Department of Computer Science and Engineering
Cloud Architecture

Lab-3A-Automation using Ansible

Student name and UCID :
Branch:

Objective: Automation in Software Install/Configuration/operations.
Description: Set up network applications, apache2, ftp,monitoring and network security devices various security devices (firewalls, IDS/IPS).
To use Ansible playbooks for automating routine tasks, such as rule updates and device configuration.

Outcomes: After successful completion of the lab, students should be able to:
[1] Install and configure ansible
[2] Configure the network setup.
[3] Adding various anomaly detectors(sensors-HIDS, NIDS) in ansible basic setup and advanced setup.
[4] To provide a roadmap for others to better secure their networks and facilitate the creation and consumption of threat intelligence.
[5] Detect and analyze malicious behavior on the network to generate data and information products that detail aspects of the Cyber Kill-Chain
[6] To develop new and innovative approaches to Cyber Threat Intelligence and information security.

System Requirements:
[1] Ubuntu Linux (Host OS)
[2] Docker installed (sudo apt-get install docker.io)
[3] VirtualBox installed
[3] Ansible
[4] Apache2
[5] Firewall (iptables)
[6] Snort/Suricata (NIDS)
[7] OSSEC/Logwatch (HIDS)
[8] Prelude-lml (Log Management)
[9] Prelude-manager (SIEM Server)

Introduction to Ansible:

Ansible is a powerful open-source automation tool that allows you to manage and configure multiple servers from a single control machine. It uses a simple YAML-based syntax for defining playbooks that automate a wide range of tasks, including installing software, configuring services, and managing network settings. With Ansible, you can reduce manual errors, increase efficiency, and standardize your infrastructure configuration across your entire organization. Whether you’re managing a small or large IT environment, Ansible can help you streamline your processes and improve productivity.

Ansible architecture:

From **figure-1,** you can see that the Ansible architecture involves a **control node, playbook, inventory, SSH to connect to managed/target nodes.**

The **control node** is where Ansible is installed, and from where automation tasks are executed. **Managed/targeted** nodes are the servers that Ansible manages and configures.

It is necessary to first install **Ansible on the control node.** Once you have installed Ansible, you will need to register your **targeted/managed hosts** in the **Ansible inventory**. The inventory is a file that contains a list of all the hosts you want Ansible to manage, along with their IP addresses or hostnames. After that, you can create **playbooks, which are YAML files** containing a series of tasks to be executed on the managed nodes. These tasks can include a wide range of operations, such as installing software, configuring services, and managing network settings.

When the playbook is run from the control node, Ansible establishes a secure communication channel with the managed nodes using SSH. Ansible then executes the tasks defined in the playbook on the managed nodes.

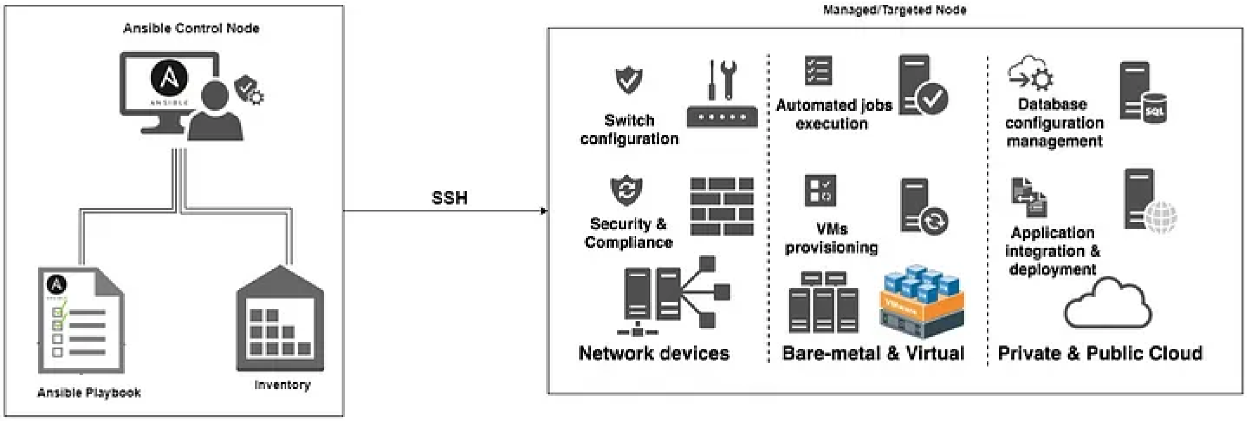


Figure-1: Ansible Architecture

(Source:Google Images[1])

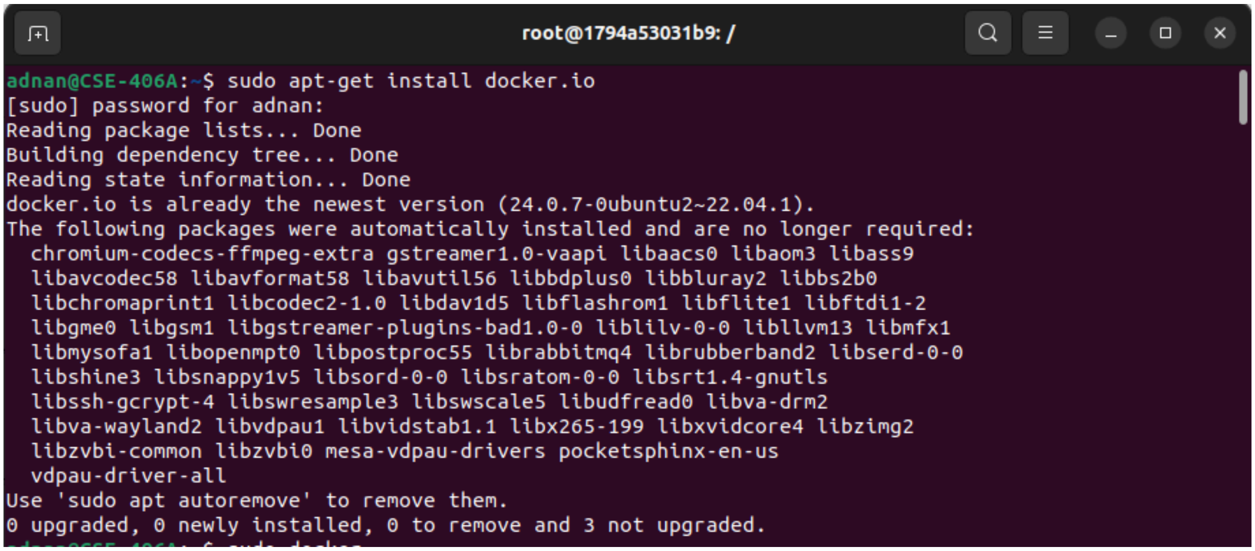
Procedure:
Read the STH article on Ansible [1] and perform the lab. Write the conclusion in your own words. (Tutorial-1,2,3)

Step-by-step instructions to install and configure ansible:

On Ubuntu Linux (Host)

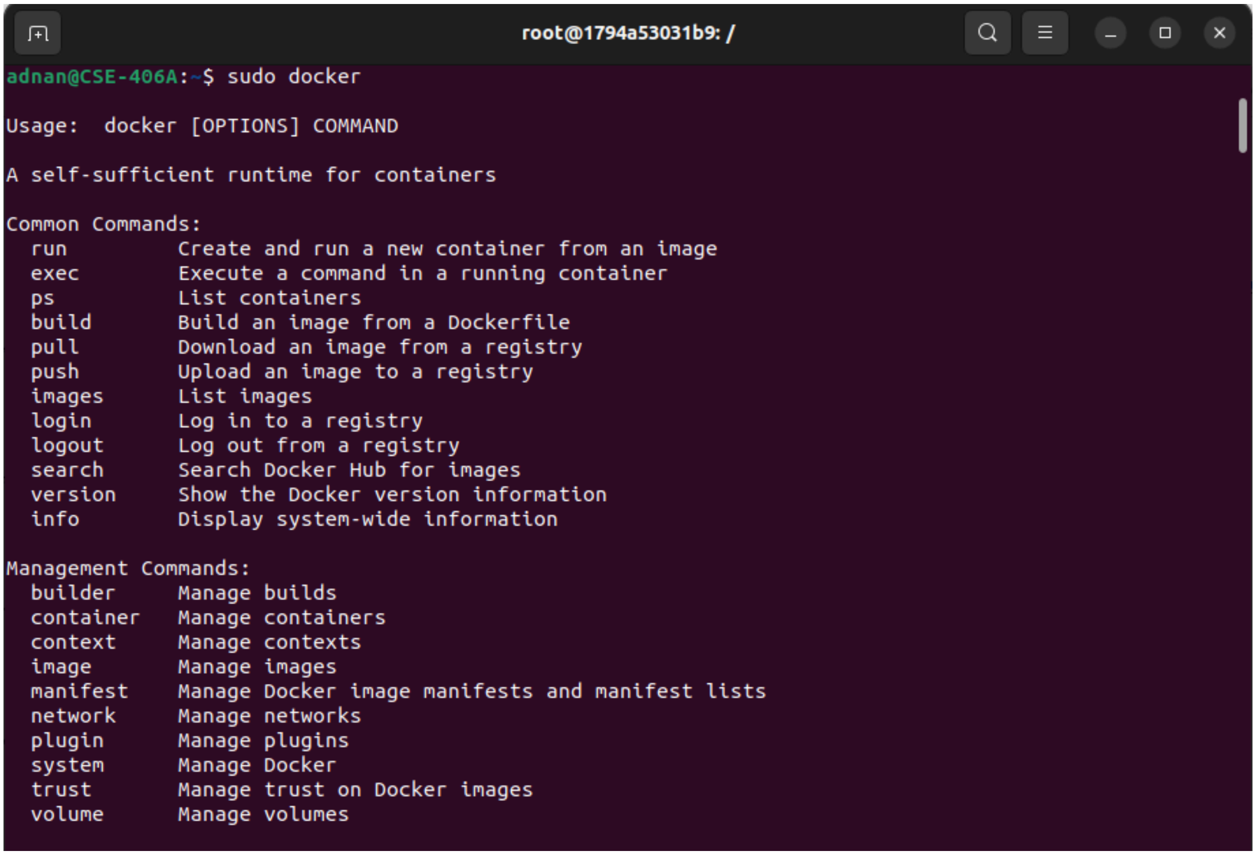
[1] Install docker

$sudo apt-get install docker.io



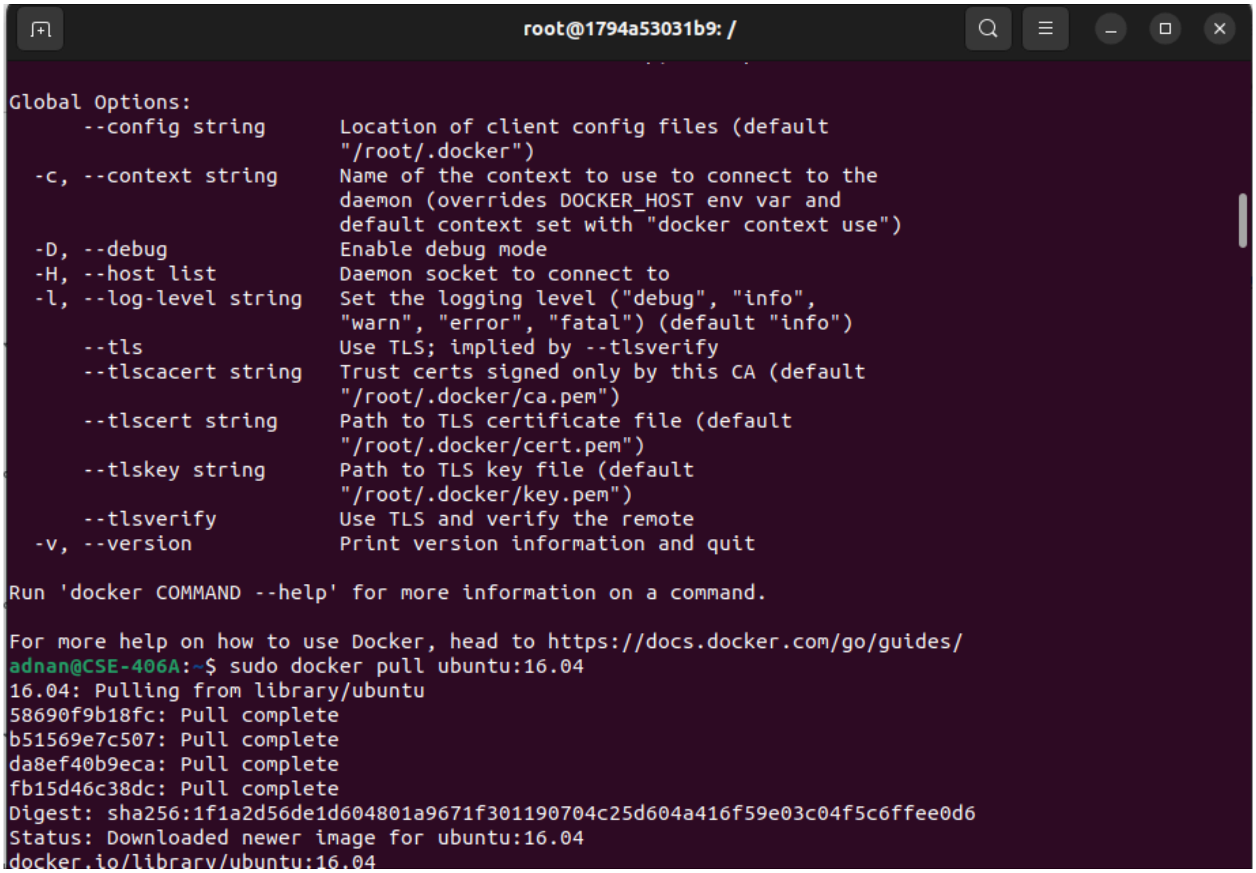
```
adnan@CSE-406A:~$ sudo apt-get install docker.io
[sudo] password for adnan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
docker.io is already the newest version (24.0.7-0ubuntu2~22.04.1).
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libaacs0 libaom3 libass9
  libavcodec58 libavformat58 libavutil56 libbdplus0 libbluray2 libbs2b0
  libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1 libftdi1-2
  libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 liblilv-0-0 libllvm13 libmfx1
  libmysofa1 libopenmpt0 libpostproc55 librabbitmq4 librubberband2 libserd-0-0
  libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0 libsrt1.4-gnutls
  libssh-gcrypt-4 libswresample3 libswscale5 libudfread0 libva-drm2
  libva-wayland2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzimg2
  libzvbi-common libzvbi0 mesa-vdpau-drivers pocketsphinx-en-us
  vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

[2] Check docker installation
$sudo docker



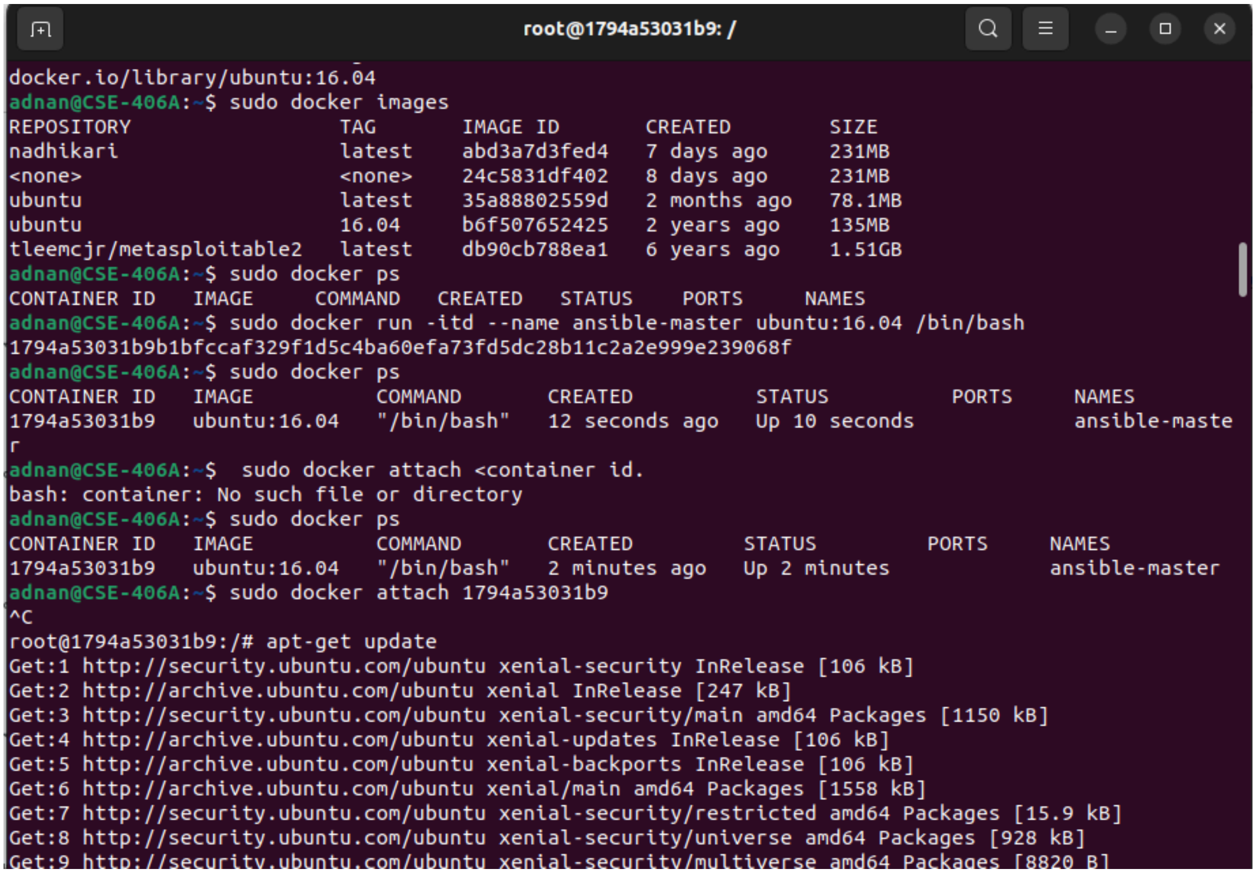
```
adnan@CSE-406A:~$ sudo docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers

Common Commands:
  run         Create and run a new container from an image
  exec        Execute a command in a running container
  ps          List containers
  build       Build an image from a Dockerfile
  pull        Download an image from a registry
  push        Upload an image to a registry
  images      List images
  login       Log in to a registry
  logout      Log out from a registry
  search      Search Docker Hub for images
  version     Show the Docker version information
  info        Display system-wide information

Management Commands:
  builder     Manage builds
  container   Manage containers
  context     Manage contexts
  image       Manage images
  manifest    Manage Docker image manifests and manifest lists
  network     Manage networks
  plugin      Manage plugins
  system      Manage Docker
  trust       Manage trust on Docker images
  volume      Manage volumes
```

[3] Use Ubuntu image from docker hub
$sudo docker pull ubuntu:16.04



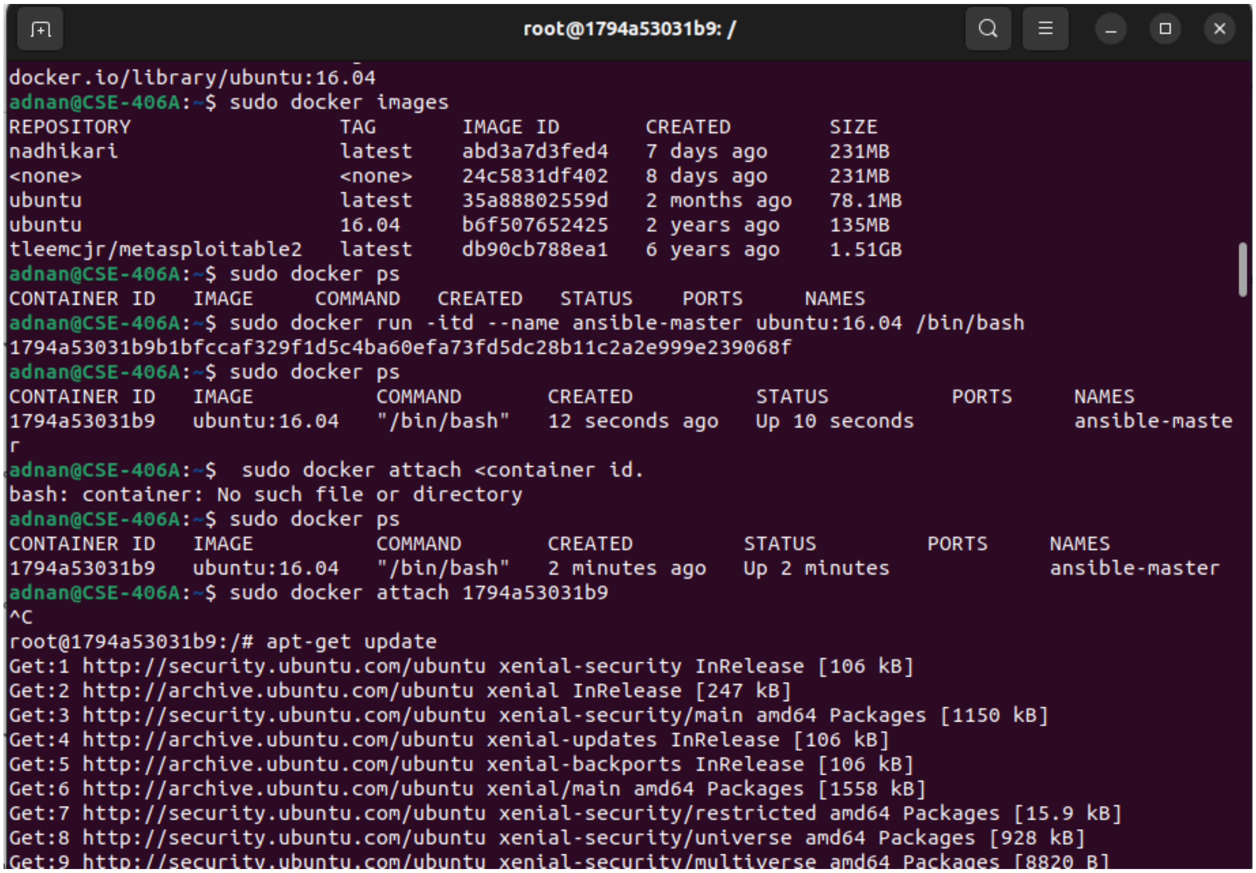
```
Global Options:
      --config string      Location of client config files (default
                           "/root/.docker")
  -c, --context string     Name of the context to use to connect to the
                           daemon (overrides DOCKER_HOST env var and
                           default context set with "docker context use")
  -D, --debug              Enable debug mode
  -H, --host list          Daemon socket to connect to
  -l, --log-level string   Set the logging level ("debug", "info",
                           "warn", "error", "fatal") (default "info")
      --tls                Use TLS; implied by --tlsverify
      --tlscacert string   Trust certs signed only by this CA (default
                           "/root/.docker/ca.pem")
      --tlscert string     Path to TLS certificate file (default
                           "/root/.docker/cert.pem")
      --tlskey string      Path to TLS key file (default
                           "/root/.docker/key.pem")
      --tlsverify          Use TLS and verify the remote
  -v, --version            Print version information and quit

Run 'docker COMMAND --help' for more information on a command.

For more help on how to use Docker, head to https://docs.docker.com/go/guides/
adnan@CSE-406A:~$ sudo docker pull ubuntu:16.04
16.04: Pulling from library/ubuntu
58690f9b18fc: Pull complete
b51569e7c507: Pull complete
da8ef40b9eca: Pull complete
fb15d46c38dc: Pull complete
Digest: sha256:1f1a2d56de1d604801a9671f301190704c25d604a416f59e03c04f5c6ffee0d6
Status: Downloaded newer image for ubuntu:16.04
docker.io/library/ubuntu:16.04
```

[4] Check docker images and container
$sudo docker images



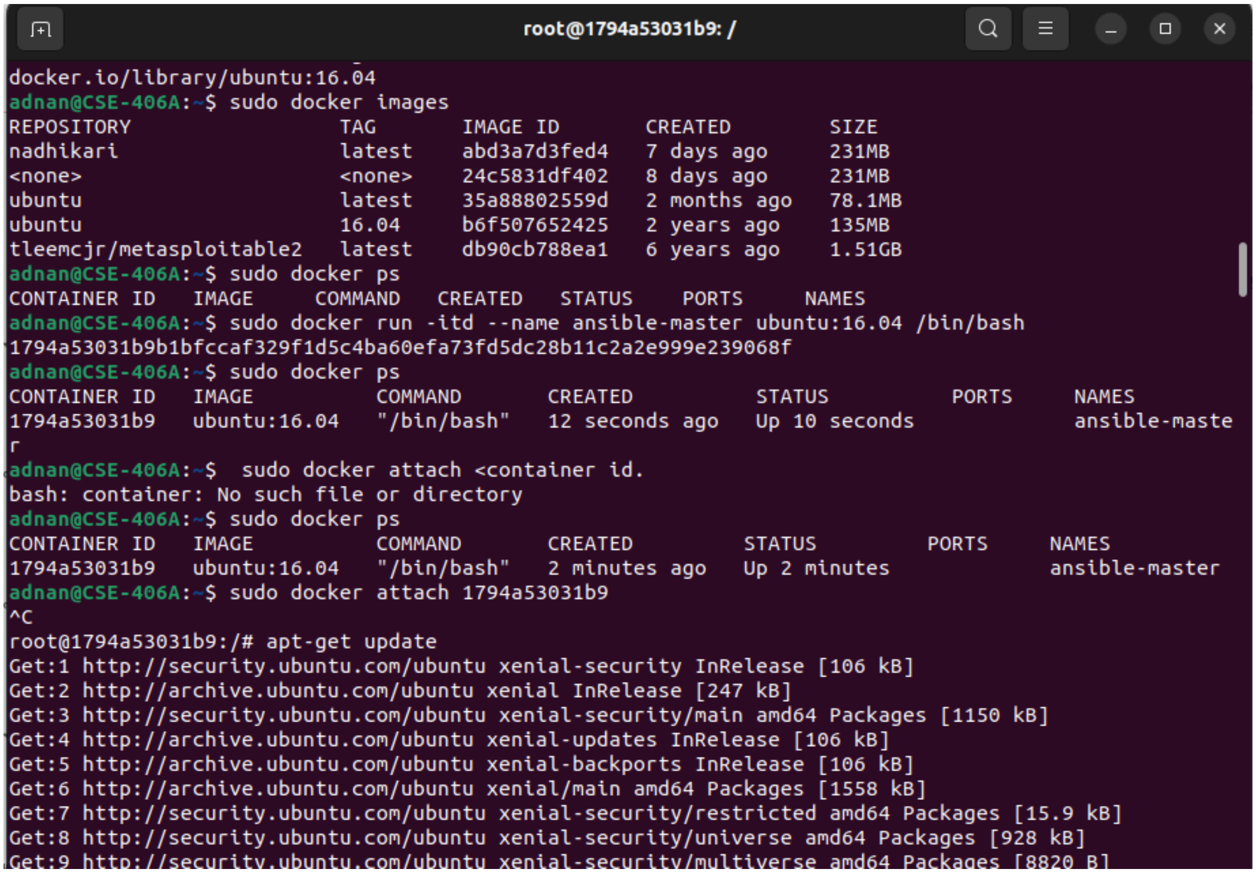
```
docker.io/library/ubuntu:16.04
adnan@CSE-406A:~$ sudo docker images
REPOSITORY                 TAG       IMAGE ID       CREATED        SIZE
nadhikari                  latest    abd3a7d3fed4   7 days ago     231MB
<none>                     <none>    24c5831df402   8 days ago     231MB
ubuntu                     latest    35a88802559d   2 months ago   78.1MB
ubuntu                     16.04     b6f507652425   2 years ago    135MB
tleemcjr/metasploitable2   latest    db90cb788ea1   6 years ago    1.51GB
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
adnan@CSE-406A:~$ sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash
1794a53031b9b1bfccaf329f1d5c4ba60efa73fd5dc28b11c2a2e999e239068f
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   12 seconds ago   Up 10 seconds             ansible-maste
r
adnan@CSE-406A:~$  sudo docker attach <container id.
bash: container: No such file or directory
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED         STATUS         PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   2 minutes ago   Up 2 minutes             ansible-master
adnan@CSE-406A:~$ sudo docker attach 1794a53031b9
^C
root@1794a53031b9:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:5 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:6 http://archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1558 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
```

$sudo docker ps



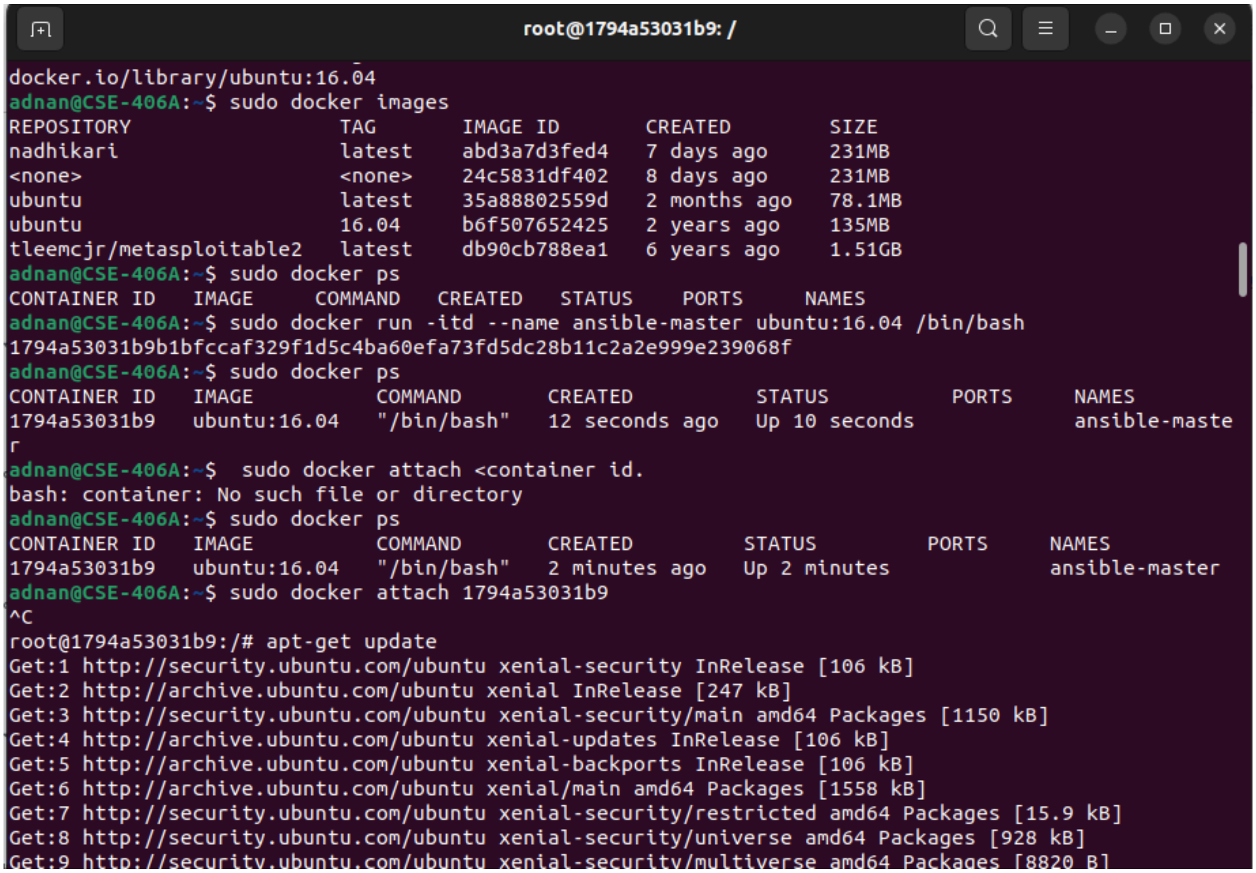
```
docker.io/library/ubuntu:16.04
adnan@CSE-406A:~$ sudo docker images
REPOSITORY                 TAG       IMAGE ID       CREATED        SIZE
nadhikari                  latest    abd3a7d3fed4   7 days ago     231MB
<none>                     <none>    24c5831df402   8 days ago     231MB
ubuntu                     latest    35a88802559d   2 months ago   78.1MB
ubuntu                     16.04     b6f507652425   2 years ago    135MB
tleemcjr/metasploitable2   latest    db90cb788ea1   6 years ago    1.51GB
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
adnan@CSE-406A:~$ sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash
1794a53031b9b1bfccaf329f1d5c4ba60efa73fd5dc28b11c2a2e999e239068f
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   12 seconds ago   Up 10 seconds             ansible-maste
r
adnan@CSE-406A:~$  sudo docker attach <container id.
bash: container: No such file or directory
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED         STATUS         PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   2 minutes ago   Up 2 minutes             ansible-master
adnan@CSE-406A:~$ sudo docker attach 1794a53031b9
^C
root@1794a53031b9:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:5 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:6 http://archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1558 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
```

[5] Start the ansible container
$sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash



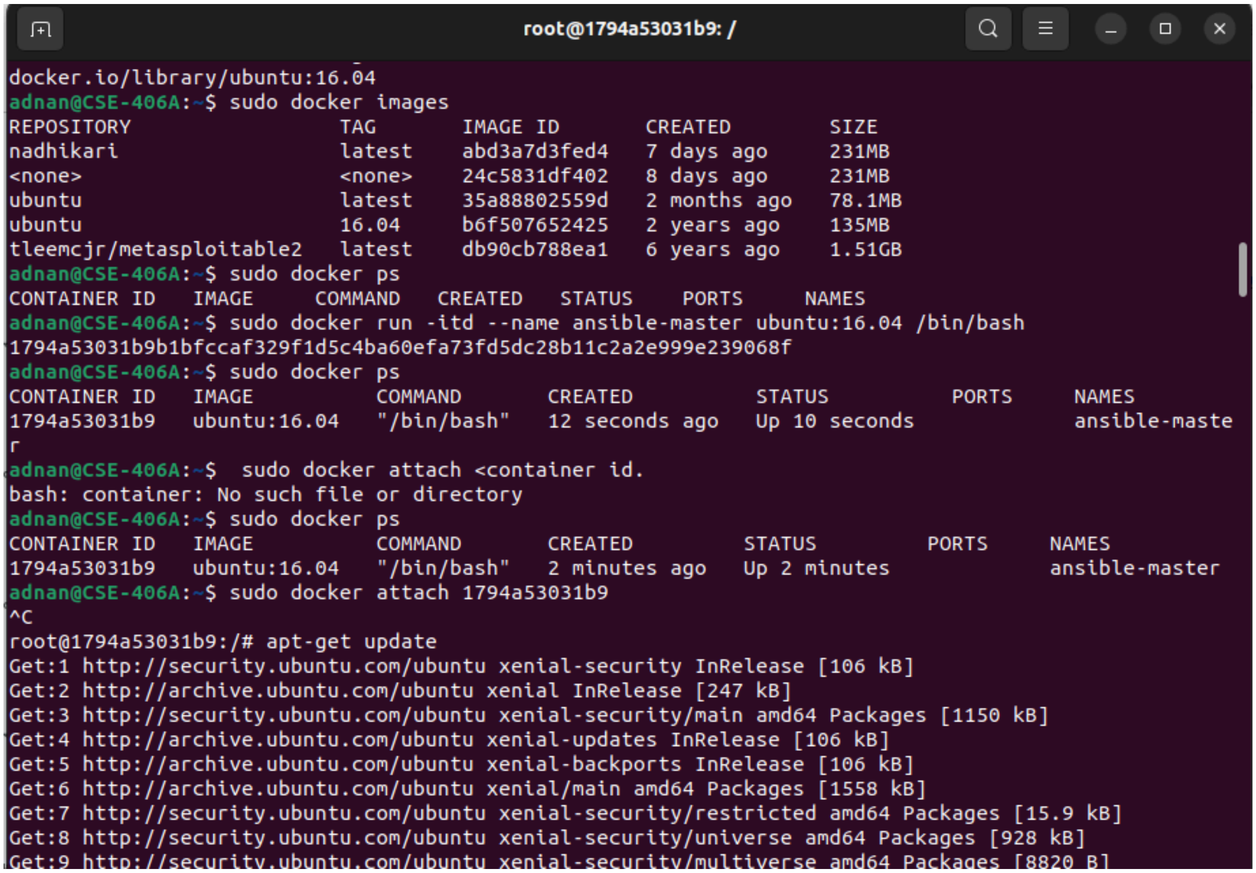
```
docker.io/library/ubuntu:16.04
adnan@CSE-406A:~$ sudo docker images
REPOSITORY                 TAG       IMAGE ID       CREATED        SIZE
nadhikari                  latest    abd3a7d3fed4   7 days ago     231MB
<none>                     <none>    24c5831df402   8 days ago     231MB
ubuntu                     latest    35a88802559d   2 months ago   78.1MB
ubuntu                     16.04     b6f507652425   2 years ago    135MB
tleemcjr/metasploitable2   latest    db90cb788ea1   6 years ago    1.51GB
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
adnan@CSE-406A:~$ sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash
1794a53031b9b1bfccaf329f1d5c4ba60efa73fd5dc28b11c2a2e999e239068f
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   12 seconds ago   Up 10 seconds             ansible-maste
r
adnan@CSE-406A:~$  sudo docker attach <container id.
bash: container: No such file or directory
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED         STATUS         PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   2 minutes ago   Up 2 minutes             ansible-master
adnan@CSE-406A:~$ sudo docker attach 1794a53031b9
^C
root@1794a53031b9:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:5 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:6 http://archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1558 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
```

[6] Find the container id and use it.
$sudo docker ps
$ sudo docker attach <container id.



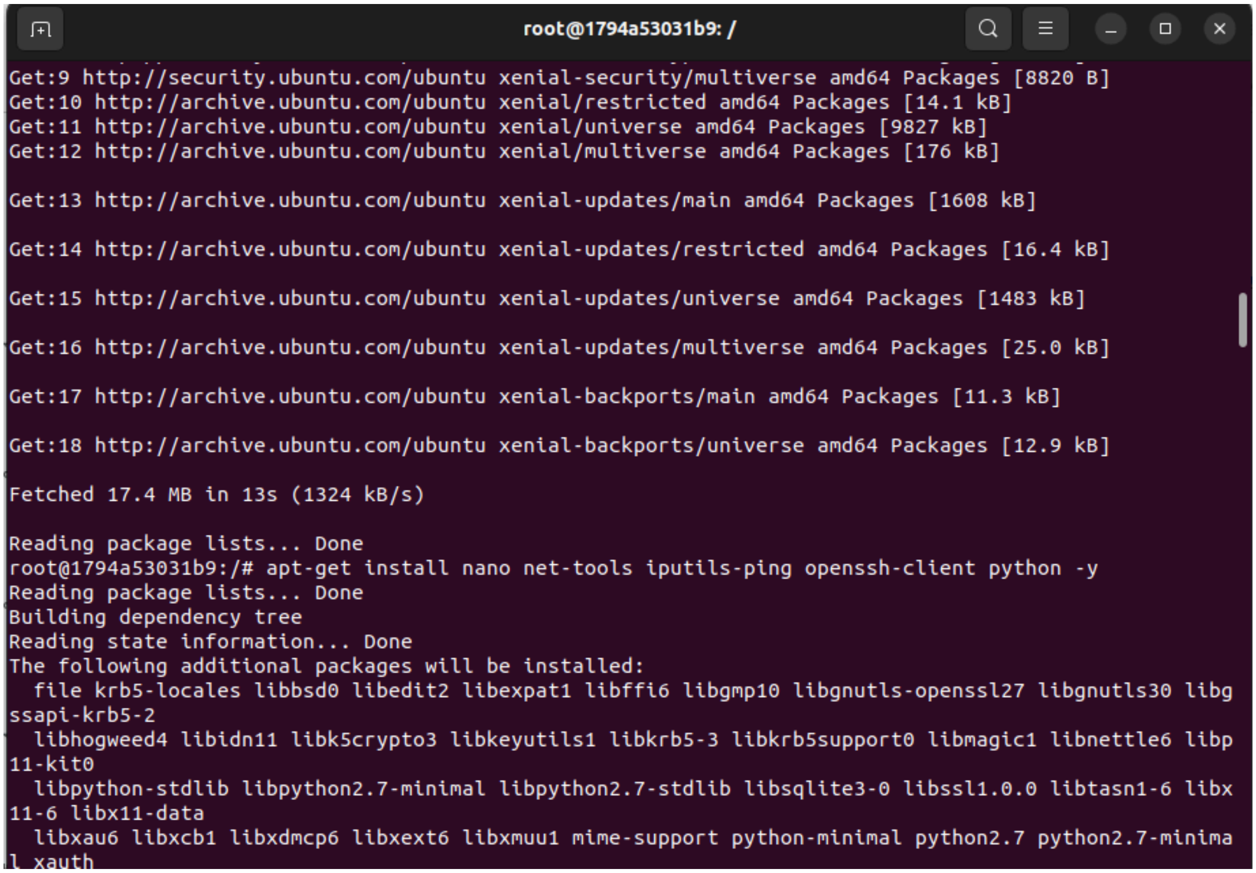
```
docker.io/library/ubuntu:16.04
adnan@CSE-406A:~$ sudo docker images
REPOSITORY                 TAG       IMAGE ID       CREATED        SIZE
nadhikari                  latest    abd3a7d3fed4   7 days ago     231MB
<none>                     <none>    24c5831df402   8 days ago     231MB
ubuntu                     latest    35a88802559d   2 months ago   78.1MB
ubuntu                     16.04     b6f507652425   2 years ago    135MB
tleemcjr/metasploitable2   latest    db90cb788ea1   6 years ago    1.51GB
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
adnan@CSE-406A:~$ sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash
1794a53031b9b1bfccaf329f1d5c4ba60efa73fd5dc28b11c2a2e999e239068f
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   12 seconds ago   Up 10 seconds             ansible-maste
r
adnan@CSE-406A:~$  sudo docker attach <container id.
bash: container: No such file or directory
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED         STATUS         PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   2 minutes ago   Up 2 minutes             ansible-master
adnan@CSE-406A:~$ sudo docker attach 1794a53031b9
^C
root@1794a53031b9:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:5 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:6 http://archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1558 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
```

[7] Update/Install the software packages
#apt-get update



```
docker.io/library/ubuntu:16.04
adnan@CSE-406A:~$ sudo docker images
REPOSITORY                 TAG       IMAGE ID       CREATED        SIZE
nadhikari                  latest    abd3a7d3fed4   7 days ago     231MB
<none>                     <none>    24c5831df402   8 days ago     231MB
ubuntu                     latest    35a88802559d   2 months ago   78.1MB
ubuntu                     16.04     b6f507652425   2 years ago    135MB
tleemcjr/metasploitable2   latest    db90cb788ea1   6 years ago    1.51GB
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
adnan@CSE-406A:~$ sudo docker run -itd --name ansible-master ubuntu:16.04 /bin/bash
1794a53031b9b1bfccaf329f1d5c4ba60efa73fd5dc28b11c2a2e999e239068f
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   12 seconds ago   Up 10 seconds             ansible-maste
r
adnan@CSE-406A:~$  sudo docker attach <container id.
bash: container: No such file or directory
adnan@CSE-406A:~$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED         STATUS         PORTS     NAMES
1794a53031b9   ubuntu:16.04   "/bin/bash"   2 minutes ago   Up 2 minutes             ansible-master
adnan@CSE-406A:~$ sudo docker attach 1794a53031b9
^C
root@1794a53031b9:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:5 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
Get:6 http://archive.ubuntu.com/ubuntu xenial/main amd64 Packages [1558 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
```

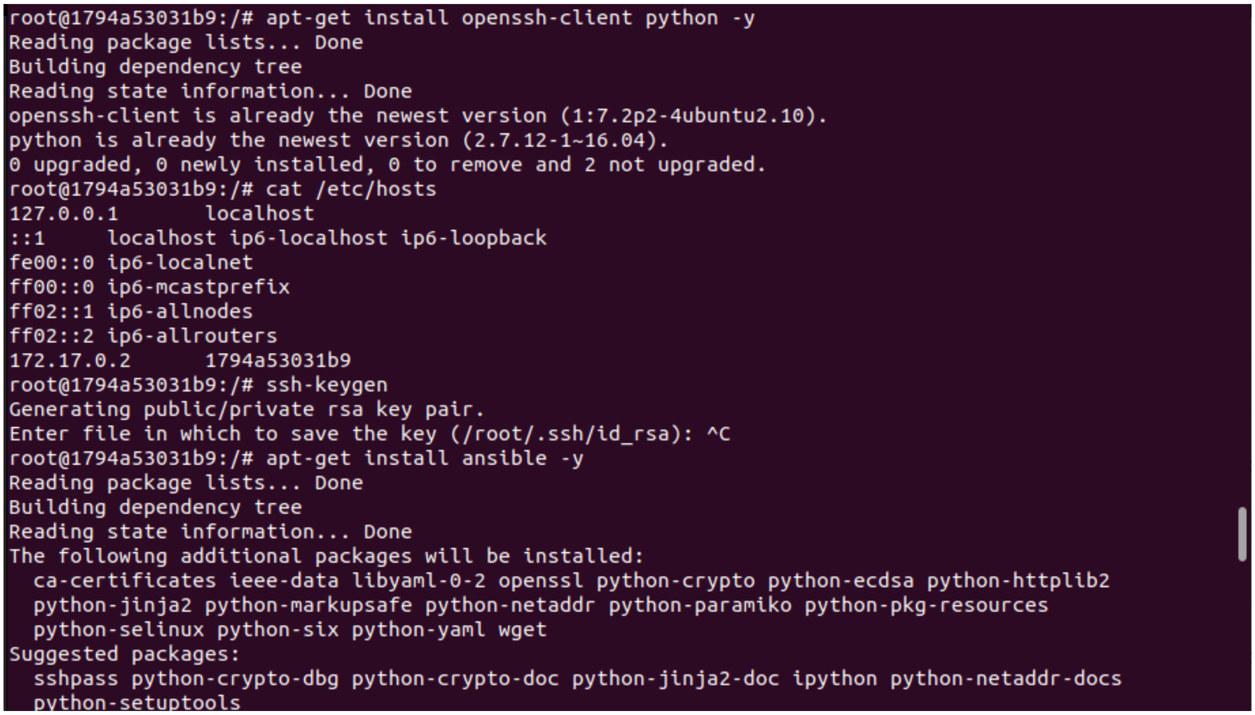
#apt-get install nano net-tools iputils-ping openssh-client python -y



```
Get:9 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
Get:10 http://archive.ubuntu.com/ubuntu xenial/restricted amd64 Packages [14.1 kB]
Get:11 http://archive.ubuntu.com/ubuntu xenial/universe amd64 Packages [9827 kB]
Get:12 http://archive.ubuntu.com/ubuntu xenial/multiverse amd64 Packages [176 kB]

Get:13 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [1608 kB]

Get:14 http://archive.ubuntu.com/ubuntu xenial-updates/restricted amd64 Packages [16.4 kB]

Get:15 http://archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [1483 kB]

Get:16 http://archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Packages [25.0 kB]

Get:17 http://archive.ubuntu.com/ubuntu xenial-backports/main amd64 Packages [11.3 kB]

Get:18 http://archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Packages [12.9 kB]

Fetched 17.4 MB in 13s (1324 kB/s)

Reading package lists... Done
root@1794a53031b9:/# apt-get install nano net-tools iputils-ping openssh-client python -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  file krb5-locales libbsd0 libedit2 libexpat1 libffi6 libgmp10 libgnutls-openssl27 libgnutls30 libg
ssapi-krb5-2
  libhogweed4 libidn11 libk5crypto3 libkeyutils1 libkrb5-3 libkrb5support0 libmagic1 libnettle6 libp
11-kit0
  libpython-stdlib libpython2.7-minimal libpython2.7-stdlib libsqlite3-0 libssl1.0.0 libtasn1-6 libx
11-6 libx11-data
  libxau6 libxcb1 libxdmcp6 libxext6 libxmuu1 mime-support python-minimal python2.7 python2.7-minima
l xauth
```

[8] Check IP address of Ansible master

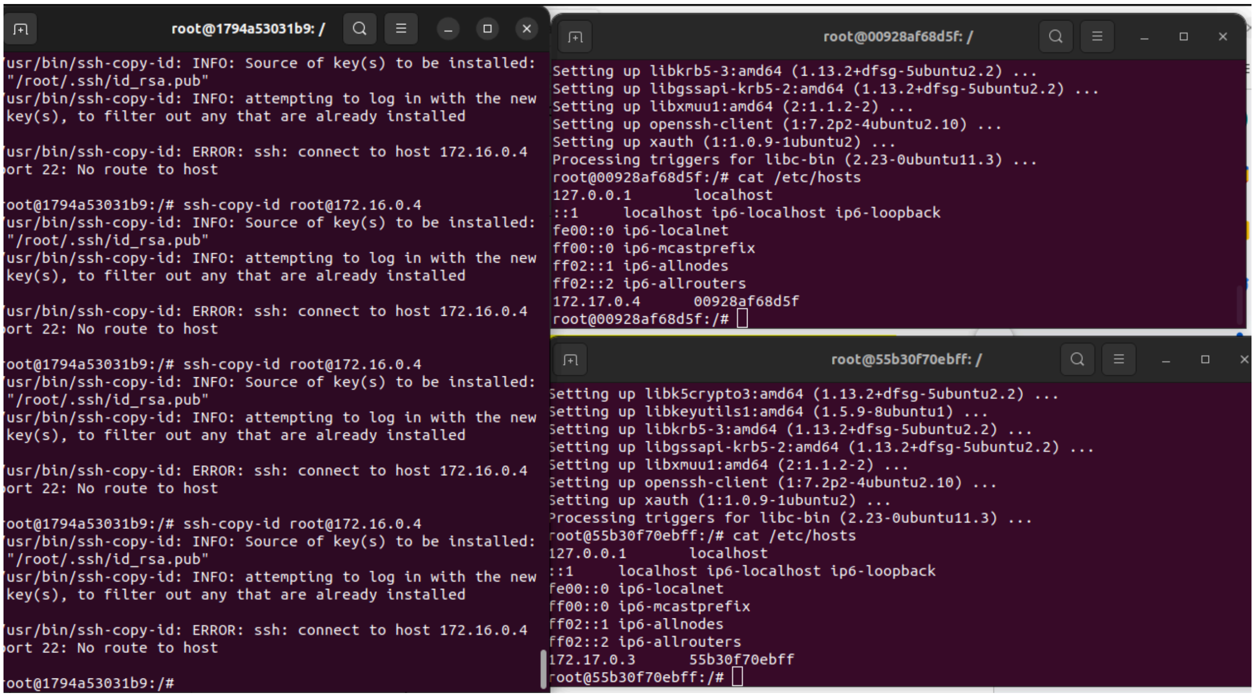
#cat /etc/hosts



```
root@1794a53031b9:/# apt-get install openssh-client python -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
openssh-client is already the newest version (1:7.2p2-4ubuntu2.10).
python is already the newest version (2.7.12-1~16.04).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
root@1794a53031b9:/# cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2      1794a53031b9
root@1794a53031b9:/# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): ^C
root@1794a53031b9:/# apt-get install ansible -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ca-certificates ieee-data libyaml-0-2 openssl python-crypto python-ecdsa python-httplib2
  python-jinja2 python-markupsafe python-netaddr python-paramiko python-pkg-resources
  python-selinux python-six python-yaml wget
Suggested packages:
  sshpass python-crypto-dbg python-crypto-doc python-jinja2-doc ipython python-netaddr-docs
  python-setuptools
```

[9] Generate key-pair of Ansible master
#ssh-keygen
ssh-keygen

[10] Share the public-key of ansible with target machine(s) (provided that ssh service running on target machine(s) and enable the root login)
#ssh-copy-id root@<target machine ip address>

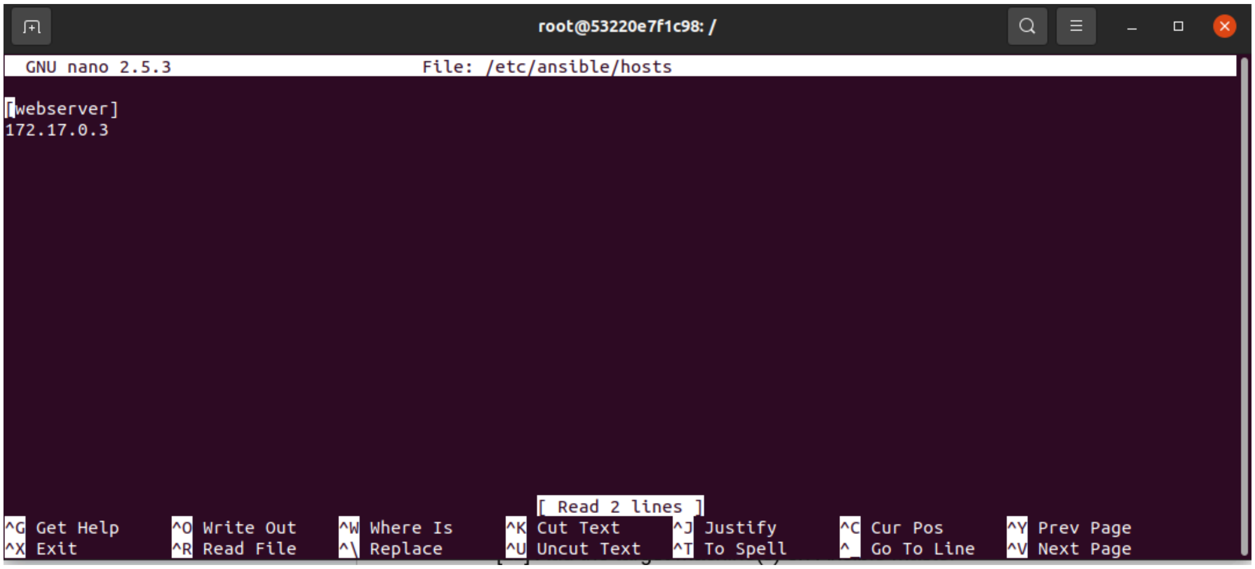


```
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to filter out any that are already installed

usr/bin/ssh-copy-id: ERROR: ssh: connect to host 172.16.0.4
ort 22: No route to host

oot@1794a53031b9:/# ssh-copy-id root@172.16.0.4
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to filter out any that are already installed

usr/bin/ssh-copy-id: ERROR: ssh: connect to host 172.16.0.4
ort 22: No route to host

oot@1794a53031b9:/# ssh-copy-id root@172.16.0.4
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to filter out any that are already installed

usr/bin/ssh-copy-id: ERROR: ssh: connect to host 172.16.0.4
ort 22: No route to host

oot@1794a53031b9:/# ssh-copy-id root@172.16.0.4
usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
"/root/.ssh/id_rsa.pub"
usr/bin/ssh-copy-id: INFO: attempting to log in with the new
key(s), to filter out any that are already installed

usr/bin/ssh-copy-id: ERROR: ssh: connect to host 172.16.0.4
ort 22: No route to host

oot@1794a53031b9:/#
```

```
Setting up libkrb5-3:amd64 (1.13.2+dfsg-5ubuntu2.2) ...
Setting up libgssapi-krb5-2:amd64 (1.13.2+dfsg-5ubuntu2.2) ...
Setting up libxmuu1:amd64 (2:1.1.2-2) ...
Setting up openssh-client (1:7.2p2-4ubuntu2.10) ...
Setting up xauth (1:1.0.9-1ubuntu2) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
root@00928af68d5f:/# cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.4      00928af68d5f
root@00928af68d5f:/#
```

```
Setting up libk5crypto3:amd64 (1.13.2+dfsg-5ubuntu2.2) ...
Setting up libkeyutils1:amd64 (1.5.9-8ubuntu1) ...
Setting up libkrb5-3:amd64 (1.13.2+dfsg-5ubuntu2.2) ...
Setting up libgssapi-krb5-2:amd64 (1.13.2+dfsg-5ubuntu2.2) ...
Setting up libxmuu1:amd64 (2:1.1.2-2) ...
Setting up openssh-client (1:7.2p2-4ubuntu2.10) ...
Setting up xauth (1:1.0.9-1ubuntu2) ...
Processing triggers for libc-bin (2.23-0ubuntu11.3) ...
root@55b30f70ebff:/# cat /etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.3      55b30f70ebff
root@55b30f70ebff:/#
```

[11] Add the target machine(s) on Ansible master
#nano /etc/ansible/hosts (Append the lines and save it)



```
  GNU nano 2.5.3                    File: /etc/ansible/hosts

[webserver]
172.17.0.3





                                   [ Read 2 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page
```

[webserver]
172.17.0.3
[12] Test the Ansible-master and target machine
#ansible -m ping 172.17.0.3

[13] Create the target-machine related YAML file
#cd /etc/ansible
#nano packages.yml

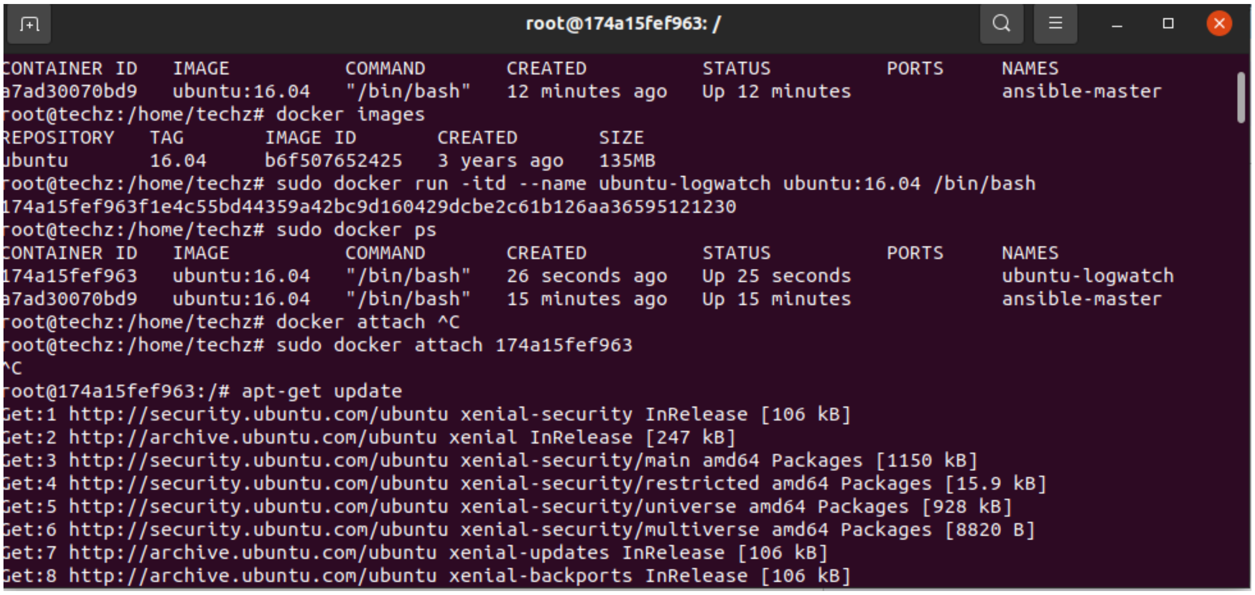
Add the following lines or as per your requirement:

```
- hosts: all
  become: true
  tasks:
  - name: Install logwatch
    ansible.builtin.apt:
    name: logwatch
```

On Target Machine (Ubuntu)- Logwatch as HIDS

[1] sudo docker run -itd --name ubuntu-logwatch ubuntu:16.04 /bin/bash

[2] sudo docker ps
[3] sudo docker attach <container id of ubuntu-logwatch>
[4] apt-get update; apt-get install nano net-tools iputils-ping python openssh-server -y
[5] nano /etc/ssh/sshd_config
(Allow root login- yes)
[6] service ssh restart



```
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
a7ad30070bd9   ubuntu:16.04   "/bin/bash"   12 minutes ago   Up 12 minutes             ansible-master
root@techz:/home/techz# docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
ubuntu       16.04     b6f507652425   3 years ago   135MB
root@techz:/home/techz# sudo docker run -itd --name ubuntu-logwatch ubuntu:16.04 /bin/bash
174a15fef963f1e4c55bd44359a42bc9d160429dcbe2c61b126aa36595121230
root@techz:/home/techz# sudo docker ps
CONTAINER ID   IMAGE          COMMAND       CREATED          STATUS          PORTS     NAMES
174a15fef963   ubuntu:16.04   "/bin/bash"   26 seconds ago   Up 25 seconds             ubuntu-logwatch
a7ad30070bd9   ubuntu:16.04   "/bin/bash"   15 minutes ago   Up 15 minutes             ansible-master
root@techz:/home/techz# docker attach ^C
root@techz:/home/techz# sudo docker attach 174a15fef963
^C
root@174a15fef963:/# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [106 kB]
Get:2 http://archive.ubuntu.com/ubuntu xenial InRelease [247 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [1150 kB]
Get:4 http://security.ubuntu.com/ubuntu xenial-security/restricted amd64 Packages [15.9 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [928 kB]
Get:6 http://security.ubuntu.com/ubuntu xenial-security/multiverse amd64 Packages [8820 B]
Get:7 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [106 kB]
Get:8 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [106 kB]
```

Follow the STH tutorials for further configuration and deployment

On Ansible-master node

```
#cd /etc/ansible/
#ansible-playbook packages.yml
Create  apache.yml file
#nano apache.yml
---
- hosts: all
  become: true
  tasks:
  - name: Install Apache
  ansible.builtin.apt:
      name: apache2
```

```
#ansible-playbook apache-yml
```

Conclusion:

In this lab, we took significant steps toward mastering Ansible as an automation tool for managing network applications and security devices. By setting up our inventory and creating playbooks, we were able to automate the installation and configuration of essential software like Apache and monitoring tools such as Logwatch.

This really highlighted how automation can simplify our workflows, reduce human errors, and enhance efficiency in our IT operations.

I explored the integration of various security measures, like Host Intrusion Detection Systems (HIDS) and Network Intrusion Detection Systems (NIDS), which are crucial for strengthening our network defenses.

Overall, this lab not only deepened our understanding of Ansible but also showcased its real-world applications. these skills will help me manage complex IT environments more effectively and improve our approach to cybersecurity.

References:
[1] https://www.softwaretestinghelp.com/ansible-tutorial-1/

[2] https://www.softwaretestinghelp.com/ansible-playbooks-ansible-vaults/

[3] https://www.softwaretestinghelp.com/ansible-roles-jenkins-integration-ec2-modules/

[4] Ansible: Automating Linux
https://blog.devops.dev/ansible-automating-linux-servers-81da5841e8a2

[5] Ansible Series
https://www.tecmint.com/understand-core-components-of-ansible/