**Ansible Config Files:**

#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

#elk.yml:

---

- name: Config Elk VM with Docker

hosts: ELK

remote\_user: zbravos

become: true

tasks:

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: '262144'

state: present

reload: yes

- 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: elk

image: sebp/elk:761

state: started

restart\_policy: always

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

- name: Enable docker service

systemd:

name: docker

enabled: yes

#filebeat-playbook.yml:

---

- name: Installing and Launch Filebeat

hosts: webservers

become: yes

tasks:

- name: Download filebeat .deb file

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

- name: Install filebeat .deb

command: dpkg -i filebeat-7.4.0-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: service filebeat start

- name: Enable service filebeat on boot

systemd:

name: filebeat

enabled: yes