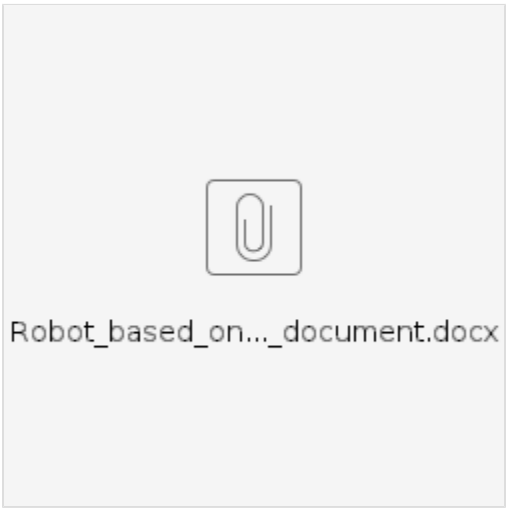
Robot basic architecture based on SSES Test Documentation

Test document

Robot_based_on_SSES_BP_Test_document.pdf

*The following word file is base file of the above pdf.



Pass (16/16 test cases)

Vuls

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/sses-vuls/

IoT Gateway

There are 23 CVEs with a CVSS score >= 9.0. These are exceptions requested here:

Release 5: Akraino CVE Vulnerability Exception Request

CVE-ID	CVSS	NVD	Fix/Notes	PACKAGES
CVE-2016-1585	9.8	https://nvd.nist.gov/vuln/detail/CVE-2016-1585	No fix available	apparmor
CVE-2017-18201	9.8	https://nvd.nist.gov/vuln/detail/CVE-2017-18201	No fix available	libcdio17
CVE-2017-7827	9.8	https://nvd.nist.gov/vuln/detail/CVE-2017-7827	No fix available	libmozjs-52-0
CVE-2018-5090	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5090	Reported fixed in 58 and later version (installed), but still reported by Vuls	libmozjs-52-0
CVE-2018-5126	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5126	Reported fixed in 58 and later version (installed), but still reported by Vuls	libmozjs-52-0
CVE-2018-5145	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5145	Reported fixed in 1:52.7.0 and later version (installed), but still reported by Vuls	libmozjs-52-0
CVE-2018-5151	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5151	Reported fixed in 60 and later version (installed), but still reported by Vuls	libmozjs-52-0
CVE-2019-17041	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-17041	No fix available	rsyslog
CVE-2019-17042	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-17042	No fix available	rsyslog

CVE-2021-31870	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31870	No fix available	klibc-utils, libklibc
CVE-2021-31872	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31872	No fix available	klibc-utils, libklibc
CVE-2021-31873	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-31873	No fix available	klibc-utils, libklibc
CVE-2021-39713	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-39713	No fix available	linux-image-5.4.0-1055-raspi
CVE-2022-22822	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-22822	install firefox 99.0+build2-0ubuntu0.18.04.2 > 98(fix version)	firefox
CVE-2022-22823	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-22823	install firefox 99.0+build2-0ubuntu0.18.04.2 > 98(fix version)	firefox
CVE-2022-22824	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-22824	install firefox 99.0+build2-0ubuntu0.18.04.2 > 98(fix version)	firefox
CVE-2022-23852	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23852	No fix available	firefox, thunderbird
CVE-2022-23990	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23990	No fix available	firefox, thunderbird
CVE-2022-25235	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25235	No fix available	firefox, thunderbird
CVE-2022-25236	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25236	No fix available	firefox, thunderbird
CVE-2022-25315	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25315	No fix available	firefox, thunderbird
CVE-2016-9180	9.1	https://nvd.nist.gov/vuln/detail/CVE-2016-9180	No fix available	libxml-twig-perl
CVE-2019-20433	9.1	https://nvd.nist.gov/vuln/detail/CVE-2019-20433	No fix available	aspell

PC/Server for robot control

There are 30 CVEs with a CVSS score >= 9.0. These are exceptions requested here:

Release 5: Akraino CVE Vulnerability Exception Request

CVE-ID	CVSS	NVD	Fix/Notes	PACKAGES
CVE-2005-2541	10.0	https://nvd.nist.gov/vuln/detail/CVE-2005-2541	No fix available	tar
CVE-2014-2830	10.0	https://nvd.nist.gov/vuln/detail/CVE-2014-2830	No fix available	cifs-utils
CVE-2016-1585	9.8	https://nvd.nist.gov/vuln/detail/CVE-2016-1585	No fix available	libapparmor1
CVE-2017-17479	9.8	https://nvd.nist.gov/vuln/detail/CVE-2017-17479	No fix available	libopenjp2-7
CVE-2017-9117	9.8	https://nvd.nist.gov/vuln/detail/CVE-2017-9117	No fix available	libtiff5
CVE-2018-13410	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-13410	No fix available	zip
CVE-2019-1010022	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-1010022	No fix available	libc-bin, libc-dev-bin, libc-devtools, libc-l10n, libc6, libc6-dbg, libc6-dev, locales
CVE-2019-8341	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8341	No fix available	python3-jinja2
CVE-2020-27619	9.8	https://nvd.nist.gov/vuln/detail/CVE-2020-27619	No fix available	python3.9
CVE-2021-29462	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-29462	No fix available	libixml10, libupnp13
CVE-2021-29921	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-29921	Reported fixed in python3.9 (installed), but still reported by Vuls	python3.9
CVE-2021-30473	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-30473	No fix available	libaom0

CVE-2021-30474	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-30474	No fix available	libaom0
CVE-2021-30475	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-30475	No fix available	libaom0
CVE-2021-30498	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-30498	No fix available	libcaca0
CVE-2021-30499	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-30499	No fix available	libcaca0
CVE-2021-3756	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-3756	install libmysofa 1.2.1	libmysofa1
CVE-2021-42377	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-42377	No fix available	busybox
CVE-2021-45951	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45951	No fix available	dnsmasq
CVE-2021-45952	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45952	No fix available	dnsmasq
CVE-2021-45953	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45953	No fix available	dnsmasq
CVE-2021-45954	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45954	No fix available	dnsmasq
CVE-2021-45955	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45955	No fix available	dnsmasq
CVE-2021-45956	9.8	https://nvd.nist.gov/vuln/detail/CVE-2021-45956	No fix available	dnsmasq
CVE-2022-0318	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-0318	unistall vim	vim
CVE-2022-23303	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23303	No fix available	hostapd, wpasupplicant
CVE-2022-23304	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23304	No fix available	hostapd, wpasupplicant
CVE-2021-22945	9.1	https://nvd.nist.gov/vuln/detail/CVE-2021-22945	unistall curl	curl
CVE-2021-4048	9.1	https://nvd.nist.gov/vuln/detail/CVE-2021-4048	No fix available	libblas3, liblapack3
CVE-2021-43400	9.1	https://nvd.nist.gov/vuln/detail/CVE-2021-43400	No fix available	bluez

Lynis

Nexus URL(before fix): https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/sses-lynis/11

Nexus URL(after fix): https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/sses-lynis/3

The initial results compare with the Lynis Incubation: PASS/FAIL Criteria, v1.0 as follows.

IoT Gateway

The Lynis Program Update test MUST pass with no errors.

```
2022-03-29 22:55:42 Test: Checking for program update...
2022-03-29 22:55:43 Current installed version  : 308
2022-03-29 22:55:43 Latest stable version      : 307
2022-03-29 22:55:43 No Lynis update available.
```

Fix: Download and run the latest Lynis directly on SUT.

Steps To Implement Security Scan Requirements#InstallandExecute

The following list of tests MUST complete as passing

No.	Test	Result	Fix
1	Test: Checking PASS_MAX_DAYS option in /etc/login.defs	Result: password aging limits are not configured Suggestion: Configure maximum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-] Hardening: assigned partial number of hardening points (0 of 1). Currently having 13 points (out of 28)	Set PASS_MAX_DAYS 180 in /etc/login.defs
2	Performing test ID AUTH-9328 (Default umask values)	Test: Checking umask value in /etc/login.defs Result: found umask 022, which could be improved Suggestion: Default umask in /etc/login.defs could be more strict like 027 [test:AUTH-9328] [details:-] [solution:-]	Set UMASK 027 in /etc/login.defs
3	Performing test ID SSH-7440 (Check OpenSSH option: AllowUsers and AllowGroups)	Result: AllowUsers is not set Result: AllowGroups is not set Result: SSH has no specific user or group limitation. Most likely all valid users can SSH to this machine. Hardening: assigned partial number of hardening points (0 of 1). Currently having 140 points (out of 217) Security check: file is normal Checking permissions of /home/ubuntu/lynis/include /tests_snmp File permissions are OK	Configure AllowUsers, AllowGroups in /etc/ssh /sshd_config
4	Test: checking for file /etc/network/if-up.d /ntpdate	Result: file /etc/network/if-up.d/ntpdate does not exist Result: Found a time syncing daemon/client. Hardening: assigned maximum number of hardening points for this item (3). Currently having 149 points (out of 232)	OK
5	Performing test ID KRNL-6000 (Check sysctl key pairs in scan profile) : Following sub-tests required	N/A	N/A
5a	sysctl key fs.suid_dumpable contains equal expected and current value (0)	Result: sysctl key fs.suid_dumpable has a different value than expected in scan profile. Expected=0, Real=2 Hardening: assigned partial number of hardening points (0 of 1). Currently having 151 points (out of 247)	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf echo 'fs.suid_dumpable=0' | sudo tee -a /etc/sysctl.d/90-lynis-hardening.conf sudo /sbin/sysctl --system sudo sysctl -a |grep suid
5b	sysctl key kernel.dmesg_restrict contains equal expected and current value (1)	Result: sysctl key kernel.dmesg_restrict has a different value than expected in scan profile. Expected=1, Real=0	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf echo 'kernel.dmesg_restrict=1' | sudo tee -a /etc/sysctl.d/90-lynis-hardening.conf sudo /sbin/sysctl --system sudo sysctl -a |grep dmesg
5c	sysctl key net.ipv4.conf.default. accept_source_route contains equal expected and current value (0)	Result: sysctl key net.ipv4.conf.default.accept_source_route has a different value than expected in scan profile. Expected=0, Real=1	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf echo 'net.ipv4.conf.default. accept_source_route=0' | sudo tee -a /etc/sysctl.d/90-lynis-hardening.conf sudo /sbin/sysctl --system sudo sysctl -a |grep ipv4.conf.default. accept_source_route
6	Test: Check if one or more compilers can be found on the system	Result: found installed compiler. See top of logfile which compilers have been found or use /bin/grep to filter on 'compiler' Hardening: assigned partial number of hardening points (1 of 3). Currently having 168 points (out of 280)	Uninstall gcc and remove /usr/bin/as

PC/Server for robot control

The Lynis Program Update test MUST pass with no errors.

```
2022-03-23 05:13:56 Test: Checking for program update...
2022-03-23 05:14:03 Current installed version : 308
2022-03-23 05:14:03 Latest stable version : 307
2022-03-23 05:14:03 No Lynis update available
```

Fix: Download and run the latest Lynis directly on SUT.

Steps To Implement Security Scan Requirements#InstallandExecute

The following list of tests MUST complete as passing

No.	Test	Result	Fix
1	Test: Checking PASS_MAX_DAYS option in /etc/login.defs	Result: password aging limits are not configured Suggestion: Configure maximum password age in /etc/login.defs [test:AUTH-9286] [details:-] [solution:-] Hardening: assigned partial number of hardening points (0 of 1). Currently having 11 points (out of 24)	Set PASS_MAX_DAYS 180 in /etc/login.defs
2	Performing test ID AUTH-9328 (Default umask values)	Result: found /etc/profile.d, with one or more files in it	OK
3	Performing test ID SSH-7440 (Check OpenSSH option: AllowUsers and AllowGroups)	Result: AllowUsers is not set Result: AllowGroups is not set Result: SSH has no specific user or group limitation. Most likely all valid users can SSH to this machine. Hardening: assigned partial number of hardening points (0 of 1). Currently having 102 points (out of 155) Security check: file is normal Checking permissions of /home/pi/lynis/lynis/include/tests_snmp File permissions are OK	Configure AllowUsers, AllowGroups in /etc/ssh/sshd_config
4	Test: checking for file /etc/network/if-up.d/ntpdate	Result: file /etc/network/if-up.d/ntpdate does not exist Result: Found a time syncing daemon/client. Hardening: assigned maximum number of hardening points for this item (3). Currently having 111 points (out of 170)	OK
5	Performing test ID KRNL-6000 (Check sysctl key pairs in scan profile) : Following sub-tests required	N/A	N/A
5a	sysctl key fs.suid_dumpable contains equal expected and current value (0)	Result: sysctl key fs.suid_dumpable contains equal expected and current value (0)	OK
5b	sysctl key kernel.dmesg_restrict contains equal expected and current value (1)	Result: sysctl key kernel.dmesg_restrict has a different value than expected in scan profile. Expected=1, Real=0	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf echo 'kernel.dmesg_restrict=1' | sudo tee -a /etc/sysctl.d/90-lynis-hardening.conf sudo /sbin/sysctl --system sudo sysctl -a |grep dmesg
5c	sysctl key net.ipv4.conf.default.accept_source_route contains equal expected and current value (0)	Result: sysctl key net.ipv4.conf.default.accept_source_route has a different value than expected in scan profile. Expected=0, Real=1	Set recommended value in /etc/sysctl.d/90-lynis-hardening.conf echo 'net.ipv4.conf.default.accept_source_route=0' | sudo tee -a /etc/sysctl.d/90-lynis-hardening.conf sudo /sbin/sysctl --system sudo sysctl -a |grep ipv4.conf.default.accept_source_route
6	Test: Check if one or more compilers can be found on the system	Result: found installed compiler. See top of logfile which compilers have been found or use /usr/bin/grep to filter on 'compiler' Hardening: assigned partial number of hardening points (1 of 3). Currently having 128 points (out of 217)	Uninstall gcc and remove /usr/bin/as