

Final Audit Report

Audit Results: Additional Software Audit

Check	Status	Recommendation
Ensure vlock is installed	failed	Install vlock using 'sudo apt install vlock -y'.
Ensure Endpoint Security for Linux Threat Prevention is installed	failed	Install Endpoint Security for Linux Threat Prevention using the appropriate package from the vendor.

Audit Results: Aide Integrity Check

Check	Status	Recommendation
Ensure AIDE is installed	failed	Install aide using: apt install aide -y
Ensure aide script to check file integrity is the default	failed	Verify manually that the correct aide check script is set as default.
Ensure filesystem integrity is regularly checked	failed	Schedule integrity check using: (echo '0 5 * * * /usr/sbin/aide --check') crontab -u root -l
Ensure administrator are notified of changes to the baseline configuration	failed	Schedule integrity check using: (echo '0 5 * * * /usr/sbin/aide --check') crontab -u root -l
Ensure cryptographic mechanisms are used to protect the integrity of audit tools	failed	Ensure AIDE is installed and configured properly.

Audit Results: Apparmor Audit Report

Check	Status	Recommendation
N/A	N/A	N/A

Audit Results: Auditd Rules

Check	Status	Recommendation
Ensure sudoers changes are collected	failed	Add '-w /etc/sudoers -p wa -k scope' to /etc/audit/rules.d/audit.rules and restart auditd.
Ensure sudo log changes are collected	failed	Add '-w /log/sudo.log -p wa -k sudo_log' to /etc/audit/rules.d/audit.rules and restart auditd.
Ensure time change events are collected	failed	Add '-w /localtime -p wa -k time-change' to /etc/audit/rules.d/audit.rules and restart auditd.
Ensure permission modification events are collected	failed	Add '-F arch=4096 -S chmod -S fchmod -S fchmodat -k perm_mod' to /etc/audit/rules.d/audit.rules and restart auditd.
Ensure unsuccessful file access attempts are collected	failed	Add '-F arch=4096 -S openat -F exit=-EACCES -F audit>=1000 -k access' to /etc/audit/rules.d/audit.rules and restart auditd.
Ensure file deletion events are collected	failed	Add '-F arch=4096 -S unlink -S unlinkat -S rename -S renameat -k delete' to /etc/audit/rules.d/audit.rules and restart auditd.

Ensure audit configuration is immutable	failed	Add '-e 2' to /etc/audit/rules.d/audit.rules and restart auditd.
---	--------	--

Audit Results: Chrony Audit

Check	Status	Recommendation
Ensure Chrony is enabled and running	failed	Enable Chrony using 'systemctl enable --now chronyd'.
Ensure Chrony is running as user _chrony	failed	Ensure Chrony runs as '_chrony' by checking '/etc/systemd/system/chronyd.service'.
Ensure Chrony is configured with authorized time servers	failed	Ensure Chrony is configured with authorized time servers by checking '/etc/chrony/chrony.conf'. Ensure it contains

Audit Results: Cli Warning Banners Audit

Check	Status	Recommendation
N/A	N/A	N/A

Audit Results: Data Retention Audit

Check	Status	Recommendation
Ensure audit log storage size is configured	passed	
Ensure audit logs are not automatically deleted	failed	Edit /etc/audit/auditd.conf and set 'max_log_file_action = keep_logs', then restart auditd.
Ensure system is disabled when audit logs are full	failed	Edit /etc/audit/auditd.conf and set 'space_left_action = email' and 'admin_space_left_action = halt', then restart auditd.
Ensure shut down by default upon audit failure	failed	Edit /etc/audit/auditd.conf and set 'disk_full_action = halt', then restart auditd.
Ensure audit event multiplexor is configured to off-load audit	failed	Edit /etc/audit/auditd.conf and set 'dispatcher = /sbin/audispd', then restart auditd.

Audit Results: Filesystem Audit Report

Check	Status	Recommendation
Ensure cramfs kernel module is not loaded	passed	
Ensure freevxfs kernel module is not loaded	passed	
Ensure hfs kernel module is not loaded	passed	
Ensure hfsplus kernel module is not loaded	passed	
Ensure jffs2 kernel module is not loaded	passed	
Ensure overlayfs kernel module is not loaded	passed	

Ensure squashfs kernel module is not loaded	passed	
Ensure udf kernel module is not loaded	passed	
Ensure usb-storage kernel module is not loaded	passed	
Ensure sticky bit is set on all world-writable directories	passed	

Audit Results: Fips Audit

Check	Status	Recommendation
Ensure FIPS mode is enabled	Failed	Enable FIPS mode using 'sudo fips-mode-setup --enable' and reboot the system.

Audit Results: Gdm Security Audit

Check	Status	Recommendation
Ensure GNOME Display Manager is removed	failed	Remove GDM using 'sudo apt purge gdm3 -y'.
Ensure GDM login banner is configured	failed	Set 'banner-message-enable=true' in /etc/gdm3/custom.conf.
Ensure GDM disable-user-list option is enabled	failed	Set 'disable-user-list=true' in /etc/gdm3/custom.conf.

Audit Results: Host Based Firewall Audit

Check	Status	Recommendation
Ensure UFW is installed	passed	
Ensure iptables-persistent is not installed with UFW	passed	
Ensure UFW service is enabled	passed	
Ensure UFW loopback traffic is configured	failed	Allow loopback traffic using 'ufw allow in from 127.0.0.0/8'.
Ensure UFW default deny firewall policy	failed	Set default deny policy using 'ufw default deny incoming'.

Audit Results: Iptables Audit

Check	Status	Recommendation
Ensure iptables packages are installed	passed	
Ensure nftables is not installed with iptables	failed	Remove nftables using 'apt remove nftables -y'.
Ensure iptables default deny firewall policy	passed	

Ensure iptables loopback traffic is configured	failed	Allow loopback using 'iptables -A INPUT -i lo -j ACCEPT'
--	--------	--

Audit Results: Local User Group Audit

	Check	Status	Recommendation
Ensure	accounts in /etc/passwd use shadowed passwords	passed	
Ensure	/etc/shadow password fields are not empty	passed	
Ensure	all groups in /etc/passwd exist in /etc/group	passed	
	Ensure shadow group is empty	passed	
	Ensure no duplicate UIDs exist	passed	
	Ensure no duplicate GIDs exist	passed	
	Ensure no duplicate user names exist	passed	
	Ensure no duplicate group names exist	passed	
	Ensure root PATH Integrity	passed	
	Ensure root is the only UID 0 account	passed	
Ensure	local interactive user home directories are configured	failed	Users have valid home directories using: usermod -d /home/<username> <username>
Ensure	local interactive user dot files access is configured	passed	

Audit Results: Log File Access Audit

	Check	Status	Recommendation
Ensure /var/log is owned by root	Ensure /var/log is owned by root	passed	
	Ensure /var/log is group-owned by syslog	passed	
	Ensure /var/log has mode 0755 or more restrictive	failed	Run: chmod 0755 /var/log
	Ensure /var/log/syslog is owned by syslog	passed	
	Ensure /var/log/syslog is group-owned by adm	passed	
Ensure /var/log/syslog has mode 0640 or more restrictive	failed	Run: chmod 0640 /var/log/syslog	
Ensure auditd is installed	Ensure auditd is installed	passed	
	Ensure auditd service is enabled and active	passed	
Ensure auditing for processes that start prior to auditd is enabled	Ensure auditd is installed	passed	
	Ensure auditd service is enabled and active	passed	
Ensure audit_backlog_limit is sufficient	Ensure audit_backlog_limit is sufficient/default/grub	failed	add 'audit_backlog_limit=8192' to GRUB_CMDLINE_LINUX, then run: update-grub

Audit Results: Logging Audit

Check	Status	Recommendation
Ensure systemd-journal-remote is installed	not installed	N/A
Ensure journald service is enabled	enabled	N/A
Ensure journald is not configured to receive logs from a remote peer	passed	
Ensure journald is configured to compress large log files	Failed	Enable log compression by adding 'Compress=yes' in /etc/systemd/journald.conf
Ensure journald is configured to write logfiles to persistent storage	Failed	Write logs to persistent storage by setting 'Storage=persistent' in /etc/systemd/journald.conf
Ensure systemd-journal-remote is configured	Verify	Verify systemd-journal-remote configuration in /etc/systemd/journal-remote.conf
Ensure systemd-journal-remote is enabled	manual	Check if systemd-journal-remote is enabled using systemctl.
Ensure journald is not configured to send logs to rsyslog	manual	Verify ForwardToSyslog setting in /etc/systemd/journald.conf.
Ensure journald log rotation is configured per site policy	Ensure	Ensure log rotation settings in /etc/systemd/journald.conf follow site requirements.
Ensure journald default file permissions are configured manually	Review	Review /etc/systemd/journald.conf and set appropriate file permissions.

Audit Results: Network Devices Audit

Check	Status	Recommendation
Ensure IPv6 status is identified	Review	Review and disable IPv6 if not required using 'sysctl -w net.ipv6.conf.all.disable_ipv6=1' and update sysctl.conf
Ensure wireless interfaces are disabled	passed	
Ensure Bluetooth services are not in use	failed	Disable Bluetooth using 'systemctl disable --now bluetooth'.

Audit Results: Network Kernel Modules Audit

Check	Status	Recommendation
Ensure dccp kernel module is not loaded	passed	
Ensure sctp kernel module is not loaded	passed	
Ensure rds kernel module is not loaded	passed	
Ensure tipc kernel module is not loaded	passed	

Audit Results: Network Kernel Parameters Audit

Check	Status	Recommendation
net.ipv4.ip_forward	passed	

net.ipv4.conf.all.send_redirects	Failed	Set net.ipv4.conf.all.send_redirects=0 in /etc/sysctl.conf and reload using 'sysctl -p'.
net.ipv4.icmp_ignore_bogus_error_responses	passed	
net.ipv4.icmp_echo_ignore_broadcasts	passed	
net.ipv4.conf.all.accept_redirects	passed	
net.ipv4.conf.all.secure_redirects	Failed	Set net.ipv4.conf.all.secure_redirects=0 in /etc/sysctl.conf and reload using 'sysctl -p'.
net.ipv4.conf.all.rp_filter	Failed	Set net.ipv4.conf.all.rp_filter=1 in /etc/sysctl.conf and reload using 'sysctl -p'.
net.ipv4.tcp_syncookies	passed	
net.ipv4.conf.all.accept_source_route	passed	
net.ipv4.conf.all.log_martians	Failed	Set net.ipv4.conf.all.log_martians=1 in /etc/sysctl.conf and reload using 'sysctl -p'.
net.ipv6.conf.all.accept_ra	Failed	Set net.ipv6.conf.all.accept_ra=0 in /etc/sysctl.conf and reload using 'sysctl -p'.

Audit Results: Nftables Audit

Check	Status	Recommendation
Ensure nftables is installed	passed	
Ensure UFW is uninstalled or disabled with nftables	failed	Disable UFW using 'systemctl stop ufw && systemctl disable ufw'.
Ensure nftables base chains exist	passed	
Ensure nftables service is enabled	failed	Enable nftables using 'systemctl enable --now nftables'.

Audit Results: Pam Pkcs11 Audit

Check	Status	Recommendation
Ensure libpam-pkcs11 package is installed	not installed	N/A
Ensure opensc-pkcs11 package is installed	not installed	N/A
Ensure pam_pkcs11 configuration file exists	failed	If using smart card authentication, ensure /etc/pam_pkcs11/pam_pkcs11.conf configuration file exists.
Ensure PKCS#11 user/group mappings are configured	skipped	Configuration file missing.

Audit Results: Pam Pwquality Audit

Check	Status	Recommendation
Ensure password is at least 15 characters	failed	Configure 'minlen' in /etc/security/pwquality.conf.
Ensure password includes at least one upper-case character	failed	Configure 'ucredit=-1' in /etc/security/pwquality.conf.

Ensure password includes at least one lower-case character	failed	Configure 'lcredit=-1' in /etc/security/pwquality.conf.
Ensure password includes at least one numeric character	failed	Configure 'dcredit=-1' in /etc/security/pwquality.conf.
Ensure password includes at least one special character	failed	Configure 'ocredit=-1' in /etc/security/pwquality.conf.
Ensure change of at least 8 characters when passwords are changed	failed	Configure 'difok=8' in /etc/security/pwquality.conf.
Maximum number of same consecutive characters in a password is configured	failed	Configure 'maxrepeat=3' in /etc/security/pwquality.conf.
Preventing the use of dictionary words for passwords is configured	failed	Configure 'dictcheck=1' in /etc/security/pwquality.conf.

Audit Results: Partition Audit Report

Check	Status	Recommendation
Ensure /tmp is on a separate partition	failed	Update /etc/fstab to mount /tmp on a separate partition.
Ensure nodev option is set on /tmp	failed	Add 'nodev' to the mount options in /etc/fstab for /tmp.
Ensure nosuid option is set on /tmp	failed	Add 'nosuid' to the mount options in /etc/fstab for /tmp.
Ensure noexec option is set on /tmp	failed	Add 'noexec' to the mount options in /etc/fstab for /tmp.
Ensure /dev/shm is on a separate partition	passed	
Ensure nodev option is set on /dev/shm	passed	
Ensure nosuid option is set on /dev/shm	passed	
Ensure noexec option is set on /dev/shm	failed	Add 'noexec' to the mount options in /etc/fstab for /dev/shm.
Ensure /home is on a separate partition	failed	Update /etc/fstab to mount /home on a separate partition.
Ensure nodev option is set on /home	failed	Add 'nodev' to the mount options in /etc/fstab for /home.
Ensure nosuid option is set on /home	failed	Add 'nosuid' to the mount options in /etc/fstab for /home.
Ensure /var is on a separate partition	failed	Update /etc/fstab to mount /var on a separate partition.
Ensure nodev option is set on /var	failed	Add 'nodev' to the mount options in /etc/fstab for /var.
Ensure nosuid option is set on /var	failed	Add 'nosuid' to the mount options in /etc/fstab for /var.
Ensure /var/tmp is on a separate partition	failed	Update /etc/fstab to mount /var/tmp on a separate partition.
Ensure nodev option is set on /var/tmp	failed	Add 'nodev' to the mount options in /etc/fstab for /var/tmp.
Ensure nosuid option is set on /var/tmp	failed	Add 'nosuid' to the mount options in /etc/fstab for /var/tmp.
Ensure noexec option is set on /var/tmp	failed	Add 'noexec' to the mount options in /etc/fstab for /var/tmp.
Ensure /var/log is on a separate partition	failed	Update /etc/fstab to mount /var/log on a separate partition.
Ensure nodev option is set on /var/log	failed	Add 'nodev' to the mount options in /etc/fstab for /var/log.
Ensure nosuid option is set on /var/log	failed	Add 'nosuid' to the mount options in /etc/fstab for /var/log.
Ensure noexec option is set on /var/log	failed	Add 'noexec' to the mount options in /etc/fstab for /var/log.
Ensure /var/log/audit is on a separate partition	failed	Update /etc/fstab to mount /var/log/audit on a separate partition.
Ensure nodev option is set on /var/log/audit	failed	Add 'nodev' to the mount options in /etc/fstab for /var/log/audit.

Ensure nosuid option is set on /var/log/audit	failed	Add 'nosuid' to the mount options in /etc/fstab for /var/log/audit.
Ensure noexec option is set on /var/log/audit	failed	Add 'noexec' to the mount options in /etc/fstab for /var/log/audit.

Audit Results: Password Policy Audit

Check	Status	Recommendation
N/A	N/A	N/A

Audit Results: Privilege Escalation Audit

Check	Status	Recommendation
Ensure sudo is installed	passed	
Ensure sudo commands use pty	failed	Add Defaults requiretty to /etc/sudoers.
Ensure sudo log file exists	failed	Configure sudo logging in /etc/sudoers with Defaults logfile=/var/log/sudo.log
Ensure users must provide password for privilege escalation	passed	
Ensure sudo authentication timeout is configured correctly	failed	Set Defaults timestamp_timeout=<value> in /etc/sudoers.
Ensure access to the su command is restricted	failed	Ensure su access is restricted to wheel group using pam_wheel.so.

Audit Results: Rsyslog Audit

Check	Status	Recommendation
Ensure rsyslog is installed	installed	N/A
Ensure rsyslog service is enabled	enabled	N/A
Ensure rsyslog default file permissions are configured	failed	Add FileCreateMode 0640 to /etc/rsyslog.conf to enforce secure log file permissions
Ensure rsyslog is not configured to receive logs from a remote peer	passed	
Ensure remote access methods are monitored	failed	Ensure remote access logs (e.g., /var/log/auth.log) are monitored by rsyslog
Ensure journald is configured to send logs to rsyslog	manual	Check /etc/systemd/journald.conf and set 'ForwardToSyslog=yes'.
Ensure logging is configured	manual	Review /etc/rsyslog.conf and ensure necessary logging rules are in place.
Ensure rsyslog is configured to send logs to a remote log host	verify	Verify if logs are forwarded to a remote syslog server via *.* @remote-host:514

Audit Results: Secure Boot Audit Report

Check	Status	Recommendation
Bootloader Password	Set GRUB password using 'grub-mkpasswd-pbkdf2' and update /etc/grub.d/00_header	
Bootloader Config Permissions	passed	
Single-User Mode Authentication	Add 'sudo LOGIN=yes' to /etc/default/grub and update GRUB using 'sudo update-grub'	

Audit Results: Service Clients Audit

Check	Status	Recommendation
N/A	passed	
N/A	passed	
N/A	passed	
N/A	Removed with 'apt remove --purge telnet -y' and disable it using 'systemctl disable telnet'	
N/A	Removed with 'apt remove --purge ldap-utils -y' and disable it using 'systemctl disable ldap-utils'	
N/A	passed	
Ensure nonessential services are removed or masked using 'systemctl list-units --type=service' and mask any unnecessary services using 'systemctl mask'	Review all non-essential services and remove or mask them using 'systemctl remove' or 'systemctl mask'	

Audit Results: Software Patch Audit Report

Check	Status	Recommendation
Ensure APT requires a recognized digital signature before installing	Run 'dpkg-query -f='\${Package} \${Version} \${Architecture}\n'	Unauthenticated "false"; > /etc/apt/apt.conf.d/00secure' to enforce signature
Ensure APT removes outdated software configurations	Run 'dpkg-query -f='\${Package} \${Version} \${Architecture}\n'	Periodic::Autoremove "1"; > /etc/apt/apt.conf.d/10periodic' to enable automatic removal of old versions

Audit Results: Special Services Audit

Check	Status	Recommendation
N/A	Removed with 'apt remove --purge xserver-xorg* -y' and disable it using 'systemctl disable xserver-xorg'	
N/A	Removed with 'apt remove --purge avahi-daemon -y' and disable it using 'systemctl disable avahi-daemon'	
N/A	Removed with 'apt remove --purge cups -y' and disable it using 'systemctl disable cups'	
N/A	passed	None
N/A	passed	None
N/A	passed	None
N/A	Removed with 'apt remove --purge bind9 -y' and disable it using 'systemctl disable bind9'	

	N/A	Removed with 'apt remove --purge vsftpd -y' and disable it using 'systemctl disable vsftpd'	disabled
	N/A	Removed with 'apt remove --purge apache2 -y' and disable it using 'systemctl disable apache2'	disabled
	N/A	passed	None
	N/A	Removed with 'apt remove --purge samba -y' and disable it using 'systemctl disable samba'	disabled
	N/A	passed	None
	N/A	passed	None
	N/A	passed	None
	N/A	Removed with 'apt remove --purge dnsmasq -y' and disable it using 'systemctl disable dnsmasq'	disabled
	N/A	passed	None
	N/A	passed	None
Ensure mail transfer agent is configured for local-only mode	Failed	Set inet_interfaces = loopback-only in '/etc/postfix/main.cf' and restart Postfix	Not Configured
Ensure rsync is either not installed or is masked	Masked	Masked using 'systemctl mask rsync' or remove it using 'apt remove --purge rsync'	Masked

Audit Results: Ssh Server Audit

Check	Status	Recommendation
Ensure SSH is installed and active	passed	
Ensure permissions on /etc/ssh/sshd_config are configured properly	passed	
Ensure SSH root login is disabled	failed	Set PermitRootLogin no in /etc/ssh/sshd_config.
Ensure SSH PAM is enabled	passed	

Audit Results: Timesyncd Audit

Check	Status	Recommendation
Ensure systemd-timesyncd is enabled and enabled manually	Failed	Enable it using 'systemctl status systemd-timesyncd'. If not, enable it with 'systemctl enable systemd-timesyncd'
Ensure systemd-timesyncd is configured with authorized timeservers	Failed	Edit /etc/systemd-timesyncd.conf to specify an authorized timeserver under the 'NTP=' directive

Audit Results: Time Sync Audit

Check	Status	Recommendation
Ensure time synchronization is in use	passed	
Ensure a single time synchronization daemon is in use	Failed	Use a single time synchronization service (e.g., 'systemctl enable --now systemd-timesyncd')

Audit Results: User Accounts Audit

Check		Status	Recommendation
Ensure PASS_MIN_DAYS is 1 or less		passed	
Ensure PASS_MAX_DAYS is 60 or less		failed	Set PASS_MAX_DAYS to 60 or lower in /etc/login.defs.
Ensure PASS_WARN_AGE is 7 or less		passed	
Ensure INACTIVE is 30 or less		failed	Set INACTIVE to 30 or lower in /etc/login.defs.
Ensure ENCRYPT_METHOD is SHA512		passed	
Ensure root account is locked		passed	
Ensure system accounts are secured		failed	Disable unnecessary system accounts.
Ensure default group for the root account is GID 0		passed	
Ensure UMASK is 027 or more restrictive		failed	Set UMASK to 027 or lower in /etc/profile and /etc/bash.bashrc.
Ensure UMASK is 077 or more restrictive		failed	Set UMASK to 077 or lower in /etc/profile and /etc/bash.bashrc.
Ensure default user shell timeout is 600 seconds or less	failed	Set TMOUT to 600 seconds or less in /etc/profile or /etc/bash.bashrc.	
Ensure nologin is not listed in /etc/shells		passed	
Ensure temporary accounts expiration time of 72 hours or less	manual		Verify temporary accounts expire in 72 hours or less.
Ensure emergency accounts are removed or disabled after 72 hours	manual		Manually ensure emergency accounts do not exist beyond 72 hours.
Ensure immediate change to a permanent password	manual		Ensure temporary passwords are changed immediately to a permanent one.
Ensure /etc/ssl/certs only contains authorized certificates	manual		Verify /etc/ssl/certs contains only DoD PKI-authorized certificates.