Security Benchmark Implementation for Linux

Lizette Ponce - Poolesville High School
Mentored by Dr. Alan Munter

Introduction

- NIST is a government organization; stores important data
    - Needs to be protected from cyber attacks
    - Cyberattacks evolving each day; defenses must be improved

Project Goal

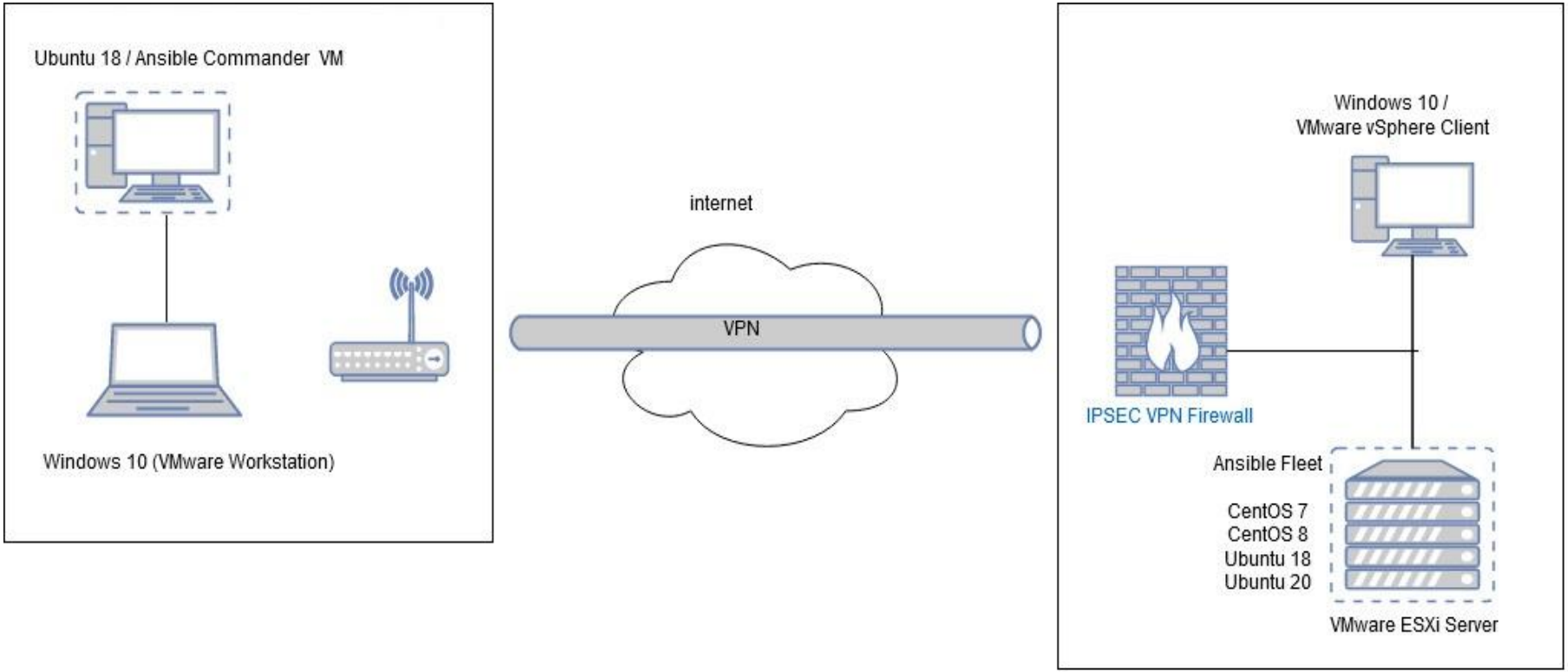
- Test benchmarks set by the Center for Internet Security (CIS) for the Linux OS
  - Focus on Ubuntu Linux
- Ensure defenses are up to par

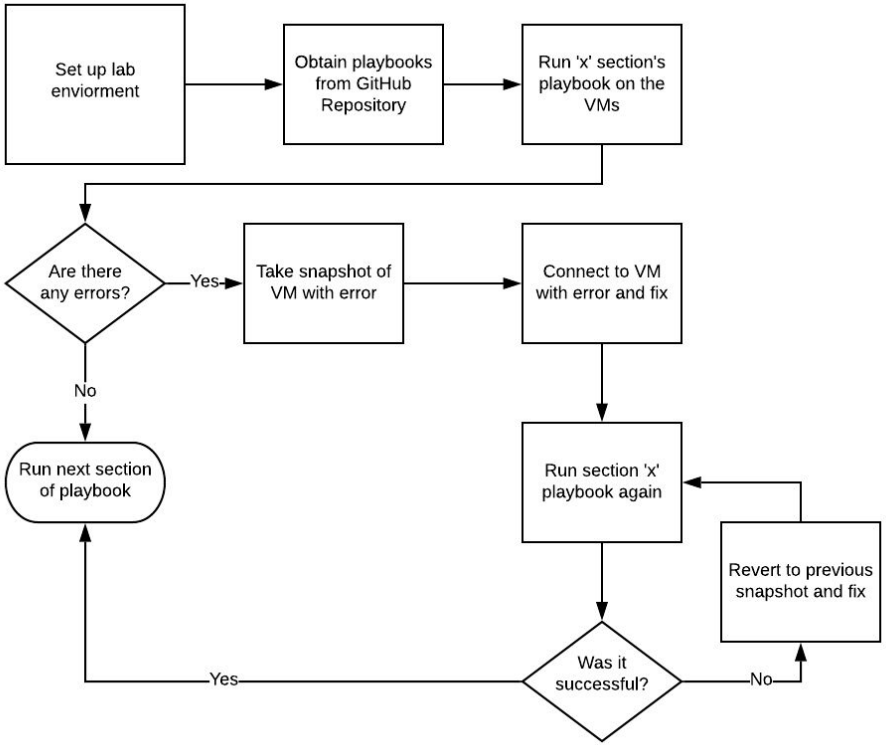
How will it be done

- CIS Benchmarks for Linux have been turned into ansible playbooks (list of tasks to run)
  - Written in python
  - Playbooks for each benchmark section (6)

```
- name: "SCORED | 1.1.1.1 | PATCH | Remove cramfs module"
  modprobe:
      name: cramfs
      state: absent
  when:
      - cis_rule_1_1_1_1|bool
      - ansible_connection != 'docker'
  tags:
      - level1
      - scored
      - patch
      - section1
      - rule_1.1.1.1
      - cramfs
```

Lab Environment




Set up lab enviorment
Obtain playbooks from GitHub Repository
Run 'x' section's playbook on the VMs
Are there any errors?
Yes
Take snapshot of VM with error
Connect to VM with error and fix
No
Run next section of playbook
Run section 'x' playbook again
Revert to previous snapshot and fix
Was it successful?
Yes
No

Process

Example

- CIS considered this program “unneeded”
  - Removing it helps reduce attack surface
- Successful; both VMs do not have the cramfs filesystem and passed

```
TASK [dilcis-ansible : SCORED | 1.1.1.1 | PATCH | Ensure mounting of cramfs filesystems is disabled] ***************************************
ok: [ubuntu20]
ok: [ubuntu18]

TASK [dilcis-ansible : SCORED | 1.1.1.1 | PATCH | Remove cramfs module] ***********************************************************************
ok: [ubuntu20]
ok: [ubuntu18]
```

Future Steps

- Work on other linux distributions (Centos)
- Await any new CIS Benchmarks to be announced

Thanks to:

Any questions?