Tenable.io Report

cis-amzlnx-level2-hardening

Tue, 20 Jun 2017 10:39:19 UTC

Table Of Contents

Hosts Summary (Executive)

i-0341de1bd15f808d8

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	1	1

Details

Severity	Plugin Id	Name
Info	14272	Netstat Portscanner (SSH)

Compliance Executive

Compliance Tests

PASSED	1.1.1.1 Ensure mounting of cramfs filesystems is disabled
PASSED	1.1.1.2 Ensure mounting of freevxfs filesystems is disabled
PASSED	1.1.1.3 Ensure mounting of jffs2 filesystems is disabled
PASSED	1.1.1.4 Ensure mounting of hfs filesystems is disabled
PASSED	1.1.1.5 Ensure mounting of hfsplus filesystems is disabled
PASSED	1.1.1.6 Ensure mounting of squashfs filesystems is disabled
PASSED	1.1.1.7 Ensure mounting of udf filesystems is disabled
PASSED	1.1.1.8 Ensure mounting of FAT filesystems is disabled
FAILED	1.1.3 Ensure nodev option set on /tmp partition
FAILED	1.1.4 Ensure nosuid option set on /tmp partition
PASSED	1.1.5 Ensure noexec option set on /tmp partition
PASSED	1.1.6 Ensure separate partition exists for /var
FAILED	1.1.7 Ensure separate partition exists for /var/tmp
FAILED	1.1.8 Ensure nodev option set on /var/tmp partition
FAILED	1.1.9 Ensure nosuid option set on /var/tmp partition
FAILED	1.1.10 Ensure noexec option set on /var/tmp partition
PASSED	1.1.11 Ensure separate partition exists for /var/log
PASSED	1.1.12 Ensure separate partition exists for /var/log/audit
PASSED	1.1.13 Ensure separate partition exists for /home
PASSED	1.1.14 Ensure nodev option set on /home partition
FAILED	1.1.15 Ensure nodev option set on /dev/shm partition
FAILED	1.1.16 Ensure nosuid option set on /dev/shm partition
FAILED	1.1.17 Ensure noexec option set on /dev/shm partition
PASSED	1.1.18 Ensure sticky bit is set on all world-writable directories
PASSED	1.1.19 Disable Automounting
WARNING	1.2.1 Ensure package manager repositories are configured
FAILED	1.2.2 Ensure GPG keys are configured
PASSED	1.2.3 Ensure gpgcheck is globally activated
PASSED	1.3.1 Ensure AIDE is installed
PASSED	1.3.2 Ensure filesystem integrity is regularly checked

PASSED 1.4.1 Ensure permissions on bootloader config are configured

PASSED 1.4.2 Ensure authentication required for single user mode

PASSED 1.4.3 Ensure interactive boot is not enabled

PASSED 1.5.1 Ensure core dumps are restricted - fs.suid_dump = 0

PASSED 1.5.1 Ensure core dumps are restricted - hard core = 0

PASSED 1.5.2 Ensure XD/NX support is enabled

PASSED 1.5.3 Ensure address space layout randomization (ASLR) is enabled

PASSED 1.5.4 Ensure prelink is disabled

PASSED 1.6.1.1 Ensure SELinux is not disabled in bootloader configuration - enforcing = 0

PASSED 1.6.1.1 Ensure SELinux is not disabled in bootloader configuration - selinux = 0

PASSED 1.6.1.2 Ensure the SELinux state is enforcing

PASSED 1.6.1.3 Ensure SELinux policy is configured

PASSED 1.6.1.4 Ensure SETroubleshoot is not installed

PASSED 1.6.1.5 Ensure the MCS Translation Service (mcstrans) is not installed

FAILED 1.6.1.6 Ensure no unconfined daemons exist

PASSED 1.6.2 Ensure SELinux is installed

FAILED 1.7.1.1 Ensure message of the day is configured properly

FAILED 1.7.1.2 Ensure local login warning banner is configured properly

FAILED 1.7.1.3 Ensure remote login warning banner is configured properly

PASSED 1.7.1.4 Ensure permissions on /etc/motd are configured

PASSED 1.7.1.5 Ensure permissions on /etc/issue are configured

PASSED 1.7.1.6 Ensure permissions on /etc/issue.net are configured

WARNING 1.8 Ensure updates, patches, and additional security software are installed

PASSED 2.1.1 Ensure chargen services are not enabled - chargen-dgram

PASSED 2.1.1 Ensure chargen services are not enabled - chargen-stream

PASSED 2.1.2 Ensure daytime services are not enabled - daytime-dgram

PASSED 2.1.2 Ensure daytime services are not enabled - daytime-stream

PASSED 2.1.3 Ensure discard services are not enabled - discard-dgram

PASSED 2.1.3 Ensure discard services are not enabled - discard-stream

PASSED 2.1.4 Ensure echo services are not enabled - echo-dgram

PASSED 2.1.4 Ensure echo services are not enabled - echo-stream

PASSED 2.1.5 Ensure time services are not enabled - time-dgram

PASSED 2.1.5 Ensure time services are not enabled - time-stream

PASSED 2.1.6 Ensure rsh server is not enabled - rexec

PASSED 2.1.6 Ensure rsh server is not enabled - rlogin

PASSED 2.1.6 Ensure rsh server is not enabled - rsh

PASSED 2.1.7 Ensure talk server is not enabled

PASSED 2.1.8 Ensure telnet server is not enabled

PASSED 2.1.9 Ensure tftp server is not enabled

PASSED 2.1.10 Ensure rsync service is not enabled

PASSED 2.1.11 Ensure xinetd is not enabled

PASSED 2.2.1.1 Ensure time synchronization is in use

FAILED 2.2.1.2 Ensure ntp is configured 'OPTIONS=-u ntp:ntp'

FAILED 2.2.1.2 Ensure ntp is configured 'remote server'

PASSED 2.2.1.2 Ensure ntp is configured 'restrict -4'

PASSED 2.2.1.2 Ensure ntp is configured 'restrict -6'

PASSED 2.2.2 Ensure X Window System is not installed

PASSED 2.2.3 Ensure Avahi Server is not enabled

PASSED 2.2.4 Ensure CUPS is not enabled

PASSED 2.2.5 Ensure DHCP Server is not enabled

PASSED 2.2.6 Ensure LDAP server is not enabled

PASSED 2.2.7 Ensure NFS and RPC are not enabled - NFS

PASSED 2.2.7 Ensure NFS and RPC are not enabled - RPC

PASSED 2.2.8 Ensure DNS Server is not enabled

PASSED 2.2.9 Ensure FTP Server is not enabled

PASSED 2.2.10 Ensure HTTP server is not enabled

PASSED 2.2.11 Ensure IMAP and POP3 server is not enabled

PASSED 2.2.12 Ensure Samba is not enabled

PASSED 2.2.13 Ensure HTTP Proxy Server is not enabled

PASSED 2.2.14 Ensure SNMP Server is not enabled

FAILED 2.2.15 Ensure mail transfer agent is configured for local-only mode

PASSED 2.2.16 Ensure NIS Server is not enabled

PASSED 2.3.1 Ensure NIS Client is not installed

PASSED 2.3.2 Ensure rsh client is not installed

PASSED 2.3.3 Ensure talk client is not installed

PASSED 2.3.4 Ensure telnet client is not installed

PASSED 2.3.5 Ensure LDAP client is not installed

PASSED 3.1.1 Ensure IP forwarding is disabled

PASSED 3.1.2 Ensure packet redirect sending is disabled 'net.ipv4.conf.all.send_redirects = 0'

PASSED 3.1.2 Ensure packet redirect sending is disabled - 'net.ipv4.conf.default.send_redirects = 0'

PASSED 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.all.accept_source_route = 0'

PASSED 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.default.accept_source_route = 0'

PASSED 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.all.accept_redirects = 0'

PASSED 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects = 0'

PASSED 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects = 0'

PASSED 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects = 0'

PASSED 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians = 1'

PASSED 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians = 1'

PASSED 3.2.5 Ensure broadcast ICMP requests are ignored

PASSED 3.2.6 Ensure bogus ICMP responses are ignored

PASSED 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.all.rp_filter = 1'

PASSED 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.default.rp_filter = 1'

PASSED 3.2.8 Ensure TCP SYN Cookies is enabled

PASSED 3.3.1 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.all.accept_ra = 0'

PASSED 3.3.1 Ensure IPv6 router advertisements are not accepted - 'net.ipv6.conf.default.accept_ra = 0'

PASSED 3.3.2 Ensure IPv6 redirects are not accepted - 'net.ipv6.conf.all.accept_redirects = 0'

PASSED 3.3.2 Ensure IPv6 redirects are not accepted - 'net.ipv6.conf.default.accept_redirects = 0'

PASSED 3.3.3 Ensure IPv6 is disabled

PASSED 3.4.1 Ensure TCP Wrappers is installed

FAILED 3.4.2 Ensure /etc/hosts.allow is configured

PASSED 3.4.3 Ensure /etc/hosts.deny is configured

PASSED 3.4.4 Ensure permissions on /etc/hosts.allow are configured

PASSED 3.4.5 Ensure permissions on /etc/hosts.deny are 644

PASSED 3.5.1 Ensure DCCP is disabled

PASSED 3.5.2 Ensure SCTP is disabled

PASSED 3.5.3 Ensure RDS is disabled

PASSED 3.5.4 Ensure TIPC is disabled

PASSED 3.6.1 Ensure iptables is installed

FAILED 3.6.2 Ensure default deny firewall policy - Chain FORWARD

FAILED 3.6.2 Ensure default deny firewall policy - Chain INPUT

FAILED 3.6.2 Ensure default deny firewall policy - Chain OUTPUT

WARNING 3.6.3 Ensure loopback traffic is configured

WARNING 3.6.4 Ensure outbound and established connections are configured

WARNING 3.6.5 Ensure firewall rules exist for all open ports

FAILED 4.1.1.1 Ensure audit log storage size is configured

PASSED 4.1.1.2 Ensure system is disabled when audit logs are full - 'action_mail_acct is configured'

PASSED 4.1.1.2 Ensure system is disabled when audit logs are full - 'admin_space_left_action'

PASSED 4.1.1.2 Ensure system is disabled when audit logs are full - 'space_left_action is configured'

PASSED 4.1.1.3 Ensure audit logs are not automatically deleted

PASSED 4.1.2 Ensure auditd service is enabled

FAILED 4.1.3 Ensure auditing for processes that start prior to auditd is enabled

FAILED 4.1.4 Ensure events that modify date and time information are collected - /etc/localtime

FAILED 4.1.4 Ensure events that modify date and time information are collected - adjtimex

FAILED 4.1.4 Ensure events that modify date and time information are collected - clock_settime

PASSED 4.1.5 Ensure events that modify user/group information are collected - '/etc/group'

PASSED 4.1.5 Ensure events that modify user/group information are collected - '/etc/gshadow'

PASSED 4.1.5 Ensure events that modify user/group information are collected - '/etc/passwd'

PASSED 4.1.5 Ensure events that modify user/group information are collected - '/etc/security/opasswd'

PASSED 4.1.5 Ensure events that modify user/group information are collected - '/etc/shadow'

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - 32b sethostname

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - 64b sethostname

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - /etc/hosts

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - /etc/sysconfig/network

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - issue

PASSED 4.1.6 Ensure events that modify the system's network environment are collected - issue.net

PASSED 4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected

PASSED 4.1.8 Ensure login and logout events are collected - /var/log/lastlog

FAILED 4.1.8 Ensure login and logout events are collected - /var/run/faillock/

PASSED 4.1.9 Ensure session initiation information is collected - btmp

PASSED 4.1.9 Ensure session initiation information is collected - utmp

PASSED 4.1.9 Ensure session initiation information is collected - wtmp

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - b64 chmod/fchmod/fchmodat

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - b64 chown/fchown/fchownat/lchown

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - b64 setxattr/lsetxattr/fsetxattr/removexattr

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - chmod/fchmod/fchmodat

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - chown/fchown/fchownat/lchown

PASSED 4.1.10 Ensure discretionary access control permission modification events are collected - setxattr/lsetxattr/fsetxattr/removexattr

FAILED 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EACCES

FAILED 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - EPERM

FAILED 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - b64 EACCES

FAILED 4.1.11 Ensure unsuccessful unauthorized file access attempts are collected - b64 EPERM

FAILED 4.1.12 Ensure use of privileged commands is collected

PASSED 4.1.13 Ensure successful file system mounts are collected - b64 mounts

PASSED 4.1.13 Ensure successful file system mounts are collected - mounts

PASSED 4.1.14 Ensure file deletion events by users are collected

PASSED 4.1.14 Ensure file deletion events by users are collected - b64

FAILED 4.1.15 Ensure changes to system administration scope (sudoers) is collected

PASSED 4.1.16 Ensure system administrator actions (sudolog) are collected

PASSED 4.1.17 Ensure kernel module loading and unloading is collected - b64 init_module/delete_module

PASSED 4.1.17 Ensure kernel module loading and unloading is collected - insmod

PASSED 4.1.17 Ensure kernel module loading and unloading is collected - modprobe

PASSED 4.1.17 Ensure kernel module loading and unloading is collected - rmmod

FAILED 4.1.18 Ensure the audit configuration is immutable

PASSED 4.2.1.1 Ensure rsyslog Service is enabled

WARNING 4.2.1.2 Ensure logging is configured

PASSED 4.2.1.3 Ensure rsyslog default file permissions configured

FAILED 4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

PASSED 4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts. - InputTCPServerRun 514

PASSED 4.2.1.5 Ensure remote rsyslog messages are only accepted on designated log hosts. - imtcp.so

PASSED 4.2.3 Ensure rsyslog or syslog-ng is installed

FAILED 4.2.4 Ensure permissions on all logfiles are configured

WARNING 4.3 Ensure logrotate is configured

PASSED 5.1.1 Ensure cron daemon is enabled

PASSED 5.1.2 Ensure permissions on /etc/crontab are configured

PASSED 5.1.3 Ensure permissions on /etc/cron.hourly are configured

PASSED 5.1.4 Ensure permissions on /etc/cron.daily are configured

PASSED 5.1.5 Ensure permissions on /etc/cron.weekly are configured

PASSED 5.1.6 Ensure permissions on /etc/cron.monthly are configured

PASSED 5.1.7 Ensure permissions on /etc/cron.d are configured

FAILED 5.1.8 Ensure at/cron is restricted to authorized users - at.deny

FAILED 5.1.8 Ensure at/cron is restricted to authorized users - cron.deny

PASSED 5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

PASSED 5.2.2 Ensure SSH Protocol is set to 2

PASSED 5.2.3 Ensure SSH LogLevel is set to INFO

PASSED 5.2.4 Ensure SSH X11 forwarding is disabled

PASSED 5.2.5 Ensure SSH MaxAuthTries is set to 4 or less

PASSED 5.2.6 Ensure SSH IgnoreRhosts is enabled

PASSED 5.2.7 Ensure SSH HostbasedAuthentication is disabled

PASSED 5.2.8 Ensure SSH root login is disabled

PASSED 5.2.9 Ensure SSH PermitEmptyPasswords is disabled

PASSED 5.2.10 Ensure SSH PermitUserEnvironment is disabled

PASSED 5.2.11 Ensure only approved ciphers are used

PASSED 5.2.12 Ensure only approved MAC algorithms are used

PASSED 5.2.13 Ensure SSH Idle Timeout Interval is configured - ClientAliveCountMax

PASSED 5.2.13 Ensure SSH Idle Timeout Interval is configured - ClientAliveInterval

PASSED 5.2.14 Ensure SSH LoginGraceTime is set to one minute or less

PASSED 5.2.15 Ensure SSH access is limited

PASSED 5.2.16 Ensure SSH warning banner is configured

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth dcredit

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth lcredit

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth minlen

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth ocredit

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth retry=3

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth try_first_pass

FAILED 5.3.1 Ensure password creation requirements are configured - password-auth ucredit

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth dcredit

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth lcredit

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth minlen

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth ocredit

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth retry=3

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth try_first_pass

FAILED 5.3.1 Ensure password creation requirements are configured - system-auth ucredit

FAILED 5.3.2 Lockout for failed password attempts - password-auth 'auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900'

FAILED 5.3.2 Lockout for failed password attempts - password-auth 'auth [success=1 default=bad] pam_unix.so'

FAILED 5.3.2 Lockout for failed password attempts - password-auth 'auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900'

FAILED 5.3.2 Lockout for failed password attempts - password-auth 'auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900'

FAILED 5.3.2 Lockout for failed password attempts - system-auth 'auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900'

FAILED 5.3.2 Lockout for failed password attempts - system-auth 'auth [success=1 default=bad] pam_unix.so'

FAILED 5.3.2 Lockout for failed password attempts - system-auth 'auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900'

FAILED 5.3.2 Lockout for failed password attempts - system-auth 'auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900'

FAILED 5.3.3 Ensure password reuse is limited - password-auth

FAILED 5.3.3 Ensure password reuse is limited - system-auth

PASSED 5.3.4 Ensure password hashing algorithm is SHA-512 - password-auth

PASSED 5.3.4 Ensure password hashing algorithm is SHA-512 - system-auth

PASSED 5.4.1.1 Ensure password expiration is 90 days or less

PASSED 5.4.1.2 Ensure minimum days between password changes is 7 or more

PASSED 5.4.1.3 Ensure password expiration warning days is 7 or more

PASSED 5.4.1.4 Ensure inactive password lock is 30 days or less

FAILED 5.4.2 Ensure system accounts are non-login

PASSED 5.4.3 Ensure default group for the root account is GID 0

FAILED 5.4.4 Ensure default user umask is 027 or more restrictive - /etc/bashrc

FAILED 5.4.4 Ensure default user umask is 027 or more restrictive - /etc/profile

PASSED 5.5 Ensure access to the su command is restricted - pam_wheel.so

PASSED 5.5 Ensure access to the su command is restricted - wheel group contains root

FAILED 6.1.1 Audit system file permissions

PASSED 6.1.2 Ensure permissions on /etc/passwd are configured

PASSED 6.1.3 Ensure permissions on /etc/shadow are configured

PASSED 6.1.4 Ensure permissions on /etc/group are configured

PASSED 6.1.5 Ensure permissions on /etc/gshadow are configured

PASSED 6.1.6 Ensure permissions on /etc/passwd- are configured

PASSED 6.1.7 Ensure permissions on /etc/shadow- are configured

PASSED 6.1.8 Ensure permissions on /etc/group- are configured

PASSED 6.1.9 Ensure permissions on /etc/gshadow- are configured

PASSED 6.1.10 Ensure no world writable files exist

FAILED 6.1.11 Ensure no unowned files or directories exist

FAILED 6.1.12 Ensure no ungrouped files or directories exist

FAILED 6.1.13 Audit SUID executables

FAILED 6.1.14 Audit SGID executables

PASSED 6.2.1 Ensure password fields are not empty

PASSED 6.2.2 Ensure no legacy '+' entries exist in /etc/passwd

PASSED 6.2.3 Ensure no legacy '+' entries exist in /etc/shadow

PASSED 6.2.4 Ensure no legacy '+' entries exist in /etc/group

PASSED 6.2.5 Ensure root is the only UID 0 account

PASSED 6.2.6 Ensure root PATH Integrity

PASSED 6.2.7 Ensure all users' home directories exist

FAILED 6.2.8 Ensure users' home directories permissions are 750 or more restrictive

PASSED 6.2.9 Ensure users own their home directories

PASSED 6.2.10 Ensure users' dot files are not group or world writable

PASSED 6.2.11 Ensure no users have .forward files

PASSED 6.2.12 Ensure no users have .netrc files

PASSED 6.2.13 Ensure users' .netrc Files are not group or world accessible

PASSED 6.2.14 Ensure no users have .rhosts files

PASSED 6.2.15 Ensure all groups in /etc/passwd exist in /etc/group

PASSED 6.2.16 Ensure no duplicate UIDs exist

PASSED 6.2.17 Ensure no duplicate GIDs exist

PASSED 6.2.18 Ensure no duplicate user names exist

PASSED 6.2.19 Ensure no duplicate group names exist

PASSED CIS Amazon Linux Benchmark Level 1

PASSED CIS Amazon Linux Benchmark Level 2