Virtualization and Cloud Computing

Exercise 1: Auditing Docker Host Security Using Docker-Bench-Security Tool

Lab Scenario

Docker has been used extensively by organizations that use containers for development or production. Therefore, Docker security plays a key role in safeguarding containers. Although Docker provides many security benefits, its default configuration during installation has some security issues that a network defender must fix.

Lab Objectives

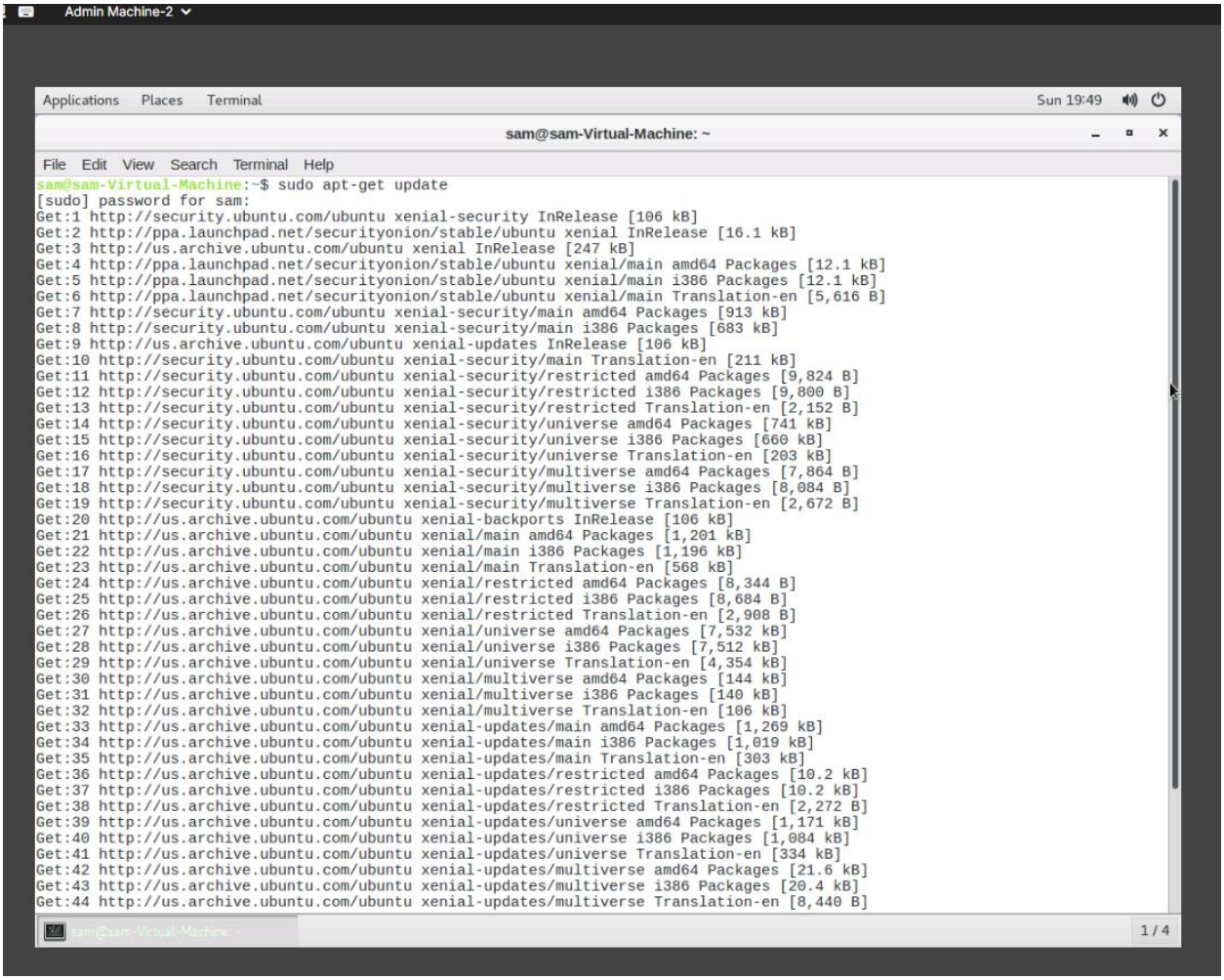
This lab will demonstrate how to audit the security of a default Docker installation on an Ubuntu host using Docker-Bench-Security Tool and how to fix some of the identified security warnings. In this lab, you will learn how to do the following:

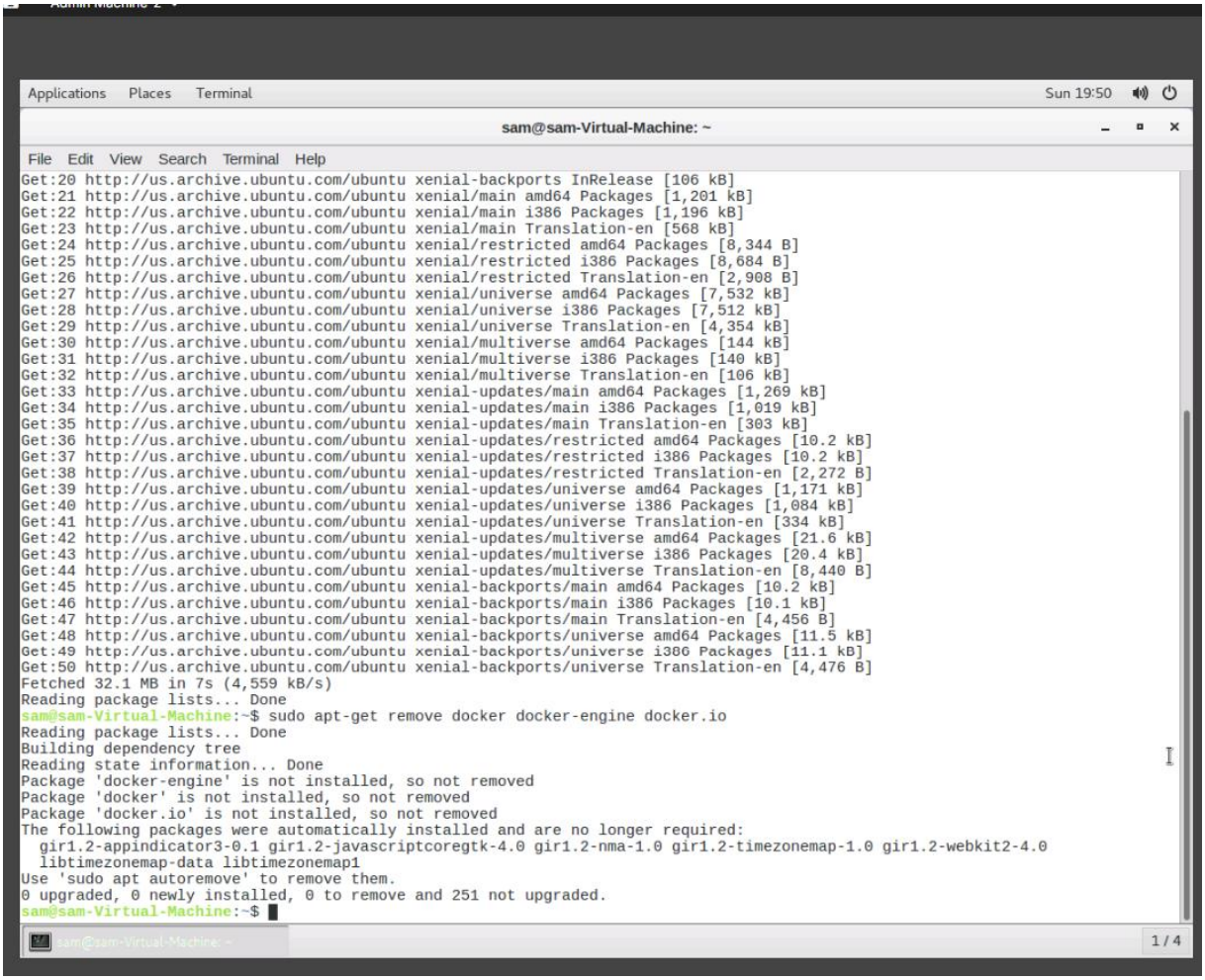
- Install Docker on Ubuntu OS
- Audit Docker Security using Docker-Bench-Security Tool

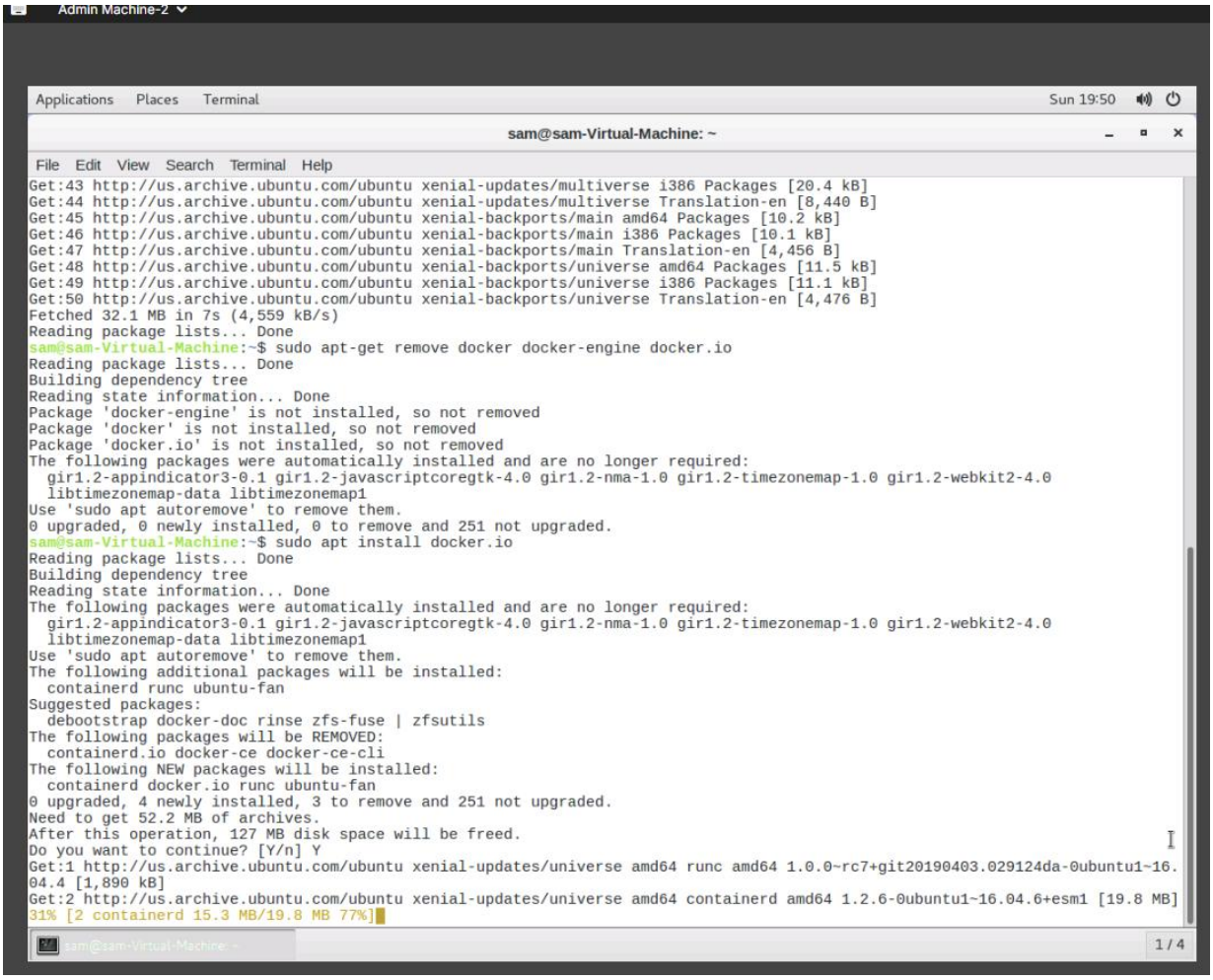
Overview of the Lab

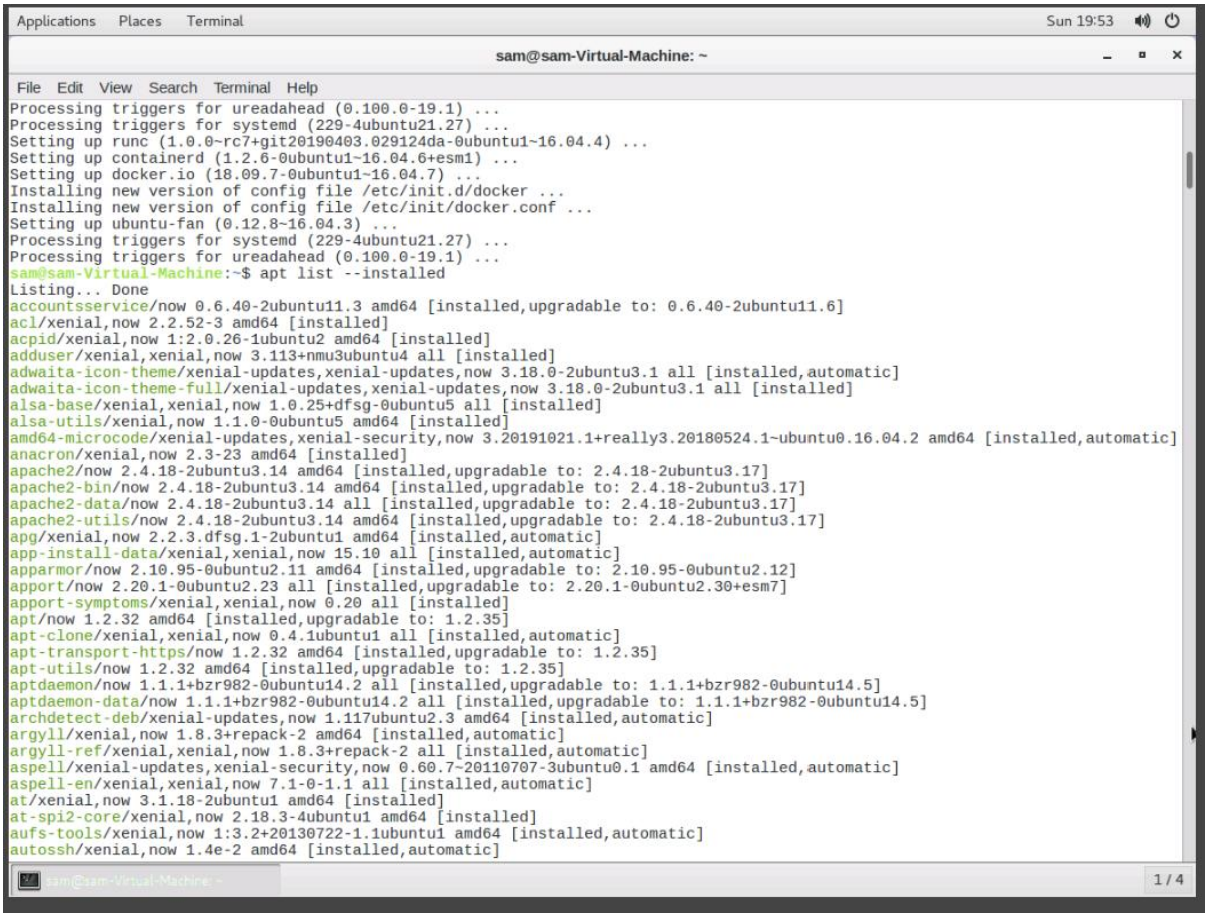
Docker is an open-source technology used for developing, packaging, and running applications, and all its dependencies in the form of containers ensure that the application works in a seamless environment. Docker provides Platform-as-a-Service (PaaS) through OS-level virtualization and delivers containerized software packages. Docker-Bench-Security is a tool for auditing Docker; this tool checks the configuration of Docker and reports the status of a current setting or configuration. Docker configuration status has four categories: note, info, warn, pass.

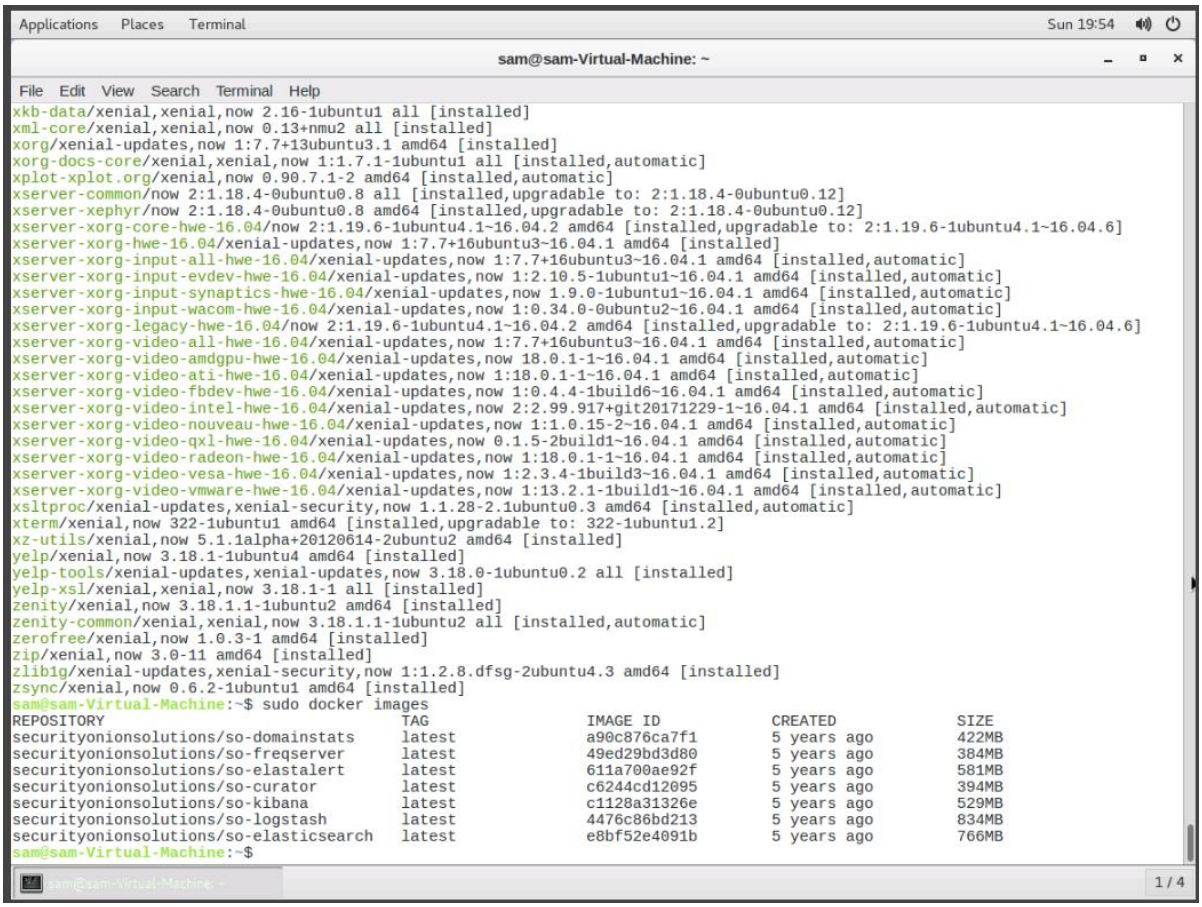
- NOTE shows recommended settings.
- INFO shows the required secure configuration.
- WARN indicates the low-security.
- PASS indicates the protected configuration.

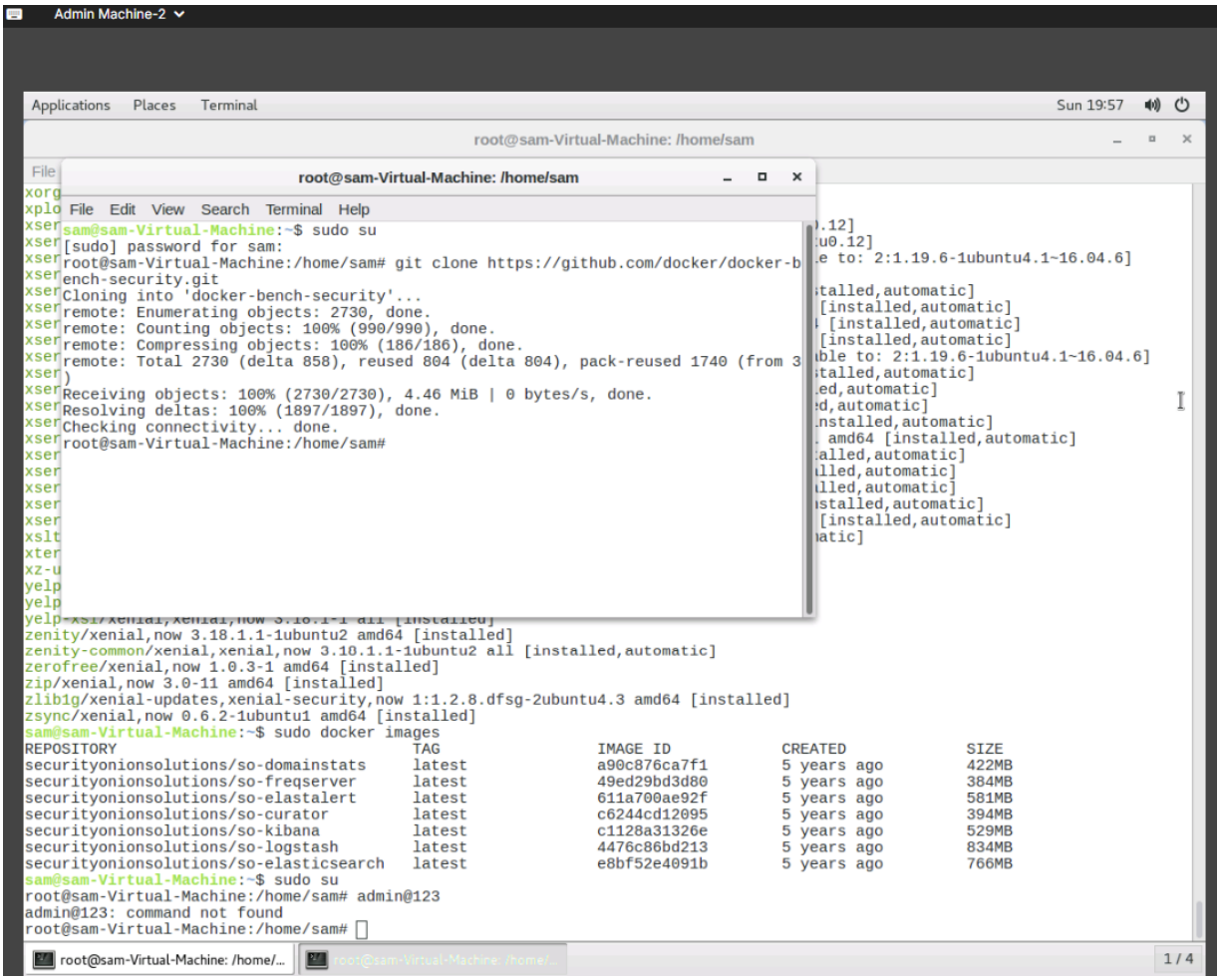

Admin Machine-2
Applications Places Terminal
Sun 19:49
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo apt-get update
[sudo] password for sam:
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial InRelease [16.1 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:4 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial/main amd64 Packages [12.1 kB]
Get:5 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial/main i386 Packages [12.1 kB]
Get:6 http://ppa.launchpad.net/securityonion/stable/ubuntu xenial/main Translation-en [5,616 B]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [913 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [683 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [211 kB]
Get:11 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [9,824 B]
Get:12 http://security.ubuntu.com/ubuntu xenial-security/restricted i386 Packages [9,800 B]
Get:13 http://security.ubuntu.com/ubuntu xenial-security/restricted Translation-en [2,152 B]
Get:14 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [741 kB]
Get:15 http://security.ubuntu.com/ubuntu xenial-security/universe i386 Packages [660 kB]
Get:16 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [203 kB]
Get:17 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [7,864 B]
Get:18 http://security.ubuntu.com/ubuntu xenial-security/multiverse i386 Packages [8,084 B]
Get:19 http://security.ubuntu.com/ubuntu xenial-security/multiverse Translation-en [2,672 B]
Get:20 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu xenial/main i386 Packages [1,196 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu xenial/main Translation-en [568 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [8,344 B]
Get:25 http://us.archive.ubuntu.com/ubuntu xenial/restricted i386 Packages [8,684 B]
Get:26 http://us.archive.ubuntu.com/ubuntu xenial/restricted Translation-en [2,908 B]
Get:27 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:28 http://us.archive.ubuntu.com/ubuntu xenial/universe i386 Packages [7,512 kB]
Get:29 http://us.archive.ubuntu.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:30 http://us.archive.ubuntu.com/ubuntu xenial/multiverse amd64 Packages [144 kB]
Get:31 http://us.archive.ubuntu.com/ubuntu xenial/multiverse i386 Packages [140 kB]
Get:32 http://us.archive.ubuntu.com/ubuntu xenial/multiverse Translation-en [106 kB]
Get:33 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1,269 kB]
Get:34 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [1,019 kB]
Get:35 http://us.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [303 kB]
Get:36 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packages [10.2 kB]
Get:37 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted i386 Packages [10.2 kB]
Get:38 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted Translation-en [2,272 B]
Get:39 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [1,171 kB]
Get:40 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [1,084 kB]
Get:41 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [334 kB]
Get:42 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Packages [21.6 kB]
Get:43 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse i386 Packages [20.4 kB]
Get:44 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translation-en [8,440 B]
sam@sam-Virtual-Machine: ~
1 / 4

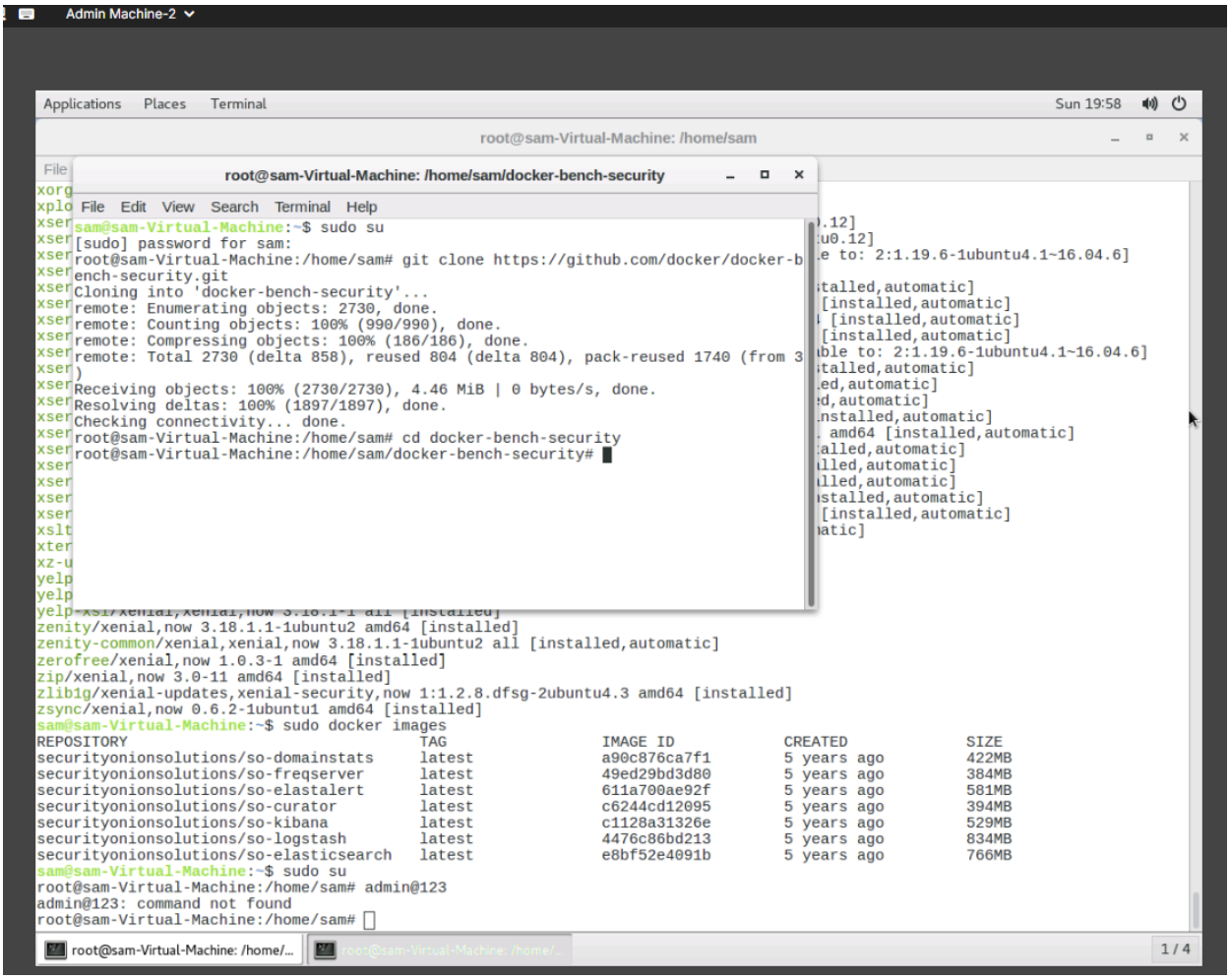

Applications Places Terminal
Sun 19:50
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
Get:20 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:21 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1,201 kB]
Get:22 http://us.archive.ubuntu.com/ubuntu xenial/main i386 Packages [1,196 kB]
Get:23 http://us.archive.ubuntu.com/ubuntu xenial/main Translation-en [568 kB]
Get:24 http://us.archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [8,344 B]
Get:25 http://us.archive.ubuntu.com/ubuntu xenial/restricted i386 Packages [8,684 B]
Get:26 http://us.archive.ubuntu.com/ubuntu xenial/restricted Translation-en [2,908 B]
Get:27 http://us.archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [7,532 kB]
Get:28 http://us.archive.ubuntu.com/ubuntu xenial/universe i386 Packages [7,512 kB]
Get:29 http://us.archive.ubuntu.com/ubuntu xenial/universe Translation-en [4,354 kB]
Get:30 http://us.archive.ubuntu.com/ubuntu xenial/multiverse amd64 Packages [144 kB]
Get:31 http://us.archive.ubuntu.com/ubuntu xenial/multiverse i386 Packages [140 kB]
Get:32 http://us.archive.ubuntu.com/ubuntu xenial/multiverse Translation-en [106 kB]
Get:33 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1,269 kB]
Get:34 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [1,019 kB]
Get:35 http://us.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [303 kB]
Get:36 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packages [10.2 kB]
Get:37 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted i386 Packages [10.2 kB]
Get:38 http://us.archive.ubuntu.com/ubuntu xenial-updates/restricted Translation-en [2,272 B]
Get:39 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [1,171 kB]
Get:40 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [1,084 kB]
Get:41 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-en [334 kB]
Get:42 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Packages [21.6 kB]
Get:43 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse i386 Packages [20.4 kB]
Get:44 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translation-en [8,440 B]
Get:45 http://us.archive.ubuntu.com/ubuntu xenial-backports/main amd64 Packages [10.2 kB]
Get:46 http://us.archive.ubuntu.com/ubuntu xenial-backports/main i386 Packages [10.1 kB]
Get:47 http://us.archive.ubuntu.com/ubuntu xenial-backports/main Translation-en [4,456 B]
Get:48 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Packages [11.5 kB]
Get:49 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe i386 Packages [11.1 kB]
Get:50 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe Translation-en [4,476 B]
Fetched 32.1 MB in 7s (4,559 kB/s)
Reading package lists... Done
sam@sam-Virtual-Machine:~$ sudo apt-get remove docker docker-engine docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'docker-engine' is not installed, so not removed
Package 'docker' is not installed, so not removed
Package 'docker.io' is not installed, so not removed
The following packages were automatically installed and are no longer required:
gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timezonemap-1.0 gir1.2-webkit2-4.0
libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 251 not upgraded.
sam@sam-Virtual-Machine:~$
1 / 4

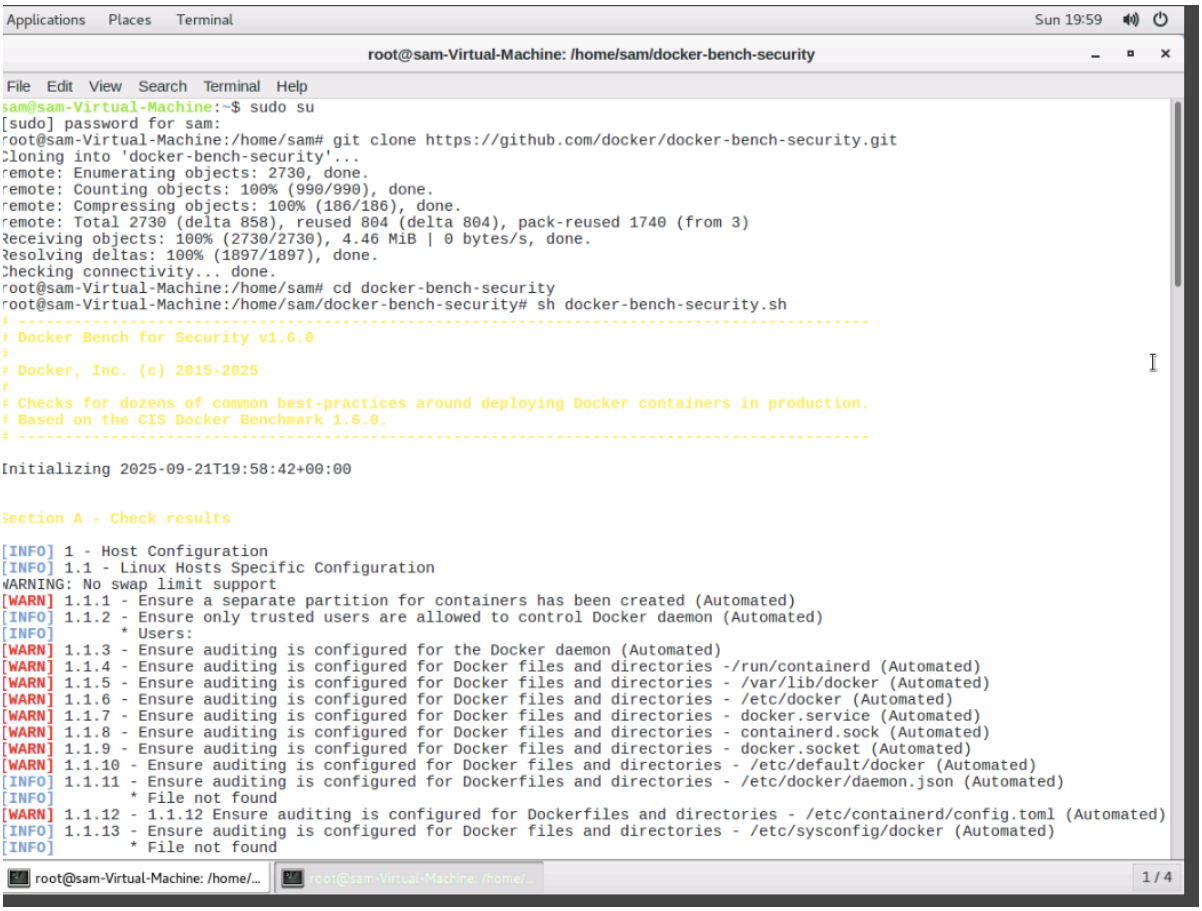

Admin Machine-2
Applications Places Terminal
Sun 19:50
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
Get:43 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse i386 Packages [20.4 kB]
Get:44 http://us.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translation-en [8,440 B]
Get:45 http://us.archive.ubuntu.com/ubuntu xenial-backports/main amd64 Packages [10.2 kB]
Get:46 http://us.archive.ubuntu.com/ubuntu xenial-backports/main i386 Packages [10.1 kB]
Get:47 http://us.archive.ubuntu.com/ubuntu xenial-backports/main Translation-en [4,456 B]
Get:48 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Packages [11.5 kB]
Get:49 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe i386 Packages [11.1 kB]
Get:50 http://us.archive.ubuntu.com/ubuntu xenial-backports/universe Translation-en [4,476 B]
Fetched 32.1 MB in 7s (4,559 kB/s)
Reading package lists... Done
sam@sam-Virtual-Machine:~$ sudo apt-get remove docker docker-engine docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
Package 'docker-engine' is not installed, so not removed
Package 'docker' is not installed, so not removed
Package 'docker.io' is not installed, so not removed
The following packages were automatically installed and are no longer required:
gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timezonemap-1.0 gir1.2-webkit2-4.0
libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 251 not upgraded.
sam@sam-Virtual-Machine:~$ sudo apt install docker.io
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
gir1.2-appindicator3-0.1 gir1.2-javascriptcoregtk-4.0 gir1.2-nma-1.0 gir1.2-timezonemap-1.0 gir1.2-webkit2-4.0
libtimezonemap-data libtimezonemap1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
containerd runc ubuntu-fan
Suggested packages:
debootstrap docker-doc rinse zfs-fuse | zfsutils
The following packages will be REMOVED:
containerd.io docker-ce docker-ce-cli
The following NEW packages will be installed:
containerd docker.io runc ubuntu-fan
0 upgraded, 4 newly installed, 3 to remove and 251 not upgraded.
Need to get 52.2 MB of archives.
After this operation, 127 MB disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 runc amd64 1.0.0~rc7+git20190403.029124da-0ubuntu1~16.04.4 [1,890 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 containerd amd64 1.2.6-0ubuntu1~16.04.6+esm1 [19.8 MB]
31% [2 containerd 15.3 MB/19.8 MB 77%]
sam@sam-Virtual-Machine: ~
1 / 4


Applications Places Terminal
Sun 19:53
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
Processing triggers for ureadahead (0.100.0-19.1) ...
Processing triggers for systemd (229-4ubuntu21.27) ...
Setting up runc (1.0.0~rc7+git20190403.029124da-0ubuntu1~16.04.4) ...
Setting up containerd (1.2.6-0ubuntu1~16.04.6+esm1) ...
Setting up docker.io (18.09.7-0ubuntu1~16.04.7) ...
Installing new version of config file /etc/init.d/docker ...
Installing new version of config file /etc/init/docker.conf ...
Setting up ubuntu-fan (0.12.8~16.04.3) ...
Processing triggers for systemd (229-4ubuntu21.27) ...
Processing triggers for ureadahead (0.100.0-19.1) ...
sam@sam-Virtual-Machine:~$ apt list --installed
Listing... Done
accountsservice/now 0.6.40-2ubuntu11.3 amd64 [installed,upgradable to: 0.6.40-2ubuntu11.6]
acl/xenial,now 2.2.52-3 amd64 [installed]
acpid/xenial,now 1:2.0.26-1ubuntu2 amd64 [installed]
adduser/xenial,xenial,now 3.113+nmu3ubuntu4 all [installed]
adwaita-icon-theme/xenial-updates,xenial-updates,now 3.18.0-2ubuntu3.1 all [installed,automatic]
adwaita-icon-theme-full/xenial-updates,xenial-updates,now 3.18.0-2ubuntu3.1 all [installed]
alsa-base/xenial,xenial,now 1.0.25+dfsg-0ubuntu5 all [installed]
alsa-utils/xenial,now 1.1.0-0ubuntu5 amd64 [installed]
amd64-microcode/xenial-updates,xenial-security,now 3.20191021.1+really3.20180524.1~ubuntu0.16.04.2 amd64 [installed,automatic]
anacron/xenial,now 2.3-23 amd64 [installed]
apache2/now 2.4.18-2ubuntu3.14 amd64 [installed,upgradable to: 2.4.18-2ubuntu3.17]
apache2-bin/now 2.4.18-2ubuntu3.14 amd64 [installed,upgradable to: 2.4.18-2ubuntu3.17]
apache2-data/now 2.4.18-2ubuntu3.14 all [installed,upgradable to: 2.4.18-2ubuntu3.17]
apache2-utils/now 2.4.18-2ubuntu3.14 amd64 [installed,upgradable to: 2.4.18-2ubuntu3.17]
apg/xenial,now 2.2.3.dfsg.1-2ubuntu1 amd64 [installed,automatic]
app-install-data/xenial,xenial,now 15.10 all [installed,automatic]
apparmor/now 2.10.95-0ubuntu2.11 amd64 [installed,upgradable to: 2.10.95-0ubuntu2.12]
apport/now 2.20.1-0ubuntu2.23 all [installed,upgradable to: 2.20.1-0ubuntu2.30+esm7]
apport-symptoms/xenial,xenial,now 0.20 all [installed]
apt/now 1.2.32 amd64 [installed,upgradable to: 1.2.35]
apt-clone/xenial,xenial,now 0.4.1ubuntu1 all [installed,automatic]
apt-transport-https/now 1.2.32 amd64 [installed,upgradable to: 1.2.35]
apt-utils/now 1.2.32 amd64 [installed,upgradable to: 1.2.35]
aptdaemon/now 1.1.1+bzr982-0ubuntu14.2 all [installed,upgradable to: 1.1.1+bzr982-0ubuntu14.5]
aptdaemon-data/now 1.1.1+bzr982-0ubuntu14.2 all [installed,upgradable to: 1.1.1+bzr982-0ubuntu14.5]
archdetect-deb/xenial-updates,now 1.117ubuntu2.3 amd64 [installed,automatic]
argyll/xenial,now 1.8.3+repack-2 amd64 [installed,automatic]
argyll-ref/xenial,xenial,now 1.8.3+repack-2 all [installed,automatic]
aspell/xenial-updates,xenial-security,now 0.60.7~20110707-3ubuntu0.1 amd64 [installed,automatic]
aspell-en/xenial,xenial,now 7.1-0-1.1 all [installed,automatic]
at/xenial,now 3.1.18-2ubuntu1 amd64 [installed]
at-spi2-core/xenial,now 2.18.3-4ubuntu1 amd64 [installed]
aufs-tools/xenial,now 1:3.2+20130722-1.1ubuntu1 amd64 [installed,automatic]
autossh/xenial,now 1.4e-2 amd64 [installed,automatic]
sam@sam-Virtual-Machine: ~
1 / 4


Applications Places Terminal
Sun 19:54
sam@sam-Virtual-Machine: ~
File Edit View Search Terminal Help
xkb-data/xenial,xenial,now 2.16-1ubuntu1 all [installed]
xml-core/xenial,xenial,now 0.13+nmu2 all [installed]
xorg/xenial-updates,now 1:7.7+13ubuntu3.1 amd64 [installed]
xorg-docs-core/xenial,xenial,now 1:1.7.1-1ubuntu1 all [installed,automatic]
xplot-xplot.org/xenial,now 0.90.7.1-2 amd64 [installed,automatic]
xserver-common/now 2:1.18.4-0ubuntu0.8 all [installed,upgradable to: 2:1.18.4-0ubuntu0.12]
xserver-xephyr/now 2:1.18.4-0ubuntu0.8 amd64 [installed,upgradable to: 2:1.18.4-0ubuntu0.12]
xserver-xorg-core-hwe-16.04/now 2:1.19.6-1ubuntu4.1~16.04.2 amd64 [installed,upgradable to: 2:1.19.6-1ubuntu4.1~16.04.6]
xserver-xorg-hwe-16.04/xenial-updates,now 1:7.7+16ubuntu3~16.04.1 amd64 [installed]
xserver-xorg-input-all-hwe-16.04/xenial-updates,now 1:7.7+16ubuntu3~16.04.1 amd64 [installed,automatic]
xserver-xorg-input-evdev-hwe-16.04/xenial-updates,now 1:2.10.5-1ubuntu1~16.04.1 amd64 [installed,automatic]
xserver-xorg-input-synaptics-hwe-16.04/xenial-updates,now 1.9.0-1ubuntu1~16.04.1 amd64 [installed,automatic]
xserver-xorg-input-wacom-hwe-16.04/xenial-updates,now 1:0.34.0-0ubuntu2~16.04.1 amd64 [installed,automatic]
xserver-xorg-legacy-hwe-16.04/now 2:1.19.6-1ubuntu4.1~16.04.2 amd64 [installed,upgradable to: 2:1.19.6-1ubuntu4.1~16.04.6]
xserver-xorg-video-all-hwe-16.04/xenial-updates,now 1:7.7+16ubuntu3~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-amdgpu-hwe-16.04/xenial-updates,now 18.0.1-1~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-ati-hwe-16.04/xenial-updates,now 1:18.0.1-1~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-fbdev-hwe-16.04/xenial-updates,now 1:0.4.4-1build6~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-intel-hwe-16.04/xenial-updates,now 2:2.99.917+git20171229-1~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-nouveau-hwe-16.04/xenial-updates,now 1:1.0.15-2~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-qxl-hwe-16.04/xenial-updates,now 0.1.5-2build1~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-radeon-hwe-16.04/xenial-updates,now 1:18.0.1-1~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-vesa-hwe-16.04/xenial-updates,now 1:2.3.4-1build3~16.04.1 amd64 [installed,automatic]
xserver-xorg-video-vmware-hwe-16.04/xenial-updates,now 1:13.2.1-1build1~16.04.1 amd64 [installed,automatic]
xsltproc/xenial-updates,xenial-security,now 1.1.28-2.1ubuntu0.3 amd64 [installed,automatic]
xterm/xenial,now 322-1ubuntu1 amd64 [installed,upgradable to: 322-1ubuntu1.2]
xz-utils/xenial,now 5.1.1alpha+20120614-2ubuntu2 amd64 [installed]
yelp/xenial,now 3.18.1-1ubuntu4 amd64 [installed]
yelp-tools/xenial-updates,xenial-updates,now 3.18.0-1ubuntu0.2 all [installed]
yelp-xsl/xenial,xenial,now 3.18.1-1 all [installed]
zenity/xenial,now 3.18.1.1-1ubuntu2 amd64 [installed]
zenity-common/xenial,xenial,now 3.18.1.1-1ubuntu2 all [installed,automatic]
zerofree/xenial,now 1.0.3-1 amd64 [installed]
zip/xenial,now 3.0-11 amd64 [installed]
zlib1g/xenial-updates,xenial-security,now 1:1.2.8.dfsg-2ubuntu4.3 amd64 [installed]
zsync/xenial,now 0.6.2-1ubuntu1 amd64 [installed]
sam@sam-Virtual-Machine:~$ sudo docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
securityonionsolutions/so-domainstats latest a90c876ca7f1 5 years ago 422MB
securityonionsolutions/so-freqserver latest 49ed29bd3d80 5 years ago 384MB
securityonionsolutions/so-elastalert latest 611a700ae92f 5 years ago 581MB
securityonionsolutions/so-curator latest c6244cd12095 5 years ago 394MB
securityonionsolutions/so-kibana latest c1128a31326e 5 years ago 529MB
securityonionsolutions/so-logstash latest 4476c86bd213 5 years ago 834MB
securityonionsolutions/so-elasticsearch latest e8bf52e4091b 5 years ago 766MB
sam@sam-Virtual-Machine:~$
sam@sam-Virtual-Machine: ~
1 / 4


Admin Machine-2
Applications Places Terminal
Sun 19:57
root@sam-Virtual-Machine: /home/sam
File Edit View Search Terminal Help
root@sam-Virtual-Machine: /home/sam
sam@sam-Virtual-Machine:~$ sudo su
[sudo] password for sam:
root@sam-Virtual-Machine:/home/sam# git clone https://github.com/docker/docker-bench-security.git
Cloning into 'docker-bench-security'...
remote: Enumerating objects: 2730, done.
remote: Counting objects: 100% (990/990), done.
remote: Compressing objects: 100% (186/186), done.
remote: Total 2730 (delta 858), reused 804 (delta 804), pack-reused 1740 (from 3)
Receiving objects: 100% (2730/2730), 4.46 MiB | 0 bytes/s, done.
Resolving deltas: 100% (1897/1897), done.
Checking connectivity... done.
root@sam-Virtual-Machine:/home/sam#
zenity/xenial,now 3.18.1.1-1ubuntu2 amd64 [installed]
zenity-common/xenial,xenial,now 3.10.1.1-1ubuntu2 all [installed,automatic]
zerofree/xenial,now 1.0.3-1 amd64 [installed]
zip/xenial,now 3.0-11 amd64 [installed]
zlib1g/xenial-updates,xenial-security,now 1:1.2.8.dfsg-2ubuntu4.3 amd64 [installed]
zsync/xenial,now 0.6.2-1ubuntu1 amd64 [installed]
sam@sam-Virtual-Machine:~$ sudo docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
securityonionsolutions/so-domainstats latest a90c876ca7f1 5 years ago 422MB
securityonionsolutions/so-freqserver latest 49ed29bd3d80 5 years ago 384MB
securityonionsolutions/so-elastalert latest 611a700ae92f 5 years ago 581MB
securityonionsolutions/so-curator latest c6244cd12095 5 years ago 394MB
securityonionsolutions/so-kibana latest c1128a31326e 5 years ago 529MB
securityonionsolutions/so-logstash latest 4476c86bd213 5 years ago 834MB
securityonionsolutions/so-elasticsearch latest e8bf52e4091b 5 years ago 766MB
sam@sam-Virtual-Machine:~$ sudo su
root@sam-Virtual-Machine:/home/sam# admin@123
admin@123: command not found
root@sam-Virtual-Machine:/home/sam#
root@sam-Virtual-Machine: /home/...
1 / 4


Admin Machine-2
Applications Places Terminal Sun 19:58
root@sam-Virtual-Machine: /home/sam
root@sam-Virtual-Machine: /home/sam/docker-bench-security
File Edit View Search Terminal Help
sam@sam-Virtual-Machine:~$ sudo su
[sudo] password for sam:
root@sam-Virtual-Machine:/home/sam# git clone https://github.com/docker/docker-bench-security.git
Cloning into 'docker-bench-security'...
remote: Enumerating objects: 2730, done.
remote: Counting objects: 100% (990/990), done.
remote: Compressing objects: 100% (186/186), done.
remote: Total 2730 (delta 858), reused 804 (delta 804), pack-reused 1740 (from 3)
Receiving objects: 100% (2730/2730), 4.46 MiB | 0 bytes/s, done.
Resolving deltas: 100% (1897/1897), done.
Checking connectivity... done.
root@sam-Virtual-Machine:/home/sam# cd docker-bench-security
root@sam-Virtual-Machine:/home/sam/docker-bench-security#
zenity/xenial,now 3.18.1.1-1ubuntu2 amd64 [installed]
zenity-common/xenial,xenial,now 3.18.1.1-1ubuntu2 all [installed,automatic]
zerofree/xenial,now 1.0.3-1 amd64 [installed]
zip/xenial,now 3.0-11 amd64 [installed]
zlib1g/xenial-updates,xenial-security,now 1:1.2.8.dfsg-2ubuntu4.3 amd64 [installed]
zsync/xenial,now 0.6.2-1ubuntu1 amd64 [installed]
sam@sam-Virtual-Machine:~$ sudo docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
securityonionsolutions/so-domainstats latest a90c876ca7f1 5 years ago 422MB
securityonionsolutions/so-freqserver latest 49ed29bd3d80 5 years ago 384MB
securityonionsolutions/so-elastalert latest 611a700ae92f 5 years ago 581MB
securityonionsolutions/so-curator latest c6244cd12095 5 years ago 394MB
securityonionsolutions/so-kibana latest c1128a31326e 5 years ago 529MB
securityonionsolutions/so-logstash latest 4476c86bd213 5 years ago 834MB
securityonionsolutions/so-elasticsearch latest e8bf52e4091b 5 years ago 766MB
sam@sam-Virtual-Machine:~$ sudo su
root@sam-Virtual-Machine:/home/sam# admin@123
admin@123: command not found
root@sam-Virtual-Machine:/home/sam#
root@sam-Virtual-Machine: /home/...
1 / 4



Exercise 2: Implementing AWS Identity and Access Management

Amazon Web Services (AWS) cloud security provides step-by-step security tasks through Identity Access Management (IAM). A network defender can easily manage and control AWS services and resources for AWS users using IAM.

Lab Scenario

AWS IAM enables network defenders to control access to AWS services and resources securely. It allows to establish access rules and permissions for specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) for resource access. This helps network defenders assign role-based access control for accessing critical information within the enterprise.

Lab Objectives

This lab will demonstrate how to create an IAM Group and IAM User, attach a policy to the user, and enable Multi-Factor Authentication (MFA) that enables adding two-factor authentication for individual users in order to ensure additional security for the user accounts in AWS.

In this lab, you will learn to do the following:

- Create IAM Group in AWS
- Create IAM User in AWS
- Assign permission policy to user
- Create custom IAM policy in AWS
- Enable MFA

Overview of IAM

IAM enables role-based access control for accessing critical information within the enterprise. It comprises business processes, policies, and technologies that allow monitoring electronic or digital identities. IAM provides tools and technologies to regulate user access (creating, managing, and removing access) to systems or networks based on the roles of individual users within the enterprise. Organizations generally prefer all-in-one authentication, which can be extended to Identity Federation. Identity Federation includes IAM with single sign-on (SSO) and centralized Active directory (AD) account for secure management. For the root user account of cloud, and its associated user accounts, MFA is enabled. MFA is used to control access to Cloud Service APIs. However, the best option is choosing either Virtual MFA or a hardware device.

Before starting this lab, you should create an AWS account using the following: https://portal.aws.amazon.com/billing/signup. Once the registration is completed, perform the following tasks.

Exercise 3: Securing Amazon Web Services Storage

Lab Scenario

In the cloud, data are stored on Internet-connected servers in data centers. It is important that network defenders understand and implement the data storage security features for data encryption and access management tools provided by service providers to secure the data stored in the data centers.

Lab Objectives

This lab will demonstrate how to restrict access to S3 resources by creating bucket policies, Access Control Lists (ACLs), and IAM policies to provide access to selected entities.

In this lab, you will learn to do the following:

- Assign Permissions to Amazon S3 Using ACL
- Assign Permissions to Amazon S3 Using Bucket Policy

Overview of AWS Storage

Amazon S3 allows uploading and retrieving data at anytime from anywhere on the internet. It stores data as objects (text file/photo/video) within buckets. In the default state, all the Amazon S3 buckets are accessed by authorized users. Restrict access to S3 resources by combining bucket policies, ACLs and IAM polices to give access to the right entities.

Lab Tasks

Before starting this lab, you should create an AWS account using the following: https://portal.aws.amazon.com/billing/signup. Once the registration is completed, perform the following tasks.

Lab Summary: Virtualization and Cloud Computing

Exercise 1: Auditing Docker Host Security Using Docker-Bench-Security Tool

This exercise demonstrated how to secure a Docker host by auditing its default configuration with the **Docker-Bench-Security** tool on Ubuntu. Docker was installed and benchmarked, with results categorized as **NOTE, INFO, WARN, PASS**. Warnings highlighted weaker security configurations that required attention, while PASS confirmed protected configurations. This exercise reinforced the importance of auditing container environments since Docker's default setup often leaves unnecessary risks open.

Exercise 2: Implementing AWS Identity and Access Management (IAM)

This exercise was designed to demonstrate IAM controls in AWS, including creating groups, users, custom policies, and enabling multi-factor authentication (MFA). However, this task was not completed because it required creating a new AWS account. A new account was not created for this course, so the exercise was not executed.

Exercise 3: Securing Amazon Web Services Storage (S3)

This exercise focused on securing Amazon S3 storage using bucket policies, access control lists (ACLs), and IAM policies to restrict access to resources. Similar to Exercise 2, this task was not completed because it required setting up an AWS account, which was not created for this course.

Reflection

The virtualization labs demonstrated two key areas of cloud and container defense:

- **Docker Security** – showed how to identify weak default settings and apply auditing tools to harden containers.
- **AWS Security** – highlighted IAM and S3 access controls conceptually, though account setup limitations prevented hands-on completion.

This module reinforced the need for auditing and enforcing least-privilege access across both virtualized and cloud-hosted environments.