GNU nano 2.9.3 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

GNU nano 2.9.3 elk.yml

---

- name: Config ELK VM with Docker

hosts: elk

remote\_user: azureuser

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: Use more memory

sysctl:

name: vm.max\_map\_count

value: '262144'

state: present

reload: yes

- name: download and run docker elk container

docker\_container:

name: sebp

image: sebp/elk:761

state: started

restart\_policy: always

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

- name: Enable docker service on boot

systemd:

name: docker

enabled: yes

GNU nano 2.9.3 filebeat-playbook.yml

---

- name: Installing and Launch Filebeat

hosts: webservers

become: yes

tasks:

- name: Download filebeat and install - update link for latest version

apt:

deb: https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-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

GNU nano 2.9.3 metricbeat-playbook.yml

---

- name: Install metric beat

hosts: webservers

become: true

tasks:

- name: Download metricbeat

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

- name: install metricbeat

command: dpkg -i metricbeat-7.4.0-amd64.deb

- name: drop in metricbeat config

copy:

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

dest: /etc/metricbeat/metricbeat.yml

- name: enable and configure docker module for metric beat

command: metricbeat modules enable docker

- name: setup metric beat

command: metricbeat setup

- name: start metric beat

command: service metricbeat start

- name: Enable service metricbeat on boot

systemd:

name: metricbeat

enabled: yes