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)
Lab Environment

Ubuntu 18 / Ansible Commander VM

Windows 10 (VMware Workstation)

internet

VPN

IPSEC VPN Firewall

Ansible Fleet
- CentOS 7
- CentOS 8
- Ubuntu 18
- Ubuntu 20

Windows 10 / VMware vSphere Client

VMware ESXi Server
Set up lab environment

Obtain playbooks from GitHub Repository

Run 'x' section's playbook on the VMs

Are there any errors?

Yes → Take snapshot of VM with error

No → Run next section of playbook

Connect to VM with error and fix

Run section 'x' playbook again

Was it successful?

Yes → Revert to previous snapshot and fix

No → Run next section of playbook
Example

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

- Work on other Linux distributions (Centos)
- Await any new CIS Benchmarks to be announced
Thanks to: NSF

Any questions?