SCAP REFRESHER

Ansible Introduction and Usage of SCAP Workbench

PRESENTER INTRODUCTION

- **Speaker:** Travis Michette
- **Github Project:** https://github.com/tmichett/LUG
- **Presentation and Materials:** Located in the **Ansible_Roles** directory of the Github project.

ANSIBLE INTRODUCTION & OVERVIEW

- **Ansible** – An automation language leveraging modules to be used in one or more tasks on managed systems. Most Ansible automation leverages and Ansible playbook which is a YAML formatted file containing Ansible directives.

- **Ansible modules** – Components used by Ansible tasks and playbooks which are generally implemented and developed in Python. Ansible modules work with certain system utilities and are optimized to be leveraged as a declarative automation language and provide idempotency.

- **Ansible ad-hoc commands** – A way of executing a single Ansible task quickly that relies on a single Ansible module to perform the tests/changes of the task.

ANSIBLE.CFG FILE

- This file defines the configuration directives which apply directly to how the **ansible and ansible-playbook** command interact with the Ansible application and which configuration items are applied to a given Ansible session.
  - **./ansible.cfg** – When located in the current working directory (CWD) this file is the highest precedence.
  - **~/.ansible.cfg** – When located in the user's home directory, this file will have precedence if an *ansible.cfg* doesn't exist in the CWD.
  - **/etc/ansible/ansible.cfg** – This is the default configuration file and has the lowest precedence. This file is used when no other *ansible.cfg* file exists.

Important	It is also possible to define the **ansible.cfg** file with the environment variable **ANSIBLE_CONFIG**. If this variable is used, it will override all other configuration files.

INVENTORY FILE

- The **inventory** file can contain both Ansible managed hosts/nodes as well as inventory variables to be used for the managed nodes.
  - Inventory location is generally specified by the **ansible.cfg** file
    - **./inventory** – Common practice to leverage inventory files with playbooks and the **ansible.cfg** file in the current working directory
    - **/etc/ansible/hosts** – Default inventory file deployed with the Ansible package

SCAP WORKBENCH AND OPENSCAP

- **SCAP:** The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization, including e.g., FISMA compliance. The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP. An example of an implementation of SCAP is OpenSCAP
  - https://csrc.nist.gov/projects/security-content-automation-protocol

- **OpenSCAP:** An auditing tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard way of expressing checklist content and defines security checklists
  - https://www.open-scap.org/

- **SCAP Workbench**: Graphical utility that allows an easy way to interact and perform common ***oscap*** tasks. It also provides an easy way to modify and tailor ***XCCDF*** profiles.

DEMO

USING SCAP WORKBENCH AND ANSIBLE