Vulnerable Machines with Ansible

Nathaniel Beckstead

whoami

Nathaniel Beckstead

Automation

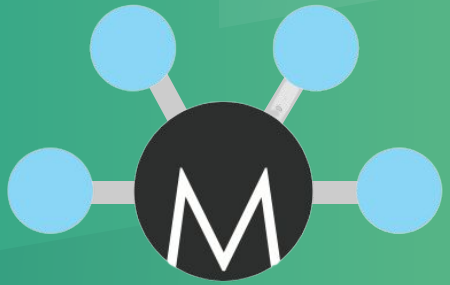
Infrastructure

Tooling

scriptingis.life

Why Vulnerable Machines?

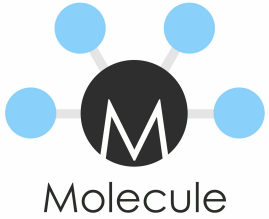
- King of the Hill
- Practice
  - Red team - scan and exploit
  - Blue team - audit configs
- Testing tools
  - Vulnerability scanner




ANSIBLE

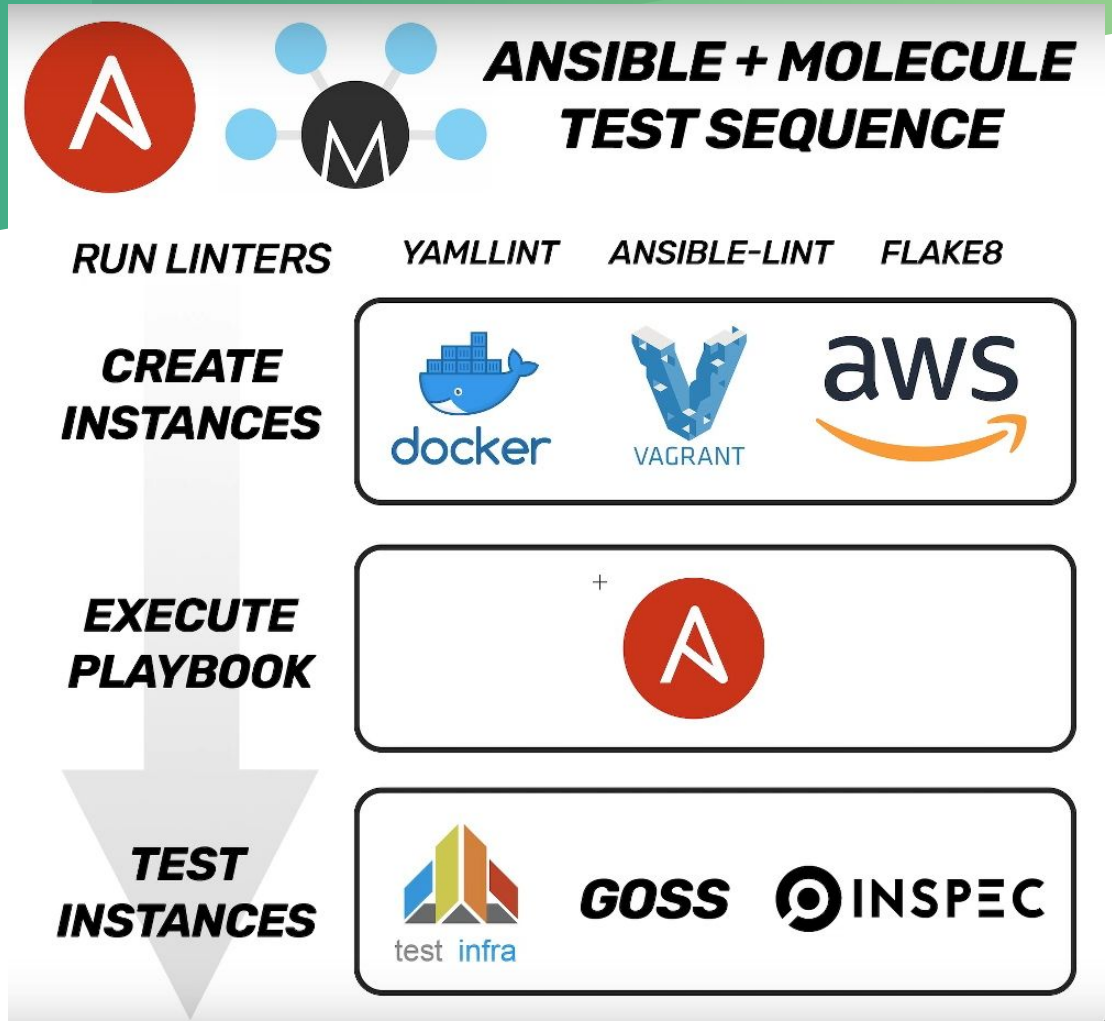
1.
Molecule

Manager



Molecule

- Manage execution and testing of roles
- Write best roles possible



[Rapidly Build & Test Ansible Roles with Molecule + Docker]

2.
Vagrant

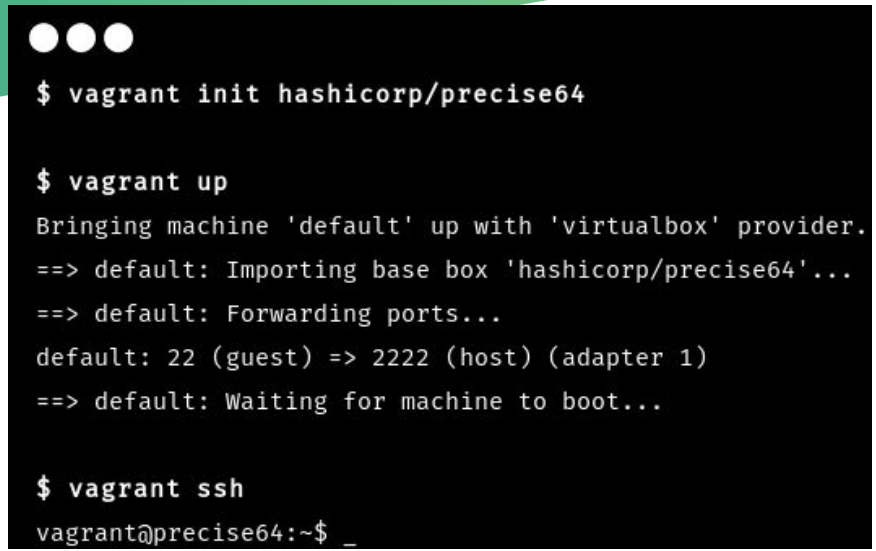
Virtual machine creation

Vagrant

- Infrastructure as code
- Automated virtual machines

```
Vagrant.configure(2) do |config|
  config.vm.box = "ubuntu/xenial64"
  config.vm.network "forwarded_port", guest: 80, host: 8080
end
```

Vagrant


$ vagrant init hashicorp/precise64
$ vagrant up
Bringing machine 'default' up with 'virtualbox' provider.
==> default: Importing base box 'hashicorp/precise64'...
==> default: Forwarding ports...
default: 22 (guest) => 2222 (host) (adapter 1)
==> default: Waiting for machine to boot...
$ vagrant ssh
vagrant@precise64:~$ _

3.
Ansible

Vulnerability automation

Ansible

- Automate configuration of software
- Manage fleet of servers from your laptop

Ansible Roles

- Single role for each service
  - HTTP
  - SQL
- Cron
  - Random Shells
  - New Users

PHP Web Shell

Random Bind Shells

Anonymous FTP

Shellshock

Open SMB Shares

SMTP Backdoor

Random Users

Trickshot

Apache Tomcat

Unauthenticated SSH

Telnet

Ansible Playbooks

- Combine roles to create a useful configuration

Ansible Playbooks

- Create cron job to open shells on random ports
- Install telnet
- Edit PAM module to disable SSH authentication. Allow everyone in.

```
---
- hosts: vulnerable
  tasks:
    - name: Constant random shells
      include_role:
        name: common/cron
      vars:
        - do_random_shells: true

    - name: Install telnet
      include_role:
        name: service/telnet

    - name: Make ssh vulnerable
      include_role:
        name: service/ssh
      vars:
          - do_insecure_login: true
```

Demo

Thanks!

https://github.com/becksteadn/Bytes-Of-Swiss/