| Control Number | Recommendation |

| ----------------- | --------------------------------------------------------------------------------------------------------------- |

| 1.1.2.5.4 | Ensure noexec option set on /var/tmp partition |

| 1.1.2.6.1 | Ensure separate partition exists for /var/log |

| 1.1.2.6.2 | Ensure nodev option set on /var/log partition |

| 1.1.2.6.3 | Ensure nosuid option set on /var/log partition |

| 1.1.2.6.4 | Ensure noexec option set on /var/log partition |

| 1.1.2.7.1 | Ensure separate partition exists for /var/log/audit |

| 1.1.2.7.2 | Ensure nodev option set on /var/log/audit partition |

| 1.1.2.7.3 | Ensure nosuid option set on /var/log/audit partition |

| 1.1.2.7.4 | Ensure noexec option set on /var/log/audit partition |

| 1.2.1.1 | Ensure GPG keys are configured |

| 1.2.1.2 | Ensure gpgcheck is globally activated |

| 1.2.1.3 | Ensure repo\_gpgcheck is globally activated |

| 1.2.1.4 | Ensure package manager repositories are configured |

| 1.2.2.1 | Ensure updates, patches, and additional security software are installed |

| 1.3.1.1 | Ensure SELinux is installed |

| 1.3.1.2 | Ensure SELinux is not disabled in bootloader configuration |

| 1.3.1.3 | Ensure SELinux policy is configured |

| 1.3.1.4 | Ensure the SELinux mode is not disabled |

| 1.3.1.5 | Ensure the SELinux mode is enforcing |

| 1.3.1.6 | Ensure no unconfined services exist |

| 1.3.1.7 | Ensure the MCS Translation Service (mcstrans) is not installed |

| 1.3.1.8 | Ensure SETroubleshoot is not installed |

| 1.4.1 | Ensure bootloader password is set |

| 1.4.2 | Ensure access to bootloader config is configured |

| 1.5.1 | Ensure address space layout randomization is enabled |

| 1.5.2 | Ensure ptrace\_scope is restricted |

| 1.6.1 | Ensure system wide crypto policy is not set to legacy |

| 1.6.2 | Ensure system wide crypto policy is not set in sshd configuration |

| 1.6.3 | Ensure system wide crypto policy disables sha1 hash and signature support |

| 1.6.4 | Ensure system wide crypto policy disables macs less than 128 bits |

| 1.6.5 | Ensure system wide crypto policy disables cbc for ssh |

| 1.6.6 | Ensure system wide crypto policy disables chacha20-poly1305 for ssh |

| 1.6.7 | Ensure system wide crypto policy disables EtM for ssh |

| 1.7.4 | Ensure access to /etc/motd is configured |

| 1.7.5 | Ensure access to /etc/issue is configured |

| 1.7.6 | Ensure access to /etc/issue.net is configured |

| 1.8.1 | Ensure GNOME Display Manager is removed |

| 1.8.4 | Ensure GDM screen locks when the user is idle |

| 1.8.5 | Ensure GDM screen locks cannot be overridden |

| 1.8.6 | Ensure GDM automatic mounting of removable media is disabled |

| 1.8.7 | Ensure GDM disabling automatic mounting of removable media is not overridden |

| 1.8.8 | Ensure GDM autorun-never is enabled |

| 1.8.9 | Ensure GDM autorun-never is not overridden |

| 1.8.10 | Ensure XDMCP is not enabled |

| 2.1.1 | Ensure autofs services are not in use |

| 2.1.2 | Ensure avahi daemon services are not in use |

| 2.1.3 | Ensure dhcp server services are not in use |

| 2.1.4 | Ensure dns server services are not in use |

| 2.1.5 | Ensure dnsmasq services are not in use |

| 2.1.6 | Ensure samba file server services are not in use |

| 2.1.7 | Ensure ftp server services are not in use |

| 2.1.8 | Ensure message access server services are not in use |

| 2.1.9 | Ensure network file system services are not in use |

| 2.1.10 | Ensure nis server services are not in use |

| 2.1.11 | Ensure print server services are not in use |

| 2.1.12 | Ensure rpcbind services are not in use |

| 2.1.13 | Ensure rsync services are not in use |

| 2.1.14 | Ensure snmp services are not in use |

| 2.1.15 | Ensure telnet server services are not in use |

| 2.1.16 | Ensure tftp server services are not in use |

| 2.1.17 | Ensure web proxy server services are not in use |

| 2.1.18 | Ensure web server services are not in use |

| 2.1.19 | Ensure xinetd services are not in use |

| 2.1.20 | Ensure X window server services are not in use |

| 2.1.21 | Ensure mail transfer agents are configured for local-only mode |

| 2.1.22 | Ensure only approved services are listening on a network interface |

| 2.2.1 | Ensure ftp client is not installed |

| 2.2.2 | Ensure ldap client is not installed |

| 2.2.3 | Ensure nis client is not installed |

| 2.2.4 | Ensure telnet client is not installed |

| 2.2.5 | Ensure tftp client is not installed |

| 2.3.1 | Ensure time synchronization is in use |

| 2.3.2 | Ensure chrony is configured |

| 2.4.1.2 | Ensure permissions on /etc/crontab are configured |

| 2.4.1.3 | Ensure permissions on /etc/cron.hourly are configured |

| 2.4.1.4 | Ensure permissions on /etc/cron.daily are configured |

| 2.4.1.5 | Ensure permissions on /etc/cron.weekly are configured |

| 2.4.1.6 | Ensure permissions on /etc/cron.monthly are configured |

| 2.4.1.7 | Ensure permissions on /etc/cron.d are configured |

| 2.4.1.8 | Ensure crontab is restricted to authorized users |

| 2.4.2.1 | Ensure at is restricted to authorized users |

| 3.1.1 | Ensure IPv6 status is identified |

| 3.1.3 | Ensure bluetooth services are not in use |

| 3.2.1 | Ensure dccp kernel module is not available |

| 3.2.2 | Ensure tipc kernel module is not available |

| 3.2.3 | Ensure rds kernel module is not available |

| 3.2.4 | Ensure sctp kernel module is not available |

| 3.3.1 | Ensure ip forwarding is disabled |

| 3.3.2 | Ensure packet redirect sending is disabled |

| 3.3.3 | Ensure bogus icmp responses are ignored |

| 3.3.4 | Ensure broadcast icmp requests are ignored |

| 3.3.5 | Ensure icmp redirects are not accepted |

| 3.3.6 | Ensure secure icmp redirects are not accepted |

| 3.3.7 | Ensure reverse path filtering is enabled |

| 3.3.8 | Ensure source routed packets are not accepted |

| 3.3.9 | Ensure suspicious packets are logged |

| 3.3.10 | Ensure tcp syn cookies is enabled |

| 3.3.11 | Ensure ipv6 router advertisements are not accepted |

| 4.1.1 | Ensure nftables is installed |

| 4.1.2 | Ensure a single firewall configuration utility is in use |

| 4.2.1 | Ensure firewalld drops unnecessary services and ports |

| 4.2.2 | Ensure firewalld loopback traffic is configured |

| 4.3.1 | Ensure nftables base chains exist |

| 4.3.2 | Ensure nftables established connections are configured |

| 4.3.3 | Ensure nftables default deny firewall policy |

| 4.3.4 | Ensure nftables loopback traffic is configured |

| 5.1.1 | Ensure permissions on /etc/ssh/sshd\_config are configured |

| 5.1.2 | Ensure permissions on SSH private host key files are configured |

| 5.1.3 | Ensure permissions on SSH public host key files are configured |

| 5.1.4 | Ensure sshd Ciphers are configured |

| 5.1.5 | Ensure sshd KexAlgorithms is configured |

| 5.1.6 | Ensure sshd MACs are configured |

| 5.1.7 | Ensure sshd access is configured |

| 5.1.10 | Ensure sshd DisableForwarding is enabled |

| 5.1.11 | Ensure sshd GSSAPIAuthentication is disabled |

| 5.1.13 | Ensure sshd IgnoreRhosts is enabled |

| 5.1.15 | Ensure sshd LogLevel is configured |

| 5.1.19 | Ensure sshd PermitEmptyPasswords is disabled |

| 5.1.20 | Ensure sshd PermitRootLogin is disabled |

| 5.1.22 | Ensure sshd UsePAM is enabled |

| 5.2.1 | Ensure sudo is installed |

| 5.2.2 | Ensure sudo commands use pty |

| 5.2.3 | Ensure sudo log file exists |

| 5.2.4 | Ensure users must provide password for escalation |

| 5.2.5 | Ensure re-authentication for privilege escalation is not disabled globally |

| 5.2.6 | Ensure sudo authentication timeout is configured correctly |

| 5.2.7 | Ensure access to the su command is restricted |

| 5.3.2.1 | Ensure active authselect profile includes pam modules |

| 5.3.2.2 | Ensure pam\_faillock module is enabled |

| 5.3.2.3 | Ensure pam\_pwquality module is enabled |

| 5.3.2.4 | Ensure pam\_pwhistory module is enabled |

| 5.3.3.1.1 | Ensure password failed attempts lockout is configured |

| 5.3.3.1.2 | Ensure password unlock time is configured |

| 5.3.3.1.3 | Ensure password failed attempts lockout includes root account |

| 5.3.3.2.1 | Ensure password number of changed characters is configured |

| 5.3.3.2.2 | Ensure password length is configured |

| 5.3.3.2.3 | Ensure password complexity is configured |

| 5.3.3.2.4 | Ensure password same consecutive characters is configured |

| 5.3.3.2.5 | Ensure password maximum sequential characters is configured |

| 5.3.3.2.6 | Ensure password dictionary check is enabled |

| 5.3.3.2.7 | Ensure password quality is enforced for the root user |

| 5.3.3.3.1 | Ensure password history remember is configured |

| 5.3.3.3.2 | Ensure password history is enforced for the root user |

| 5.3.3.3.3 | Ensure pam\_pwhistory includes use\_authtok |

| 5.3.3.4.1 | Ensure pam\_unix does not include nullok |

| 5.3.3.4.2 | Ensure pam\_unix does not include remember |

| 5.3.3.4.3 | Ensure pam\_unix includes a strong password hashing algorithm |

| 5.3.3.4.4 | Ensure pam\_unix includes use\_authtok |

| 5.4.1.1 | Ensure password expiration is configured |

| 5.4.1.2 | Ensure minimum password days is configured |

| 5.4.1.3 | Ensure password expiration warning days is configured |

| 5.4.1.4 | Ensure strong password hashing algorithm is configured |

| 5.4.1.5 | Ensure inactive password lock is configured |

| 5.4.1.6 | Ensure all users last password change date is in the past |

| 5.4.2.2 | Ensure root is the only GID 0 account |

| 5.4.2.3 | Ensure group root is the only GID 0 group |

| 5.4.2.4 | Ensure root account access is controlled |

| 5.4.2.6 | Ensure root user umask is configured |

| 5.4.2.7 | Ensure system accounts do not have a valid login shell |

| 5.4.2.8 | Ensure accounts without a valid login shell are locked |

| 5.4.3.2 | Ensure default user shell timeout is configured |

| 5.4.3.3 | Ensure default user umask is configured |

| 6.2.1.1 | Ensure journald service is enabled and active |

| 6.2.1.2 | Ensure journald log file access is configured |

| 6.2.1.3 | Ensure journald log file rotation is configured |

| 6.2.2.1.1 | Ensure systemd-journal-remote is installed |

| 6.2.2.1.2 | Ensure systemd-journal-upload authentication is configured |

| 6.2.2.1.3 | Ensure systemd-journal-upload is enabled and active |

| 6.2.2.1.4 | Ensure systemd-journal-remote service is not in use |

| 6.2.2.2 | Ensure journald ForwardToSyslog is disabled |

| 6.2.2.3 | Ensure journald Compress is configured |

| 6.2.2.4 | Ensure journald Storage is configured |

| 6.2.3.1 | Ensure rsyslog is installed |

| 6.2.3.2 | Ensure rsyslog service is enabled and active |

| 6.2.3.3 | Ensure journald is configured to send logs to rsyslog |

| 6.2.3.4 | Ensure rsyslog log file creation mode is configured |

| 6.2.3.5 | Ensure rsyslog logging is configured |

| 6.2.3.6 | Ensure rsyslog is configured to send logs to a remote log host |

| 6.2.3.7 | Ensure rsyslog is not configured to receive logs from a remote client |

| 6.2.3.8 | Ensure rsyslog logrotate is configured |

| 6.2.4.1 | Ensure access to all logfiles has been configured |

| 6.3.1.1 | Ensure auditd packages are installed |

| 6.3.1.2 | Ensure auditing for processes that start prior to auditd is enabled |

| 6.3.1.3 | Ensure audit\_backlog\_limit is sufficient |

| 6.3.1.4 | Ensure auditd service is enabled and active |

| 6.3.2.1 | Ensure audit log storage size is configured |

| 6.3.2.2 | Ensure audit logs are not automatically deleted |

| 6.3.3.1 | Ensure changes to system administration scope (sudoers) is collected |

| 6.3.3.2 | Ensure actions as another user are always logged |

| 6.3.3.3 | Ensure events that modify the sudo log file are collected |

| 6.3.3.4 | Ensure events that modify date and time information are collected |

| 6.3.3.5 | Ensure events that modify the system's network environment are collected |

| 6.3.3.6 | Ensure use of privileged commands are collected |

| 6.3.3.8 | Ensure events that modify user/group information are collected |

| 6.3.3.9 | Ensure discretionary access control permission modification events are collected |

| 6.3.3.10 | Ensure successful file system mounts are collected |

| 6.3.3.11 | Ensure session initiation information is collected |

| 6.3.3.12 | Ensure login and logout events are collected |

| 6.3.3.13 | Ensure file deletion events by users are collected |

| 6.3.3.14 | Ensure events that modify the system's Mandatory Access Controls are collected |

| 6.3.3.15 | Ensure successful and unsuccessful attempts to use the chcon command are collected |

| 6.3.3.16 | Ensure successful and unsuccessful attempts to use the setfacl command are collected |

| 6.3.3.17 | Ensure successful and unsuccessful attempts to use the chacl command are collected |

| 6.3.3.18 | Ensure successful and unsuccessful attempts to use the usermod command are collected |

| 6.3.3.19 | Ensure kernel module loading unloading and modification is collected |

| 6.3.3.20 | Ensure the audit configuration is immutable |

| 6.3.3.21 | Ensure the running and on disk configuration is the same |

| 6.3.4.1 | Ensure the audit log file directory mode is configured |

| 6.3.4.2 | Ensure audit log files mode is configured |

| 6.3.4.3 | Ensure audit log files owner is configured |

| 6.3.4.4 | Ensure audit log files group owner is configured |

| 6.3.4.5 | Ensure audit configuration files mode is configured |

| 6.3.4.6 | Ensure audit configuration files owner is configured |

| 6.3.4.7 | Ensure audit configuration files group owner is configured |

| 6.3.4.8 | Ensure audit tools mode is configured |

| 6.3.4.9 | Ensure audit tools owner is configured |

| 6.3.4.10 | Ensure audit tools group owner is configured |

| 7.1.1 | Ensure permissions on /etc/passwd are configured |

| 7.1.2 | Ensure permissions on /etc/passwd- are configured |

| 7.1.3 | Ensure permissions on /etc/group are configured |

| 7.1.4 | Ensure permissions on /etc/group- are configured |

| 7.1.5 | Ensure permissions on /etc/shadow are configured |

| 7.1.6 | Ensure permissions on /etc/shadow- are configured |

| 7.1.7 | Ensure permissions on /etc/gshadow are configured |

| 7.1.8 | Ensure permissions on /etc/gshadow- are configured |

| 7.1.9 | Ensure permissions on /etc/shells are configured |

| 7.1.10 | Ensure permissions on /etc/security/opasswd are configured |

| 7.1.11 | Ensure world writable files and directories are secured |

| 7.1.12 | Ensure no files or directories without an owner and a group exist |

| 7.1.13 | Ensure SUID and SGID files are reviewed |

| 7.2.1 | Ensure accounts in /etc/passwd use shadowed passwords |

| 7.2.2 | Ensure /etc/shadow password fields are not empty |

| 7.2.8 | Ensure local interactive user home directories are configured |

| 7.2.9 | Ensure local interactive user dot files access is configured |