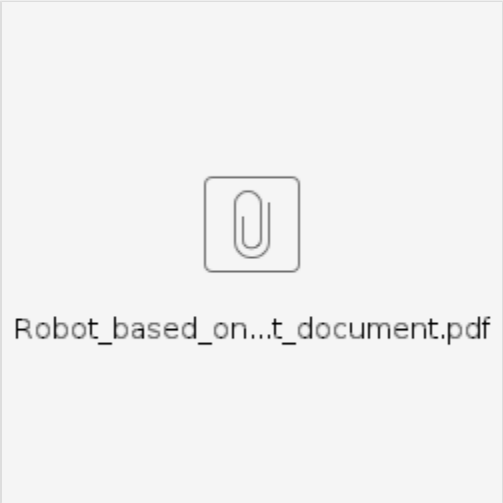
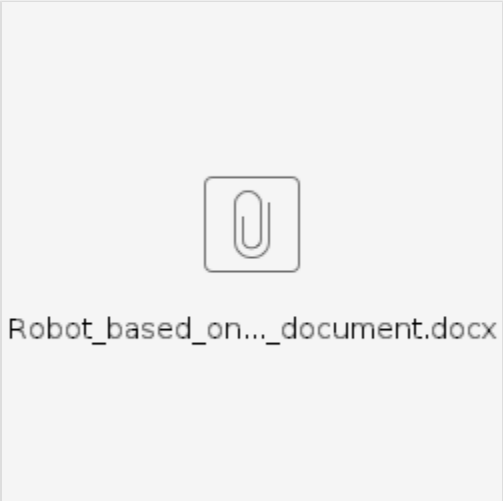
Test Document for release7

Test document



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



Pass (19/19 test cases)

Bluval Tests

Execute with reference to the following

Bluval User Guide

Steps To Implement Security Scan Requirements

https://vuls.io/docs/en/tutorial-docker.html

There are 2 security related tests: lynis & vuls. And there are 2 k8s related tests: kube-hunter & conformance tests.

In this Blueprint, we test lynis & vuls, we do not test k8s related tests: because of not using k8s.

Also refer to Bluval User Guide, the procedure is to clone the files from http://gerrit.akraino.org/r/validation and execute them,

but a configuration file:Bluval/validation/docker/os/Dockerfile does not correspond to this OS version, we execute tests manually.

The Configuration file are only supported up to Ubuntu 18.

Vuls

We use Ubuntu 18.04/22.04 or RaspberryPi(Debian 11), so we ran Vuls test as follows:

1. Create directory

```
$ mkdir ~/vuls
$ cd ~/vuls
$ mkdir go-cve-dictionary-log goval-dictionary-log gost-log
```

2. Fetch NVD

```
$ docker run --rm -it \
    -v $PWD:/go-cve-dictionary \
    -v $PWD/go-cve-dictionary-log:/var/log/go-cve-dictionary \
    vuls/go-cve-dictionary fetch nvd
```

3. Fetch OVAL

   if OS is Ubuntu 18.04/22.04, we use following command,

```
$ docker run --rm -it \
     -v $PWD:/goval-dictionary \
     -v $PWD/goval-dictionary-log:/var/log/goval-dictionary \
     vuls/goval-dictionary fetch ubuntu 18 19 20 21 22
```

   if OS is RaspberryPi(Debian 11), we use following command,

```
$ docker run --rm -it \
     -v $PWD:/goval-dictionary \
     -v $PWD/goval-dictionary-log:/var/log/goval-dictionary \
     vuls/goval-dictionary fetch debian 11
```

4. Fetch gost

   if OS is Ubuntu 18.04/22.04, we use following command,

```
$ docker run --rm -i \
     -v $PWD:/gost \
     -v $PWD/gost-log:/var/log/gost \
     vuls/gost fetch ubuntu
```

   if OS is RaspberryPi(Debian 11), we use following command,

```
$ docker run --rm -i \
     -v $PWD:/gost \
     -v $PWD/gost-log:/var/log/gost \
     vuls/gost fetch debian
```

5. Create config.toml

```
[servers]

[servers.master]
host = "192.168.51.22"
port = "22"
user = "test-user"
keyPath = "/root/.ssh/id_rsa" # path to ssh private key in docker
```

6. Start vuls container to run tests

```
$ docker run --rm -it \
    -v ~/.ssh:/root/.ssh:ro \
    -v $PWD:/vuls \
    -v $PWD/vuls-log:/var/log/vuls \
    -v /etc/localtime:/etc/localtime:ro \
    -v /etc/timezone:/etc/timezone:ro \
    vuls/vuls scan \
    -config=./config.toml
```

7. Get the report

```
$ docker run --rm -it \
     -v ~/.ssh:/root/.ssh:ro \
     -v $PWD:/vuls \
     -v $PWD/vuls-log:/var/log/vuls \
     -v /etc/localtime:/etc/localtime:ro \
     vuls/vuls report \
     -format-list \
     -config=./config.toml
```

Vuls

Nexus URL: https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/R7/sses-vuls/

PDH,IoT Gateway

There are 26 CVEs with a CVSS score >= 9.0. These are exceptions requested here:

Release 7: Akraino CVE and KHV 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	Uninstall firefox $ sudo apt remove firefox*	libmozjs-52-0
CVE-2018-5090	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5090	Uninstall firefox $ sudo apt remove firefox*	libmozjs-52-0
CVE-2018-5126	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5126	Uninstall firefox $ sudo apt remove firefox*	libmozjs-52-0
CVE-2018-5145	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5145	Uninstall firefox $ sudo apt remove firefox*	libmozjs-52-0
CVE-2018-5151	9.8	https://nvd.nist.gov/vuln/detail/CVE-2018-5151	Uninstall firefox $ sudo apt remove firefox*	libmozjs-52-0
CVE-2019-17041	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-17041	Reported fixed in 8.19 and later version (installed), but still reported by Vuls	rsyslog
CVE-2019-17042	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-17042	Reported fixed in 8.19 and later version (installed), but still reported by Vuls	rsyslog

CVE-2019-8287	9.8	https://nvd.nist.gov/vuln/detail/CVE-2019-8287	Uninstall tigervncserver
			$ sudo apt remove tigervnc*
			$ sudo apt-get remove tightvnc* -y
				tightvncserver

CVE-2022-0318	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-0318	Uninstall vim $ sudo apt remove vim*	vim
CVE-2022-23852	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-23852	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	firefox, thunderbird
CVE-2022-24791	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-24791	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	firefox, thunderbird
CVE-2022-25235	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25235	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	firefox, thunderbird
CVE-2022-25236	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25236	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	firefox, thunderbird
CVE-2022-25315	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-25315	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	firefox, thunderbird

CVE-2022-3649	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-3649	No fix available	linux-image-4.15.0-197-generic
CVE-2022-37609	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-37609	Uninstall firefox, thunderbird $ sudo apt remove firefox* thunderbird*	thunderbird
CVE-2022-39394	9.8	https://nvd.nist.gov/vuln/detail/CVE-2022-39394	Uninstall thunderbird $ sudo apt remove thunderbird*	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
CVE-2022-24303	9.1	https://nvd.nist.gov/vuln/detail/CVE-2022-24303	No fix available	python3-pil
CVE-2022-39319	9.1	https://security-tracker.debian.org/tracker/CVE-2022-39319	No fix available	libfreerdp-client2-2, libfreerdp2-2, libwinpr2-2
CVE-2022-41877	9.1	https://nvd.nist.gov/vuln/detail/CVE-2022-41877	No fix available	libfreerdp-client2-2, libfreerdp2-2, libwinpr2-2

PC/Server for robot control

There are 40 CVEs with a CVSS score >= 9.0. These are exceptions requested here:

Release 7: Akraino CVE and KHV Vulnerability Exception Request

CVE-ID	CVSS	NVD	Fix/Notes	PACKAGES
CVE-2016-1585	9.8	https://ubuntu.com/security/CVE-2016-1585	No fix available	apparmor
CVE-2017-18201	9.8	https://ubuntu.com/security/CVE-2017-18201	No fix available	libcdio17
CVE-2017-7827	9.8	https://ubuntu.com/security/CVE-2017-7827	No fix available	libmozjs-52-0
CVE-2018-5090	9.8	https://ubuntu.com/security/CVE-2018-5090	No fix available	libmozjs-52-0
CVE-2018-5126	9.8	https://ubuntu.com/security/CVE-2018-5126	No fix available	libmozjs-52-0
CVE-2018-5145	9.8	https://ubuntu.com/security/CVE-2018-5145	No fix available	libmozjs-52-0
CVE-2018-5151	9.8	https://ubuntu.com/security/CVE-2018-5151	No fix available	libmozjs-52-0
CVE-2019-17041	9.8	https://ubuntu.com/security/CVE-2019-17041	No fix available	rsyslog
CVE-2019-17042	9.8	https://ubuntu.com/security/CVE-2019-17042	No fix available	rsyslog
CVE-2022-0318	9.8	https://ubuntu.com/security/CVE-2022-0318	No fix available	xxd
CVE-2022-3649	9.8	https://ubuntu.com/security/CVE-2022-3649	No fix available	linux-image-4.15.0-197-generic
CVE-2022-3890	9.6	https://ubuntu.com/security/CVE-2022-3890	No fix available	chromium-browser
CVE-2022-4135	9.6	https://ubuntu.com/security/CVE-2022-4135	No fix available	chromium-browser
CVE-2016-9180	9.1	https://ubuntu.com/security/CVE-2016-9180	No fix available	libxml-twig-perl
CVE-2019-20433	9.1	https://ubuntu.com/security/CVE-2019-20433	No fix available	aspell
CVE-2022-24303	9.1	https://ubuntu.com/security/CVE-2022-24303	No fix available	python3-pil

Cloud/Edge Cloud

There are 2 CVEs with a CVSS score >= 9.0.

Release 7: Akraino CVE and KHV Vulnerability Exception Request

CVE-ID	CVSS	NVD	Fix/Notes	PACKAGES
CVE-2016-1585	9.8	https://ubuntu.com/security/CVE-2016-1585	No fix available	apparmor
CVE-2022-3649	9.8	https://ubuntu.com/security/CVE-2022-3649	No fix available	linux-gcp

Lynis

Nexus URL(after fix):

https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/R7/2/sses-lynis/PDH/lynis_PDH_after.log

https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/R7/sses-lynis/Robot/lynis_Robot_after.log

https://nexus.akraino.org/content/sites/logs/fujitsu/job/robot-family/R7/sses-lynis/cloud/lynis_after.log

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

PDF,IoT Gateway

The Lynis Program Update test MUST pass with no errors.

```
2022-11-22 07:46:44 Test: Checking for program update...
2022-11-22 07:46:44 Current installed version  : 308
2022-11-22 07:46:45 Latest stable version      : 308
2022-11-22 07:46:45 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)	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 108 points (out of 157) 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 If you run the lynis shell script as an ordinary user, it will output an error. So run the script as a privileged user. $ su root # whoami root # ./lynis audit system reference https://github.com/CISOfy/lynis/blob/master/include/tests_ssh#L54
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 117 points (out of 172)	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 contains equal expected and current value (1)	OK
5c	sysctl key net.ipv4.conf.default.accept_source_route contains equal expected and current value (0)	Result: sysctl key net.ipv4.conf.all.accept_source_route contains equal expected and current value (0)	OK

6	Test: Check if one or more compilers can be found on the system	Performing test ID HRDN-7220 (Check if one or more compilers are installed) Test: Check if one or more compilers can be found on the system Result: no compilers found Hardening: assigned maximum number of hardening points for this item (3). Currently having 138 points (out of 219)	OK

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 : 308
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	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	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 152 points (out of 223) 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 161 points (out of 238)	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)	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 163 points (out of 253)	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 180 points (out of 286 Found known binary: as (compiler) - /usr/bin/as Found known binary: cc (compiler) - /usr/bin/cc Found known binary: g++ (compiler) - /usr/bin/g++ Found known binary: gcc (compiler) - /usr/bin/gcc	Uninstall gcc and remove /usr/bin/as, /usr/bin/cc

Cloud/Edge Cloud

The Lynis Program Update test MUST pass with no errors.

```
2022-11-28 00:14:35 Test: Checking for program update...
2022-11-28 00:14:35 Current installed version  : 308
2022-11-28 00:14:35 Latest stable version      : 308
2022-11-28 00:14:35 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	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	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 152 points (out of 223)
		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
			
			If you run the lynis shell script as an ordinary user, it will output an error. So run the script as a privileged user.
			
			$ su root
			
			# whoami
			
			root
			
			# ./lynis audit system
			
			`reference`
			
			https://github.com/CISOfy/lynis/blob/master/include/tests_ssh#L54

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 177 points (out of 168)	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)	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 163 points (out of 253)	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 180 points (out of 286 Found known binary: as (compiler) - /usr/bin/as Found known binary: cc (compiler) - /usr/bin/cc Found known binary: g++ (compiler) - /usr/bin/g++ Found known binary: gcc (compiler) - /usr/bin/gcc	Uninstall gcc and remove /usr/bin/as, /usr/bin/cc