Lab 10 - Configuration Management

Table of Contents

Lab Descriptors

Logistics

Due Date:	November 20, 2020 at 11:59pm
Submission Location:	iLearn for documents, cyber range environment for systems
Points Available:	8

Objectives

To learn how to properly configure and use SSH for secure control of a system and how to generate and use SSH keys.

Assumptions

The student has some base knowledge of unix-based systems.

Outcomes

The student will have a properly configured SSH server that uses SSH keys to authenticate.

Topics Addressed

- CSF - 10 CIAAA-NP
- CSF - 13 Security Mechanisms
- CSP - 1A - 1N Core Cyber Principles
- ISC - 2 Storage Devices
- ISC - 3A - 3B Virtualization/Cloud
- ISC - 5 Networks
- ISC - 7 Network Security Components
- ISC - 11 Configuration Management
- LSA - 3 Command Line Interfaces
- LSA - 4 Configuration Management
- LSA - 7 Virtualization
- LSA - 11 Network Configuration
- OSA - 3 Command Line Interfaces
- OSA - 4 Configuration Management

- OSA - 7 Managing System Services
- OSA - 8 Virtualization
- WSA - 8 Virtualization

NICE Framework Categories

- Securely Provision (SP)
- Operate and Maintain (OM)

Introduction

This lab will cover configuration management using SaltStack. The lab will also provide an introduction to working with Docker containers.

Lab Details

NOTE: This lab will be entirely on the WWW machine.

Docker

1. Run **git clone https://github.com/Da-Juan/saltstack-test-lab.git**
2. Inside the new directory, edit the **docker-compose.yml** file
3. Remove line 53. It should say **name: saltstack**. This line throws an error
4. Install **docker** and **docker-compose** from apt
5. While in the **saltstack-test-lab** directory run **sudo docker-compose up -d**
    a. The -d detaches the docker console
6. Run **sudo docker exec -it saltstack-master /bin/bash**
    a. This will drop you into a root shell in the saltstack-master container. This is where you will complete the rest of the lab.

SaltStack

1. Check for minion keys, run **salt-key -L**
2. Accept all minion keys using **salt-key -A**
3. Test your connection to all minions using **salt '*' test.ping** (Screenshot result)
4. Create a file named **top.sls** in /srv/pillar/

```
base:
  '*':
    - defaults
```

5. Create a folder in **/srv/pillar/** named **defaults** and then create a file named **init.sls** inside of it.

```
editor: vim
```

6. Create a file named **top.sls** in /srv/salt/

```
base:
  '*':
    - defaults
```

7. Create a folder in **/srv/salt/** named **defaults** and then create a file named **init.sls** inside of it.

```
vim installed:
  pkg.installed:
    - name: {{pillar['editor'] }}
```

8. Run **salt '*' saltutil.refresh_pillar** and then run **salt '*' state.apply** (screenshot state.apply result)

SaltStack Extended

Now that you have successfully installed vim with Salt, you can start writing your own states!

You do not have to use pillars for these, but as your company grows or the size of controlled machines grows, pillars become a valuable resource. All of these can be done with just states however.

Using Salt:

1. Install **apache2** to minion1 and **nginx** to minion2.
2. Add your own Message of the Day to both minions. The message can be whatever you want.
3. Add a user named: **devops** with password as **Password123**!
4. **NOT WITH SALT**. On the master, create a file called **test** and put whatever you want in the file. Move the file to **/srv/salt/files/**
5. Send the file to **/home/devops/**
6. Install **openssh-server** on both minions.
7. Test ssh to at least one minion.
8. Verify that your test file is where you sent it to.
   Screenshot the results

Deliverables

1. Submit your updated changelog and screenshots

2. Why would you want to use a configuration management tool like SaltStack?
3. How could an attacker use SaltStack in a malicious attack?
4. What is the difference between a pillar and a state? Why would we use pillars?

Resources

SSH Manual
https://linux.die.net/man/1/ssh

SaltStack Tutorial
https://docs.saltstack.com/en/getstarted/config/functions.html

SaltStack Docs
https://docs.saltstack.com/en/latest/topics/using_salt.html

Sending Files with Salt
https://docs.saltstack.com/en/latest/ref/states/all/salt.states.file.html

Adding Users with Salt
https://docs.saltstack.com/en/3000/ref/states/all/salt.states.user.html

Awesome Salt Book
https://subscription.packtpub.com/book/networking_and_servers/9781784399740/1/ch01lvl1sec12/understanding-and-configuring-salt-pillars

MOTD with Salt
https://codingpackets.com/blog/salt-from-the-start-to-the-beginning/