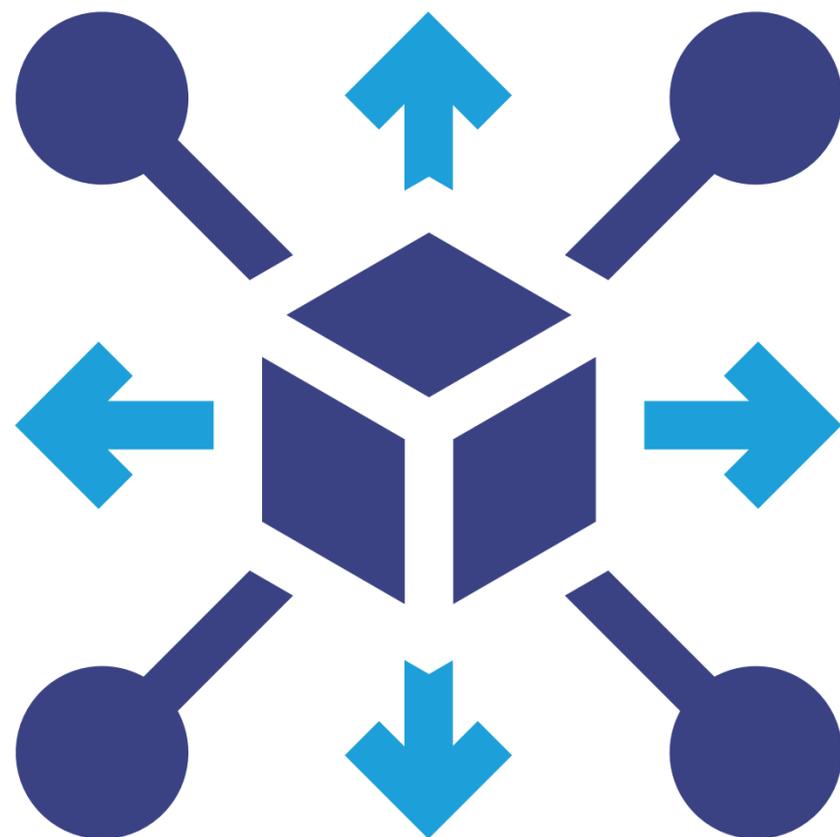
Least Amount of Privilege

Each process running, or package installed, might become a target. Security professionals call this the “**attack surface**”.

What you want is to minimize this attack surface by removing unneeded components, limit access and by default use a “deny unless” strategy.

Security Measures:

- Use minimal/basic installation
- Only allow access to people who really need it



Perform Defense in Depth



Protect the system by applying several layers of security. This principle is named “**defense in depth**” and can be compared with an onion: to get to the core, you have to peel of **layer by layer**. One broken defense might help us protect against full compromise.

Security Measures:

- IPtables / Nftables
- Hardening of software components

LINUX SECURITY

Protection is Key, Detection is a Must



Security focuses on the protection of assets. While this is a primary objective, we should consider that one day our defenses are broken.

Therefore we want to know this as soon as possible, so we can properly act. This is where principle 3 and 4 both are linked. **Set-up proper detection methods, similar to the trip wires used by the military.**

Security Measures:

- Linux audit framework
- Remote Logging
- Create backups and test them

LINUX SECURITY



Know your Enemy

You can only protect a system the right way.
If you know what threats you are facing.

Why would this system be a target and who would be targeting it?

Perform a risk analysis and determine what potential threats your system might endure.

CIS HARDENING

CIS compliance with Ubuntu Pro Plan

Ubuntu contains native tooling to automate compliance and auditing with the Center for Internet Security (CIS) benchmarks.

The Center for Internet Security (CIS), develops the CIS benchmark documents for Ubuntu LTS releases. As these documents contain a large number of hardening rules, compliance and auditing can be very efficient when using the Ubuntu native tooling that is **available to subscribers of Ubuntu Pro.**

With Ubuntu 20.04 we introduce the **Ubuntu Security Guide (USG)** an easy to use tool **for compliance and auditing that replaces our older tooling.** See the following sections for more information.

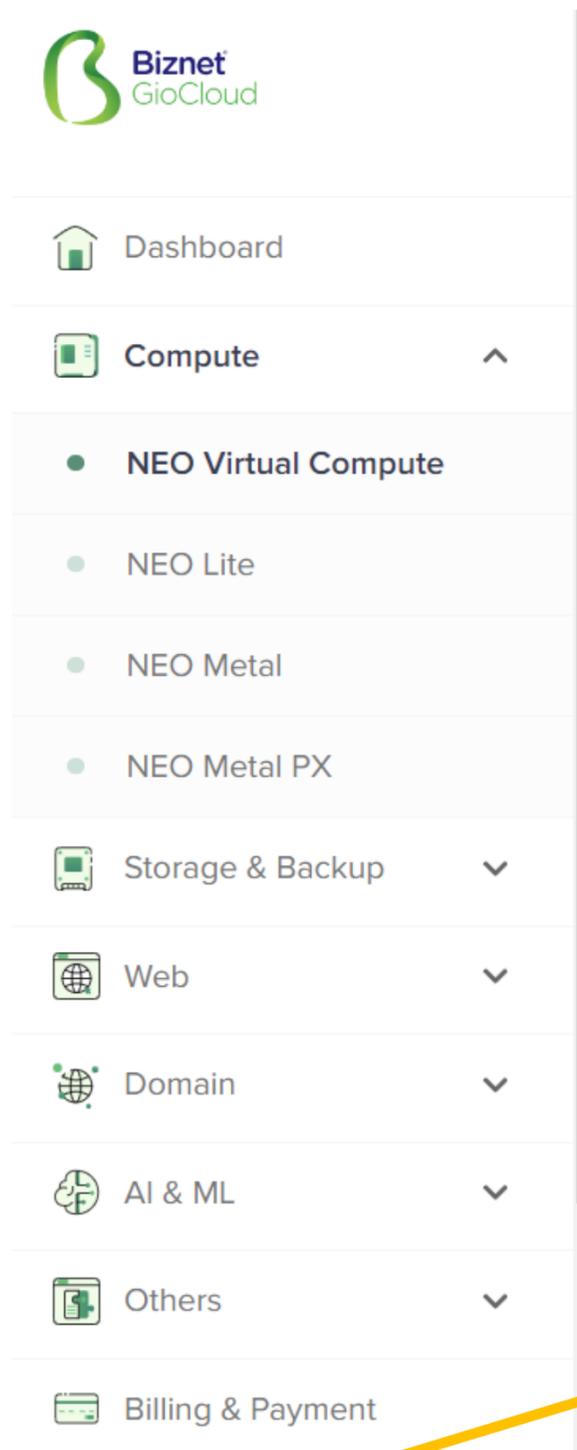


PROFILE NAME	CORRESPONDING CIS PROFILE
<code>cis_level1_workstation</code>	Level 1 Workstation profile
<code>cis_level1_server</code>	Level 1 Server profile
<code>cis_level2_workstation</code>	Level 2 Workstation profile
<code>cis_level2_server</code>	Level 2 Server profile

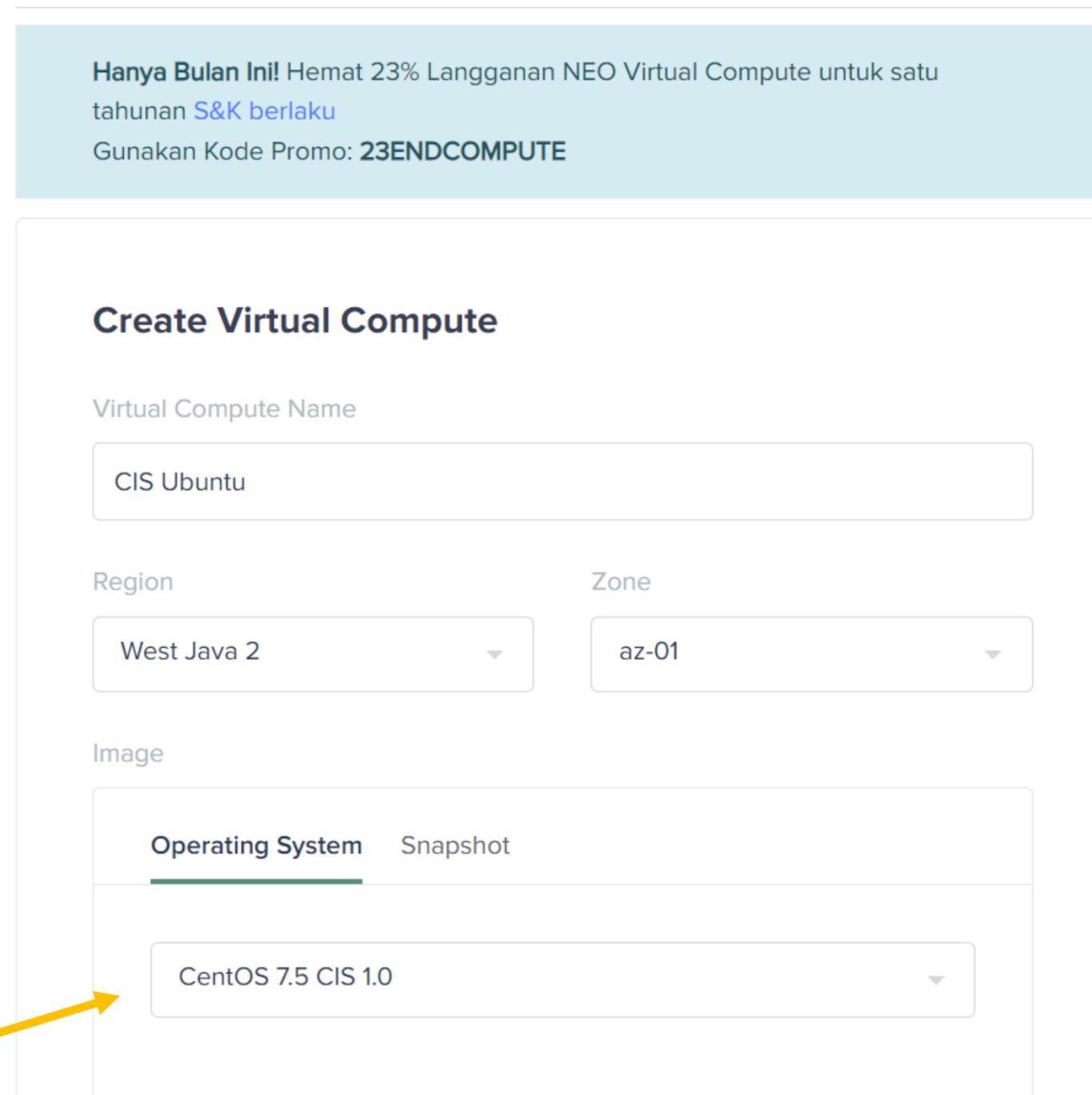
CIS HARDENING

Use Cloud Provider CIS Image

Many cloud provider like Biznet Gio Cloud provide CIS Hardened image, this is the easy way to use Secure Image in the Cloud Environment



The screenshot shows the Biznet GioCloud dashboard. The top left features the Biznet GioCloud logo. Below it is a navigation menu with the following items: Dashboard, Compute (with an upward arrow), NEO Virtual Compute (selected with a green dot), NEO Lite, NEO Metal, NEO Metal PX, Storage & Backup (with a downward arrow), Web (with a downward arrow), Domain (with a downward arrow), AI & ML (with a downward arrow), Others (with a downward arrow), and Billing & Payment (with a downward arrow).



The screenshot shows the 'Create Virtual Compute' form. At the top, there is a promotional banner: 'Hanya Bulan Ini! Hemat 23% Langganan NEO Virtual Compute untuk satu tahunan S&K berlaku. Gunakan Kode Promo: 23ENDCOMPUTE'. The form fields are: 'Virtual Compute Name' with the value 'CIS Ubuntu'; 'Region' with the value 'West Java 2'; 'Zone' with the value 'az-01'; and 'Image' with the value 'CentOS 7.5 CIS 1.0'. The 'Image' section has two tabs: 'Operating System' (selected) and 'Snapshot'. A yellow arrow points from the 'CentOS 7.5 CIS 1.0' option in the image dropdown to the 'Others' menu item in the dashboard screenshot on the left.

CIS HARDENING

CIS Ubuntu Linux 22.04 LTS Benchmark

CIS Benchmarks focus on technical configuration settings used **to maintain and/or increase the security of the addressed technology**, and they should be used in conjunction with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

At the CIS Benchmarks are designed as a key component of a comprehensive cybersecurity program.





CIS Ubuntu Linux 22.04 LTS Benchmark

Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system

Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to **disable all services that are not required for normal system operation**

CIS HARDENING

CIS Ubuntu Linux 22.04 LTS Benchmark

Networking Configuration

This section **provides guidance** on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings

Access

Authentication and Authorization

System Maintenance

Recommendations in this section are intended as **maintenance and are intended to be checked** on a frequent basis to ensure system stability



CIS HARDENING



CIS CAS Lite (free version)

CIS-CAT Lite is the free **assessment tool developed by the CIS** (Center for Internet Security, Inc.).

CIS-CAT Lite helps users implement secure configurations for multiple technologies. With unlimited scans available via CIS-CAT Lite.

With CIS-CAT Lite, We Can Easily:

- Instantly check your systems against CIS Benchmarks.
- Receive a compliance score 1-100.
- Follow remediation steps to improve your security.

CIS HARDENING

CIS CAS Lite (free version)

1 Information

Target System Name *

yhs-cis-ubuntu ?

Target System Type *

Linux ?

Port *

22 ?

Username *

yusufhadiwinata ?

Password

?

Private key file

C:\..._rsa.ppk

IP Address / Hostname *

?

Temporary Path

2 Benchmarks

Available

Benchmark

- CIS Controls Assessment Module - Implementation Group 1 for Windows 10 v1.0.3
- CIS Controls Assessment Module - Implementation Group 1 for Windows Server v1.0.0
- CIS Google Chrome Benchmark v2.1.0
- CIS Microsoft Windows 10 Enterprise Benchmark v2.0.0
- CIS Microsoft Windows 10 Stand-alone Benchmark v2.0.0
- CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1**

Selected

Grayed out selections have interactive values

Benchmark

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1

Level 1 - Server

Level 2 - Server

Level 1 - Workstation

Level

3 Configuration Assessment

- ✓ CIS-CAT Pro Assessor loaded
- ✓ Platform Applicability assessed
- ✓ Checklist Rules evaluated
- ✓ Connected to assessment target
- System Characteristics collected
- ✓ Checklist Results generated
- ✓ Assessment started
- ✓ Definitions evaluated
- ✓ Assessment Results written

Assessment complete
Assessment 1 out of 1

```

-----
,088888o. 8888 d888888o. ,088888o. 8. 888888888888888888
8888 `88. 8888 .`8888:' `88. 8888 `88. .88. 8888
,88888 `8. 8888 8.`8888. Y8 ,88888 `8. .8888. 8888
888888 8888 `8.`8888. 88888888 .`88888. 8888
888888 8888 `8.`8888. 888 888888 .8.`88888. 8888
888888 8888 `8.`8888. 88888888 .8`8.`88888. 8888
`88888 .8' 8888 8b `8.`8888. `88888 .8' .8' `8.`88888. 8888
8888 ,88' 8888 `8b. ;8.`8888 8888 ,88' .888888888.`88888. 8888
`888888P' 8888 `Y8888P ,88P' `888888P' .8' `8.`88888. 8888
-----
Welcome to CIS-CAT Pro Assessor; built on 09/27/2023 12:52 PM
-----
This is the Center for Internet Security Configuration Assessment Tool, v4.34.0
At any time during the selection process, enter 'q!' to exit.
-----

```

CIS HARDENING

CIS CAS Lite (free version)

Summary :

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Initial Setup	40	15	0	0	3	0	40.0	55.0	73%
1.1 Filesystem Configuration	24	3	0	0	0	0	24.0	27.0	89%
1.1.1 Disable unused filesystems	5	0	0	0	0	0	5.0	5.0	100%
1.1.2 Configure /tmp	3	1	0	0	0	0	3.0	4.0	75%
1.1.3 Configure /var	2	0	0	0	0	0	2.0	2.0	100%
1.1.4 Configure /var/tmp	3	0	0	0	0	0	3.0	3.0	100%
1.1.5 Configure /var/log	3	0	0	0	0	0	3.0	3.0	100%
1.1.6 Configure /var/log/audit	3	0	0	0	0	0	3.0	3.0	100%
1.1.7 Configure /home									
1.1.8 Configure /dev/shm									
1.2 Filesystem Integrity Checking									
1.3 Configure Software and Patch Management									
1.4 Secure Boot Settings									
1.5 Additional Process Hardening									
1.6 Mandatory Access Control									
1.6.1 Configure AppArmor									
1.7 Command Line Warning Banners									
1.8 GNOME Display Manager									
2 Services									
2.1 Configure Time Synchronization									
2.1.1 Ensure time synchronization is in use									
2.1.2 Configure chrony									
2.1.3 Configure systemd-timesyncd									
2.1.4 Configure ntp									
2.2 Special Purpose Services									
2.3 Service Clients									

CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1

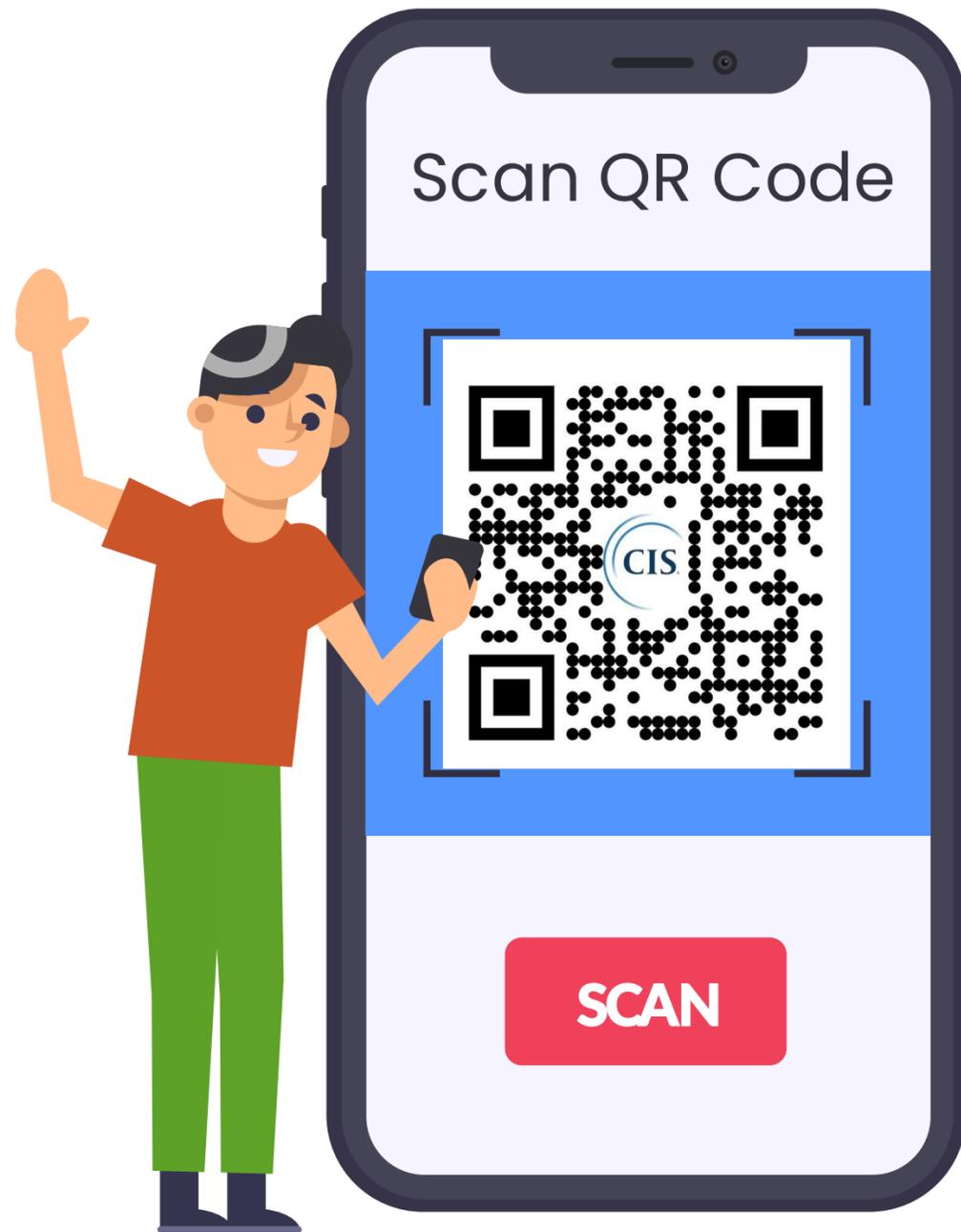
- Level 1 - Server
- Wednesday, October 4 2023 21:57:14
- Assessment Duration: 1 minute, 4 seconds

5 Logging and Auditing	7	4	0	0	8	0	7.0	11.0	64%
5.1 Configure Logging	7	3	0	0	8	0	7.0	10.0	70%
5.1.1 Configure journald	3	2	0	0	5	0	3.0	5.0	60%
5.1.1.1 Ensure journald is configured to send logs to a remote log host	2	0	0	0	2	0	2.0	2.0	100%
5.1.2 Configure rsyslog	4	0	0	0	3	0	4.0	4.0	100%
5.2 Configure System Accounting (auditd)	0	1	0	0	0	0	0.0	1.0	0%
5.2.1 Ensure auditing is enabled	0	0	0	0	0	0	0.0	0.0	0%
5.2.2 Configure Data Retention	0	0	0	0	0	0	0.0	0.0	0%
5.2.3 Configure auditd rules	0	0	0	0	0	0	0.0	0.0	0%
5.2.4 Configure auditd file access	0	1	0	0	0	0	0.0	1.0	0%
6 System Maintenance	22	2	0	0	1	0	22.0	24.0	92%
6.1 System File Permissions	11	1	0	0	1	0	11.0	12.0	92%
6.2 Local User and Group Settings	11	1	0	0	0	0	11.0	12.0	92%
Total	127	79	0	0	23	0	127.0	206.0	62%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

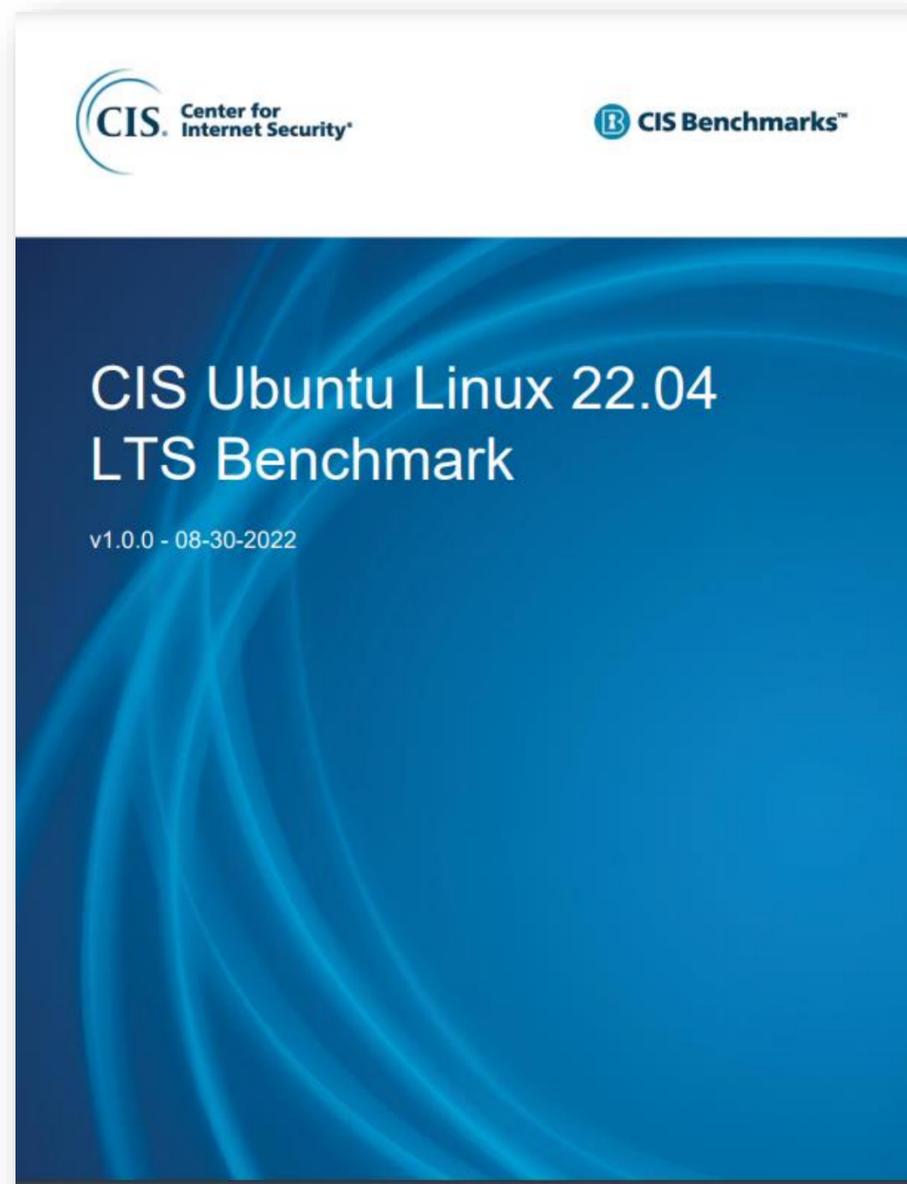
The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

CIS HARDENING DOC



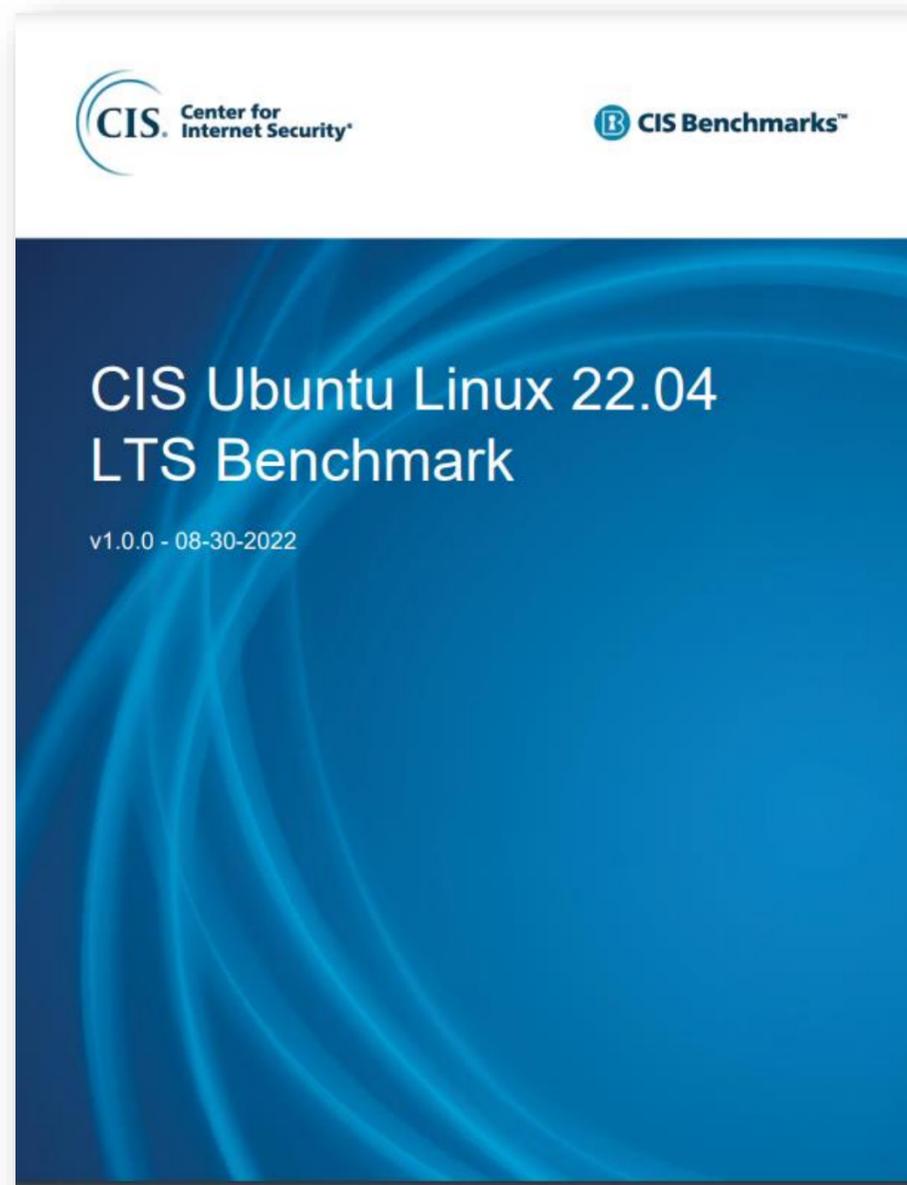
CIS Ubuntu Linux 22.04 LTS Ben

UBUNTU HARDENING



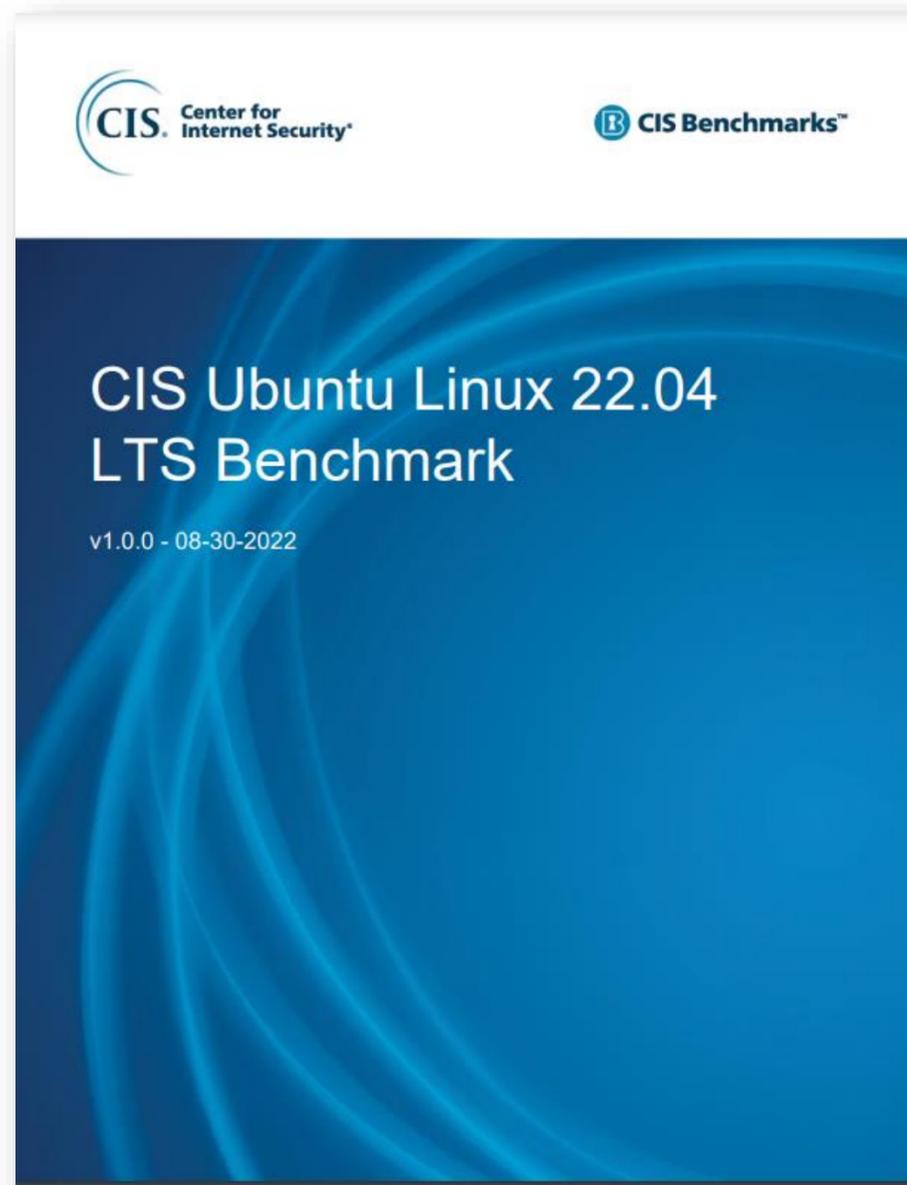
1.1 Filesystem Configuration	20
1.1.1 Disable unused filesystems	21
Start up scripts	21
Return values	21
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)	22
1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)	25
1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated).....	28
1.1.2 Configure /tmp	31
1.1.2.1 Ensure /tmp is a separate partition (Automated).....	32
1.1.2.2 Ensure nodev option set on /tmp partition (Automated)	35
1.1.2.3 Ensure noexec option set on /tmp partition (Automated)	37
1.1.2.4 Ensure nosuid option set on /tmp partition (Automated)	39
1.1.3 Configure /var	41
1.1.3.1 Ensure separate partition exists for /var (Automated)	42
1.1.3.2 Ensure nodev option set on /var partition (Automated)	45
1.1.3.3 Ensure nosuid option set on /var partition (Automated)	47
1.1.4 Configure /var/tmp	49
1.1.4.1 Ensure separate partition exists for /var/tmp (Automated)	50
1.1.4.2 Ensure noexec option set on /var/tmp partition (Automated)	53
1.1.4.3 Ensure nosuid option set on /var/tmp partition (Automated)	55
1.1.4.4 Ensure nodev option set on /var/tmp partition (Automated)	57
1.1.5 Configure /var/log	59
1.1.5.1 Ensure separate partition exists for /var/log (Automated)	60
1.1.5.2 Ensure nodev option set on /var/log partition (Automated)	62
1.1.5.3 Ensure noexec option set on /var/log partition (Automated).....	64
1.1.5.4 Ensure nosuid option set on /var/log partition (Automated).....	66

UBUNTU HARDENING



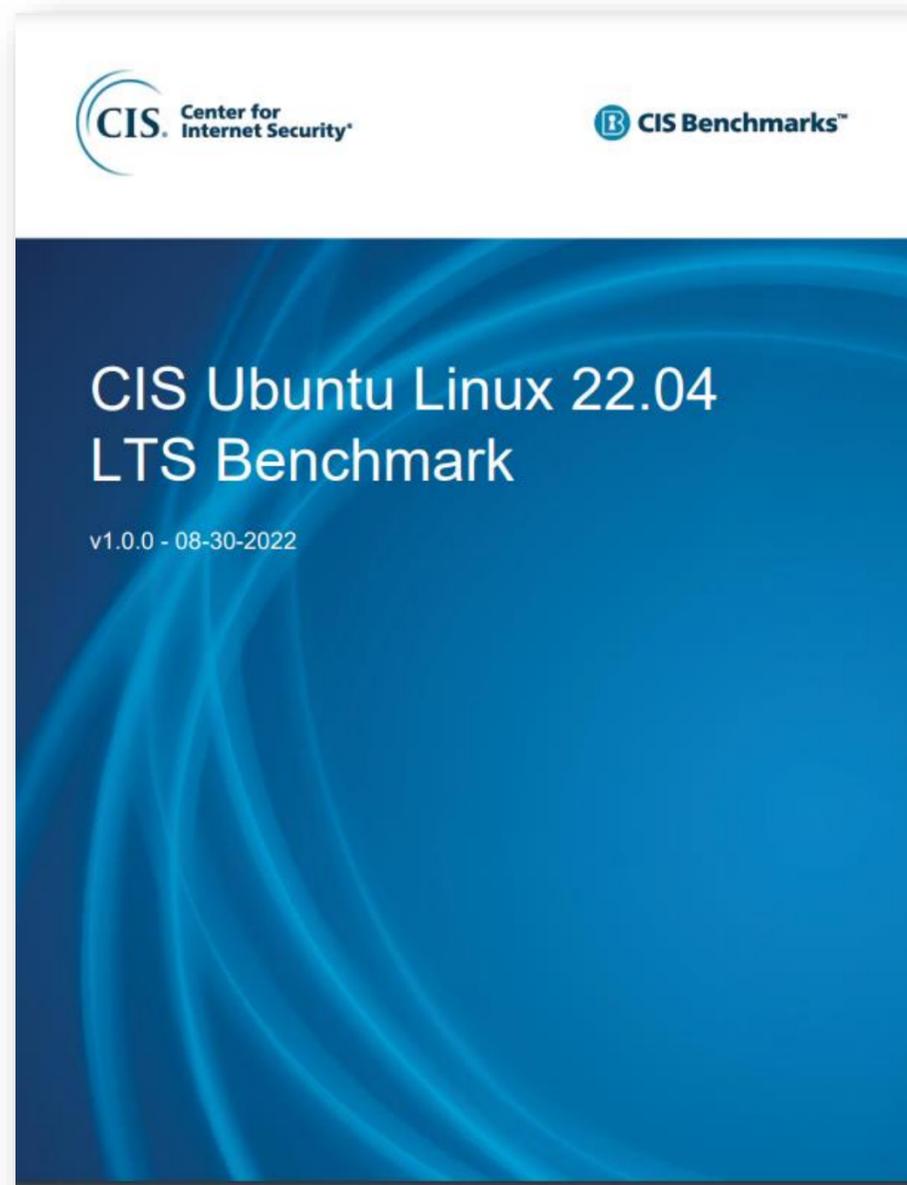
1.1.6 Configure /var/log/audit	68
1.1.6.1 Ensure separate partition exists for /var/log/audit (Automated).....	69
Protection from resource exhaustion	69
Fine grained control over the mount	69
Protection of audit data	69
1.1.6.2 Ensure noexec option set on /var/log/audit partition (Automated).....	71
1.1.6.3 Ensure nodev option set on /var/log/audit partition (Automated).....	73
1.1.6.4 Ensure nosuid option set on /var/log/audit partition (Automated).....	75
1.1.7 Configure /home	77
1.1.7.1 Ensure separate partition exists for /home (Automated)	78
Protection from resource exhaustion	78
Fine grained control over the mount	78
Protection of user data	78
1.1.7.2 Ensure nodev option set on /home partition (Automated)	81
1.1.7.3 Ensure nosuid option set on /home partition (Automated)	83
1.1.8 Configure /dev/shm	85
1.1.8.1 Ensure nodev option set on /dev/shm partition (Automated).....	86
1.1.8.2 Ensure noexec option set on /dev/shm partition (Automated).....	88
1.1.8.3 Ensure nosuid option set on /dev/shm partition (Automated).....	90
1.1.9 Disable Automounting (Automated)	92
1.1.10 Disable USB Storage (Automated)	94

UBUNTU HARDENING



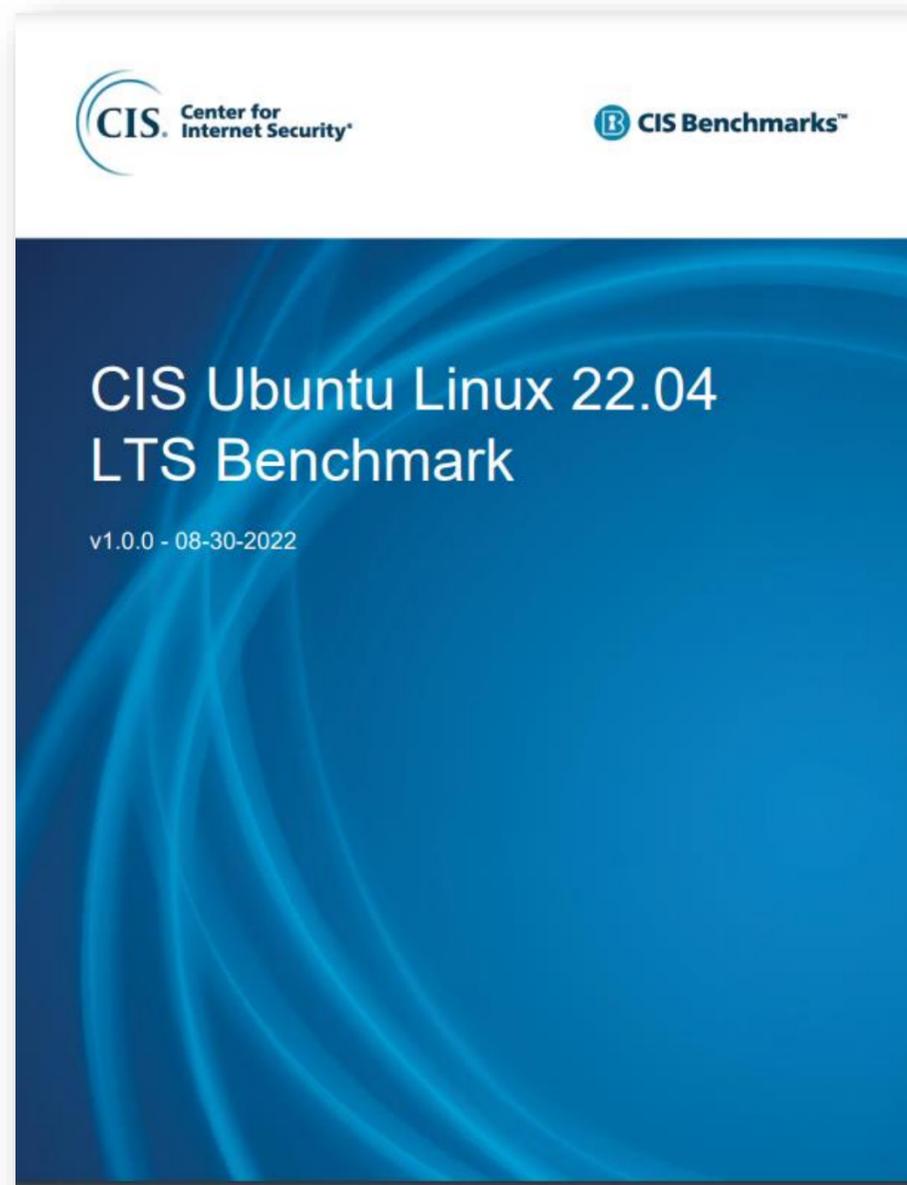
1.2 Configure Software Updates	98
1.2.1 Ensure package manager repositories are configured (Manual).....	99
1.2.2 Ensure GPG keys are configured (Manual)	101
1.3 Filesystem Integrity Checking.....	103
1.3.1 Ensure AIDE is installed (Automated).....	104
1.3.2 Ensure filesystem integrity is regularly checked (Automated).....	106
1.4 Secure Boot Settings.....	109
1.4.1 Ensure bootloader password is set (Automated)	110
1.4.2 Ensure permissions on bootloader config are configured (Automated).....	113
1.4.3 Ensure authentication required for single user mode (Automated)	115
1.5 Additional Process Hardening	117
1.5.1 Ensure address space layout randomization (ASLR) is enabled (Automated).....	118
1.5.2 Ensure prelink is not installed (Automated).....	122
1.5.3 Ensure Automatic Error Reporting is not enabled (Automated)	124
1.5.4 Ensure core dumps are restricted (Automated)	126
1.6 Mandatory Access Control	128
1.6.1 Configure AppArmor.....	129
1.6.1.1 Ensure AppArmor is installed (Automated)	130
1.6.1.2 Ensure AppArmor is enabled in the bootloader configuration.....	132
1.6.1.3 Ensure all AppArmor Profiles are in enforce or complain mode (Automated)	134
1.6.1.4 Ensure all AppArmor Profiles are enforcing (Automated).....	136

UBUNTU HARDENING



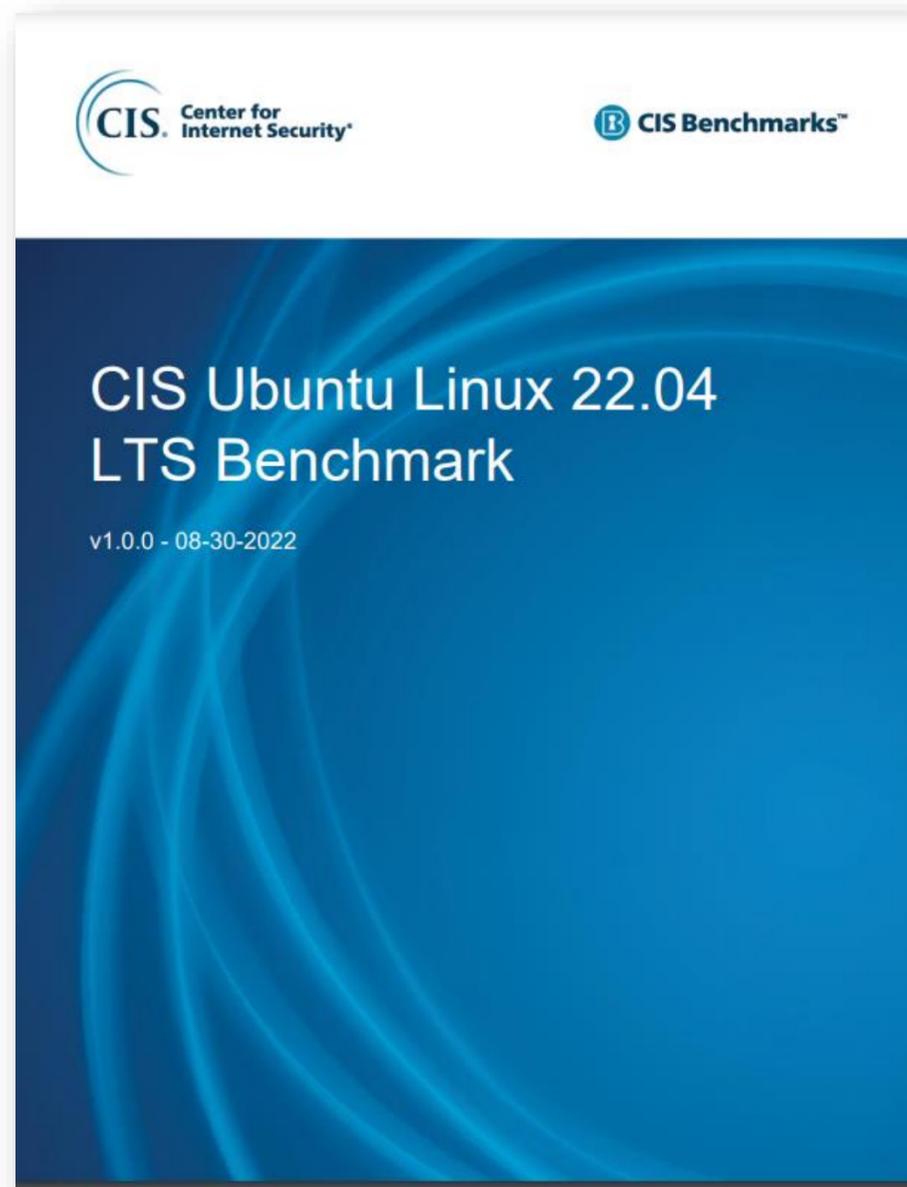
1.7 Command Line Warning Banners	138
1.7.1 Ensure message of the day is configured properly (Automated).....	139
1.7.2 Ensure local login warning banner is configured properly (Automated)	141
1.7.3 Ensure remote login warning banner is configured properly (Automated).....	143
1.7.4 Ensure permissions on /etc/motd are configured (Automated)	145
1.7.5 Ensure permissions on /etc/issue are configured (Automated)	147
1.7.6 Ensure permissions on /etc/issue.net are configured (Automated)	149
1.8 GNOME Display Manager.....	151
1.8.1 Ensure GNOME Display Manager is removed (Automated)	152
1.8.2 Ensure GDM login banner is configured (Automated).....	154
1.8.3 Ensure GDM disable-user-list option is enabled (Automated).....	158
1.8.4 Ensure GDM screen locks when the user is idle (Automated)	162
1.8.5 Ensure GDM screen locks cannot be overridden (Automated)	167
1.8.6 Ensure GDM automatic mounting of removable media is disabled (Automated)	172
1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden.....	178
1.8.8 Ensure GDM autorun-never is enabled (Automated)	183
1.8.9 Ensure GDM autorun-never is not overridden (Automated)	188
1.8.10 Ensure XDCMP is not enabled (Automated).....	193
1.9 Ensure updates, patches, and additional security software are installed (Manual)	195

UBUNTU HARDENING



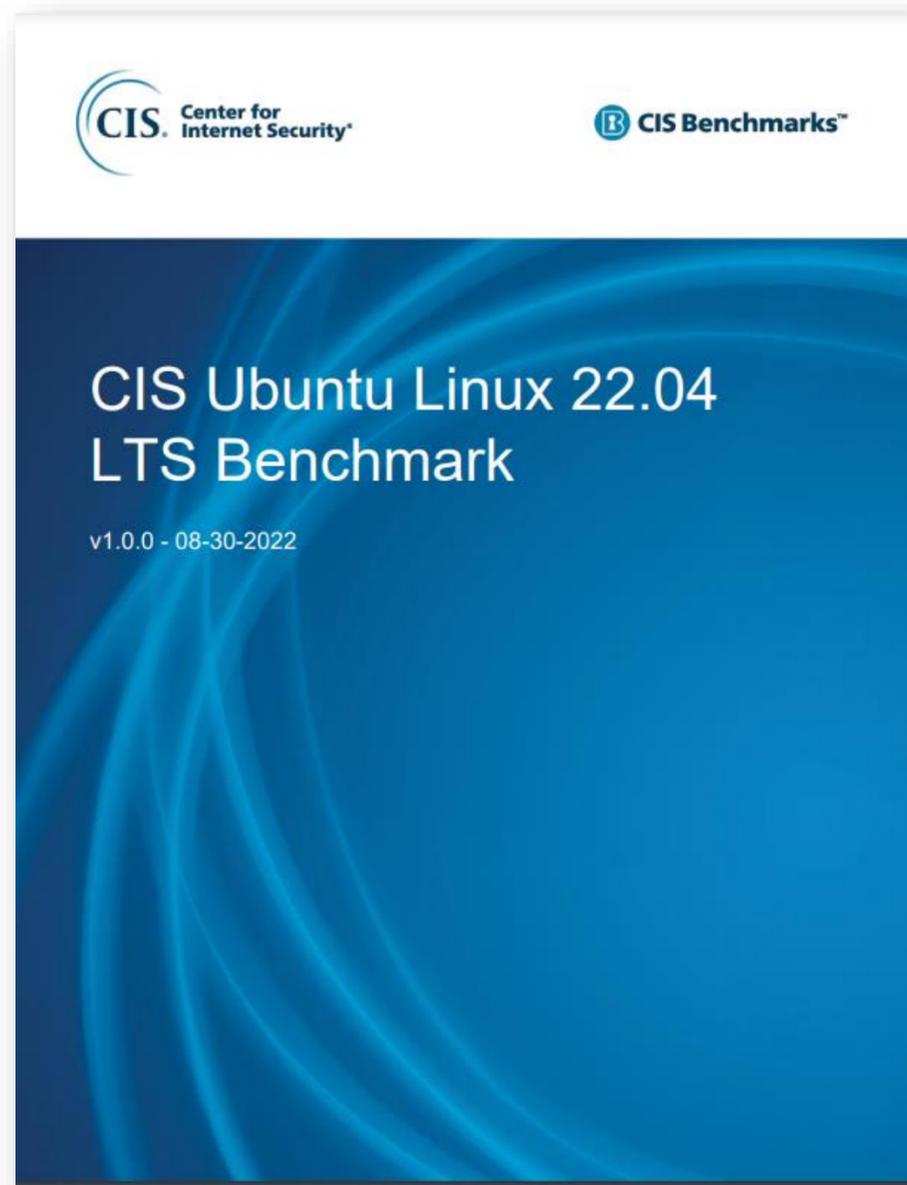
2 Services	197
2.1 Configure Time Synchronization	198
2.1.1 Ensure time synchronization is in use	199
2.1.1.1 Ensure a single time synchronization daemon is in use (Automated)	200
2.1.2 Configure chrony	204
2.1.2.1 Ensure chrony is configured with authorized timeserver (Manual)	205
2.1.2.2 Ensure chrony is running as user _chrony (Automated)	209
2.1.2.3 Ensure chrony is enabled and running (Automated)	211
2.1.3 Configure systemd-timesyncd	213
2.1.3.1 Ensure systemd-timesyncd configured with authorized timeserver (Manual).....	215
2.1.3.2 Ensure systemd-timesyncd is enabled and running (Automated)	218
2.1.4 Configure ntp	220
2.1.4.1 Ensure ntp access control is configured (Automated)	221
2.1.4.2 Ensure ntp is configured with authorized timeserver (Manual).....	225
2.1.4.3 Ensure ntp is running as user ntp (Automated).....	228
2.1.4.4 Ensure ntp is enabled and running (Automated).....	230
2.2 Special Purpose Services	232
2.2.1 Ensure X Window System is not installed (Automated)	233
2.2.2 Ensure Avahi Server is not installed (Automated).....	235
2.2.3 Ensure CUPS is not installed (Automated)	237

UBUNTU HARDENING



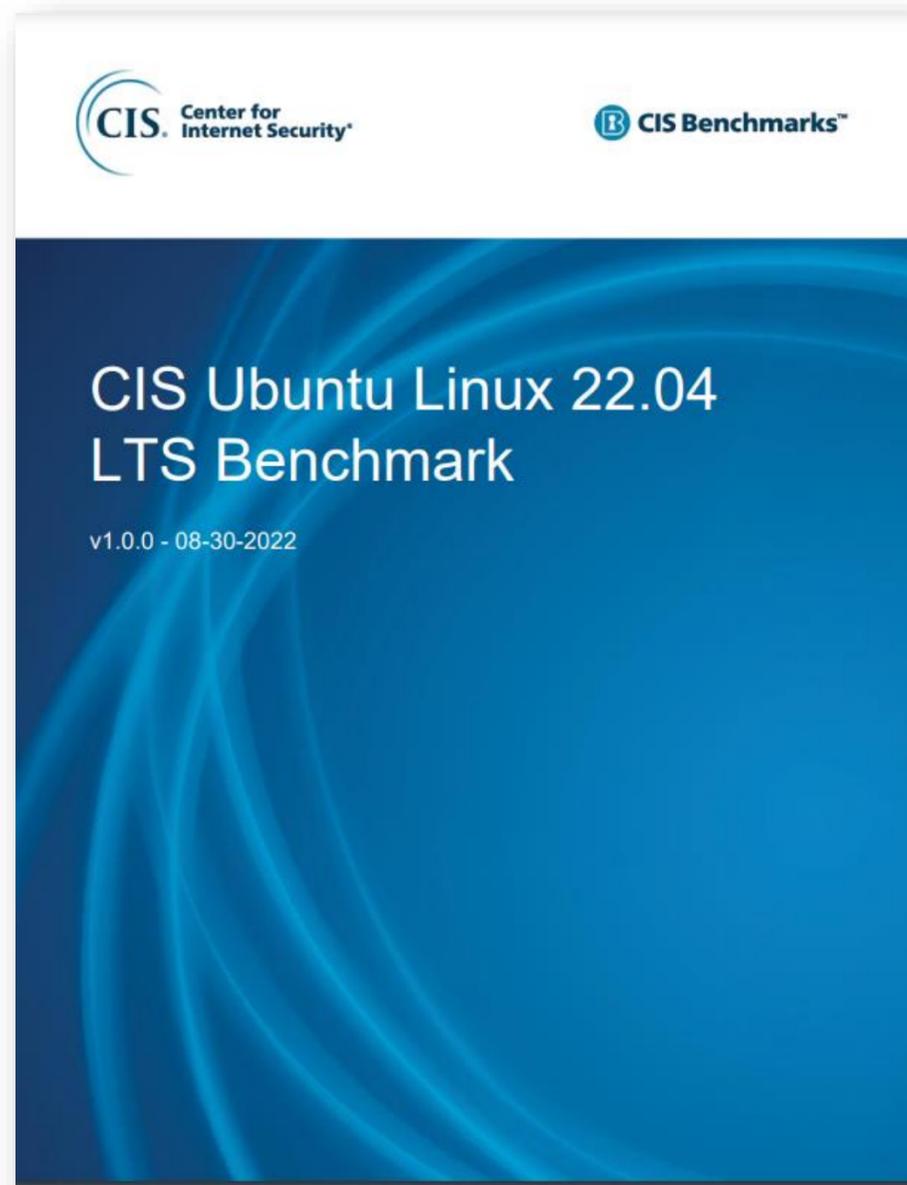
2.2.4 Ensure DHCP Server is not installed (Automated).....	239
2.2.5 Ensure LDAP server is not installed (Automated)	241
2.2.6 Ensure NFS is not installed (Automated)	243
2.2.7 Ensure DNS Server is not installed (Automated)	244
2.2.8 Ensure FTP Server is not installed (Automated)	246
2.2.9 Ensure HTTP server is not installed (Automated)	248
2.2.10 Ensure IMAP and POP3 server are not installed (Automated).....	250
2.2.11 Ensure Samba is not installed (Automated)	252
2.2.12 Ensure HTTP Proxy Server is not installed (Automated)	254
2.2.13 Ensure SNMP Server is not installed (Automated)	256
2.2.14 Ensure NIS Server is not installed (Automated).....	258
2.2.15 Ensure mail transfer agent is configured for local-only mode (Automated).....	260
2.2.16 Ensure rsync service is either not installed or masked (Automated).....	262
2.3 Service Clients	264
2.3.1 Ensure NIS Client is not installed (Automated)	265
2.3.2 Ensure rsh client is not installed (Automated)	267
2.3.3 Ensure talk client is not installed (Automated)	269
2.3.4 Ensure telnet client is not installed (Automated)	271
2.3.5 Ensure LDAP client is not installed (Automated).....	273
2.3.6 Ensure RPC is not installed (Automated).....	275
2.4 Ensure nonessential services are removed or masked (Manual).....	277

UBUNTU HARDENING



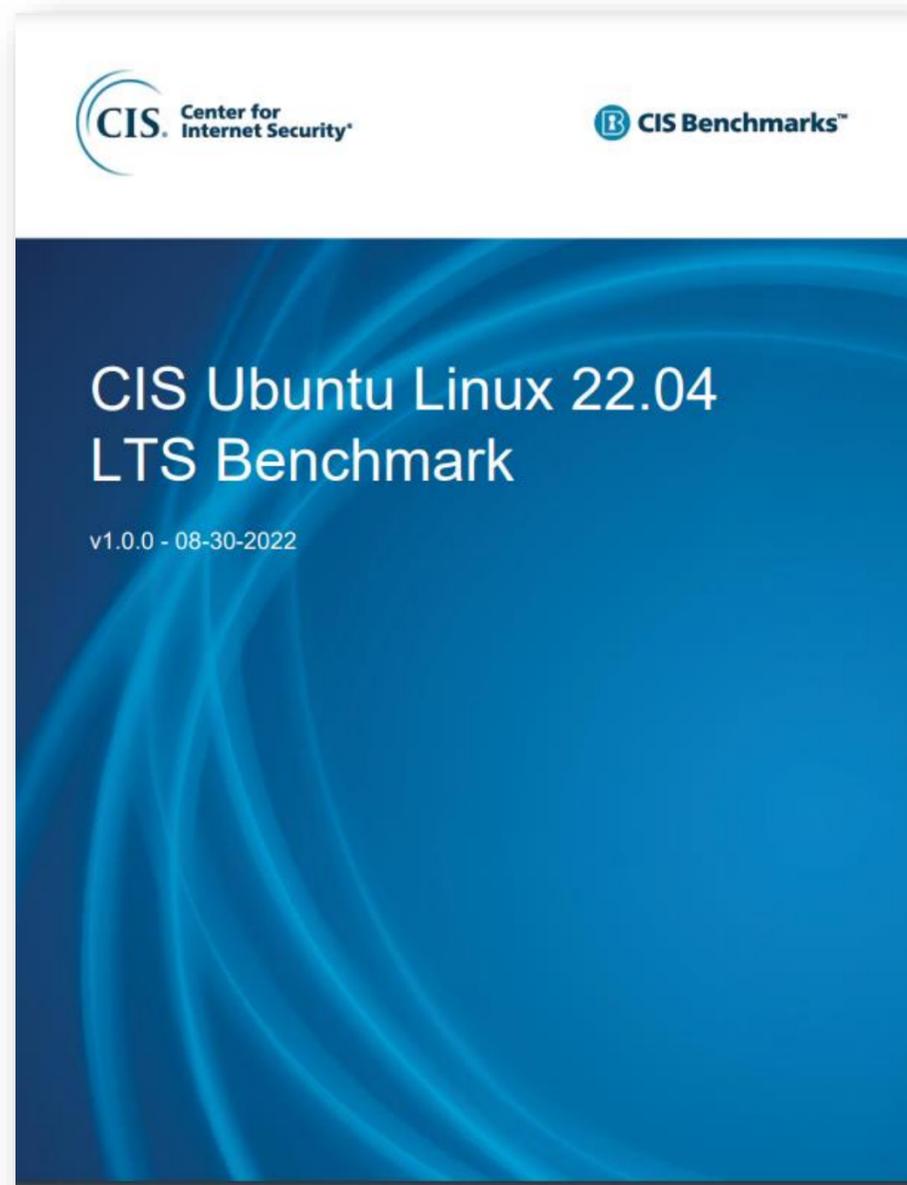
3 Network Configuration	279
3.1 Disable unused network protocols and devices	280
3.1.1 Ensure system is checked to determine if IPv6 is enabled (Manual)	281
3.1.2 Ensure wireless interfaces are disabled (Automated)	285
3.2 Network Parameters (Host Only).....	288
3.2.1 Ensure packet redirect sending is disabled (Automated)	289
3.2.2 Ensure IP forwarding is disabled (Automated)	293
3.3 Network Parameters (Host and Router).....	299
3.3.1 Ensure source routed packets are not accepted (Automated)	300
3.3.2 Ensure ICMP redirects are not accepted (Automated).....	306
3.3.3 Ensure secure ICMP redirects are not accepted (Automated)	312
3.3.4 Ensure suspicious packets are logged (Automated)	316
3.3.5 Ensure broadcast ICMP requests are ignored (Automated).....	320
3.3.6 Ensure bogus ICMP responses are ignored (Automated).....	324
3.3.7 Ensure Reverse Path Filtering is enabled (Automated)	328
3.3.8 Ensure TCP SYN Cookies is enabled (Automated)	332
3.3.9 Ensure IPv6 router advertisements are not accepted (Automated).....	336
3.4 Uncommon Network Protocols	342
3.4.1 Ensure DCCP is disabled (Automated).....	343
3.4.2 Ensure SCTP is disabled (Automated).....	346
3.4.3 Ensure RDS is disabled (Automated)	349
3.4.4 Ensure TIPC is disabled (Automated).....	352

UBUNTU HARDENING



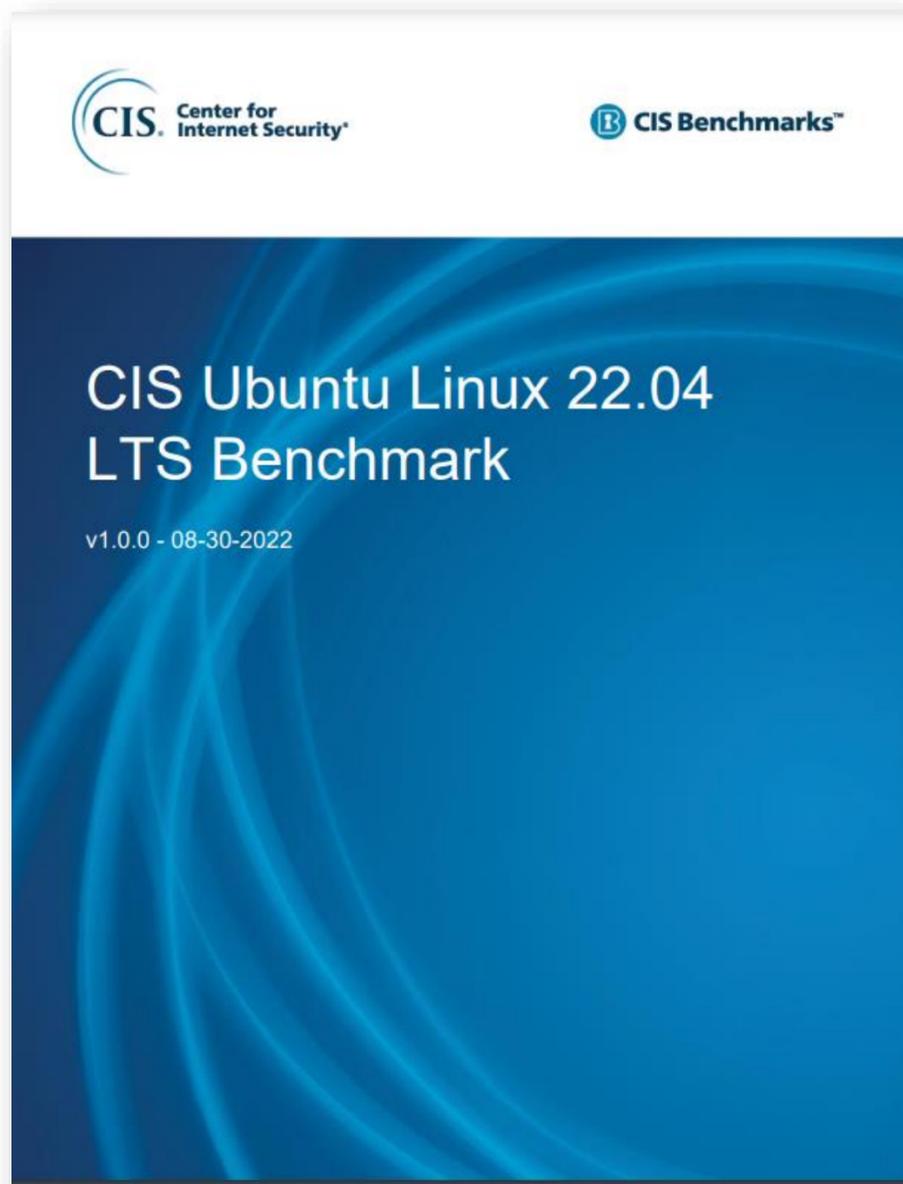
3.5 Firewall Configuration	355
3.5.1 Configure Uncomplicated Firewall	356
3.5.1.1 Ensure ufw is installed (Automated).....	357
3.5.1.2 Ensure iptables-persistent is not installed with ufw (Automated)	359
3.5.1.3 Ensure ufw service is enabled (Automated).....	361
3.5.1.4 Ensure ufw loopback traffic is configured (Automated)	364
3.5.1.5 Ensure ufw outbound connections are configured (Manual)	366
3.5.1.6 Ensure ufw firewall rules exist for all open ports (Automated).....	368
3.5.1.7 Ensure ufw default deny firewall policy (Automated).....	370
3.5.2 Configure nftables.....	372
3.5.2.1 Ensure nftables is installed (Automated).....	375
3.5.2.2 Ensure ufw is uninstalled or disabled with nftables (Automated)	377
3.5.2.3 Ensure iptables are flushed with nftables (Manual).....	379
3.5.2.4 Ensure a nftables table exists (Automated).....	381
3.5.2.5 Ensure nftables base chains exist (Automated)	383
3.5.2.6 Ensure nftables loopback traffic is configured (Automated)	385
3.5.2.7 Ensure nftables outbound and established connections are configured (Manual)	387
3.5.2.8 Ensure nftables default deny firewall policy (Automated).....	389
3.5.2.9 Ensure nftables service is enabled (Automated).....	391
3.5.2.10 Ensure nftables rules are permanent (Automated).....	393

UBUNTU HARDENING



3.5.3 Configure iptables	396
3.5.3.1 Configure iptables software	397
3.5.3.1.1 Ensure iptables packages are installed (Automated)	398
3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)	400
3.5.3.1.3 Ensure ufw is uninstalled or disabled with iptables (Automated).....	402
3.5.3.2 Configure IPv4 iptables	404
3.5.3.2.1 Ensure iptables default deny firewall policy (Automated)	405
3.5.3.2.2 Ensure iptables loopback traffic is configured (Automated)	407
3.5.3.2.3 Ensure iptables outbound and established connections are configured (Manual)	409
3.5.3.2.4 Ensure iptables firewall rules exist for all open ports (Automated).....	411
3.5.3.3 Configure IPv6 ip6tables	414
3.5.3.3.1 Ensure ip6tables default deny firewall policy (Automated)	415
3.5.3.3.2 Ensure ip6tables loopback traffic is configured (Automated)	418
3.5.3.3.3 Ensure ip6tables outbound and established connections are configured (Manual)	421
3.5.3.3.4 Ensure ip6tables firewall rules exist for all open ports (Automated).....	424

UBUNTU HARDENING



4 Logging and Auditing	427
4.1 Configure System Accounting (auditd)	428
Normalization.....	429
Capacity planning	429
4.1.1 Ensure auditing is enabled	430
4.1.1.1 Ensure auditd is installed (Automated).....	431
4.1.1.2 Ensure auditd service is enabled and active (Automated)	433
4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)	435
4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated).....	437
4.1.2 Configure Data Retention	439
4.1.2.1 Ensure audit log storage size is configured (Automated).....	440
4.1.2.2 Ensure audit logs are not automatically deleted (Automated)	442
4.1.2.3 Ensure system is disabled when audit logs are full (Automated)	444
4.1.3 Configure auditd rules	447
4.1.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated).....	448



Question?

**Lets discuss and Win
Merchandize or Voucher
Neocloud**

Thanks to Our Sponsors

