Security Automation Workshop

Sultan Taj - SUNY Poly ‘24

What we'll be going over today

1. What is Ansible?
2. How does Ansible work?
3. How can we use Ansible for Cybersecurity?
4. Workshop Lab Scenario: CIS Benchmark Configurations

Ansible

Ansible is an open-source automation tools for managing IT infrastructure using YAML code, and is popular for automating Linux servers.

- YAML (Yet Another Markup Language) is human readable data primary used for config files.
- Ansible has thousands of modules for different technologies, being able to support:
  - OS (Linux, Windows, macOS)
  - Cloud (AWS, Azure, GCP, Oracle, IBM)
  - Containers (Docker, Kubernetes)
  - DevOps & CI/CD
  - Network Devices
  - Databases
  - Applications & Services

Core components of Ansible

1. Control Node
   - Ansible operates from a main machine called the control node, which is a like a “command center” for managing other machines.
2. Managed Nodes
   - The control node connects to one or more managed nodes (other servers or devices) to perform tasks on them.
3. Playbooks
   - Tasks are organized in files called playbooks. A playbook is like a checklist that tells each managed node what to do.
   - Ex: Install software, update settings, and configure security policies.
4. Idempotence
   - Ansible only makes changes if needed. If a setting is already correct, it leaves it alone.
   - Helps avoid accidental changes and ensures consistency across all machines.
5. Simple Secure Automation
   - Everything is done over SSH.

Ansible in Cybersecurity

There are many different fields within cybersecurity that involve some form of repetitive task. Using Ansible, you can automate it to do your simpler tasks.

1. Automating Security Configurations
    - Ansible can enforce security policies consistently across multiple machines, like firewall rules and secure access configurations.
2. Vulnerability Management
    - Quickly deploy patches or updates to address security vulnerabilities, ensuring all systems are up-to-date.
3. Access Control and Compliance
    - Configure access permissions, disable insecure protocols, and meet compliance requirements
4. Incident Response Preparation
    - Ansible playbooks can be set up to automatically deploy detection tools, apply security policies, and even set up alerts

Lab Introduction

It's your first day as a Security Analyst, and you've been tasked with setting up baseline security configurations for a Linux server. Your goal is to secure the server against unauthorized access and potential attacks by applying CIS benchmark standards to an Ubuntu 24.04 LTS server.

What you'll need:

1. Laptop with VMWare or VirtualBox
2. Ubuntu VM (preferably 24.04 LTS)
3. Ansible

Follow along with my guide on my Github:

- https://github.com/STaj-55/Ansible-Workshop