YAML Scripts

root@12988e292a61:/etc/ansible# cat install-elk.yml

---

- name: Configure Elk VM with Docker

hosts: elk

remote\_user: azadmin

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

# Use apt module

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

# Use command module

- name: Increase virtual memory

command: sysctl -w vm.max\_map\_count=262144

# Use sysctl module

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: "262144"

state: present

reload: yes

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

# Please list the ports that ELK runs on

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

root@12988e292a61:/etc/ansible# cat pentest.yml

---

- name: Config Web VM with Docker

hosts: webservers

become: true

tasks:

- name: docker.io

apt:

force\_apt\_get: yes

update\_cache: yes

name: docker.io

state: present

- name: Install pip3

apt:

force\_apt\_get: yes

name: python3-pip

state: present

- name: Install Docker python module

pip:

name: docker

state: present

- name: download and launch a docker web container

docker\_container:

name: dvwa

image: cyberxsecurity/dvwa

state: started

published\_ports: 80:80

- name: Enable docker service

systemd:

name: docker

enabled: yes

root@12988e292a61:/etc/ansible# cat elk.yml

- name: Configure Elk VM with Docker

hosts: elk

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

force\_apt\_get: yes

name: docker.io

state: present

# Use apt module

- name: Install python3-pip

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module (It will default to pip3)

- name: Install Docker module

pip:

name: docker

state: present

# Use command module

- name: Increase virtual memory

command: sysctl -w vm.max\_map\_count=262144

# Use sysctl module

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: "262144"

state: present

reload: yes

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

# Please list the ports that ELK runs on

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

root@12988e292a61:/etc/ansible/roles# cat filebeat-config.yml

---

- name: installing and launching filebeat

hosts: elk

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.6.1-amd64.deb

- name: drop in filebeat.yml

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat service

command: sudo service filebeat start

root@12988e292a61:/etc/ansible/roles# cat metricbeat-playbook.yml

- name: Install metric beat

hosts: elk

become: true

tasks:

# Use command module

- name: Download metricbeat

command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbe$

# Use command module

- name: install metricbeat

command: dpkg -i metricbeat-7.6.1-amd64.deb

# Use copy module

- name: drop in metricbeat config

copy:

src: /etc/ansible/files/metricbeat-config.yml

dest: /etc/metricbeat/metricbeat.yml

# Use command module

- name: enable and configure docker module for metric beat

command: metricbeat modules enable docker

# Use command module

- name: setup metric beat

command: metricbeat setup

# Use command module

- name: start metric beat

command: sudo service metricbeat start