Jordan Bow

Project 1

Scripts:

Pentest.yml

---

- name: Config Web VM with Docker

hosts: webservers

become: true

tasks:

- name: docker.io

apt:

update\_cache: yes

name: docker.io

state: present

- name: Install pip3

apt:

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

restart\_policy: always

published\_ports: 80:80

- name: Enable docker service

systemd:

name: docker

enabled: yes

Elkplay.yml

---

- name: Config Web VM with Docker

hosts: elk

become: true

tasks:

- ansible.posix.sysctl:

name: vm.max\_map\_count

value: 262144

state: present

- name: docker.io

apt:

update\_cache: yes

name: docker.io

state: present

- name: Install pip3

apt:

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-761

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: Config Web VM with Filebeat

hosts: webservers

become: true

tasks:

- name: .deb download

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

- name: .deb installation

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

- name: Copy config to W1 W2

copy:

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

dest: /etc/filebeat/filebeat.yml

- name: Filebeat command 1

command: filebeat modules enable system

- name: Filebeat command 2

command: filebeat setup

- name: Filebeat command 3

command: service filebeat start

- name: enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

Metricbeat-playbook.yml

---

- name: Config Web VM with Filebeat

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

- name: Copy config to W1 W2

copy:

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

dest: /etc/metricbeat/metricbeat.yml

- name: Enable docker

command: metricbeat modules enable docker

- name: Metricbeat setup

command: metricbeat setup

- name: enable service metricbeat on boot

systemd:

name: metricbeat

enabled: yes