AWS AD Lab Project Plan

Selin Kabak

April 8, 2025

1 Project Overview

1.1 Description

This hands-on cybersecurity lab project focuses on implementing and securing Windows Server and Active Directory infrastructure in AWS using Infrastructure-as-Code principles. The project utilizes Terraform for infrastructure provisioning, Vagrant for development environments, and Ansible for configuration automation, providing a practical learning environment for cloud security concepts.

1.2 Objectives

This hands-on lab project will teach me how to set up and manage Active Directory in AWS cloud. I will learn how to build a complete test environment that mirrors real-world setups, but in a way that's safe for learning and experimenting.

I will start by learning how to use Terraform to create the basic AWS building blocks - like virtual networks (VPCs). Using Vagrant, I'll create a local test environment on my computer where I can practice configurations safely before trying them in AWS.

For the Windows Server part, I'll learn how to automatically set up and configure servers using Ansible. This includes installing Active Directory, creating user accounts, setting up security policies, and making sure everything is properly secured. I'll focus on understanding how Active Directory works in the cloud, including how to set up domain controllers and manage users and groups.

The project will teach me about common security problems in Active Directory and how to fix them. This includes setting up proper backups, monitoring for security issues, and knowing what to do if something goes wrong. I'll also learn how to properly test my setups and keep track of changes using version control.

2 Steps to Take

2.1 Learning the Tools

Before diving into the actual implementation, I need to understand the basic tools:

1. Learn AWS fundamentals
    - Get familiar with VPC, EC2, Security Groups through the AWS Console
2. Get comfortable with Terraform
    - Practice creating and destroying simple resources
    - Learn about state files and variable management

3. Set up Vagrant environment
    - Create a simple Windows Server VM
    - Learn basic Vagrant commands and configuration
4. Learn Ansible basics
    - Practice with simple playbooks
    - Learn Windows-specific Ansible modules

2.2 Implementation Tracks

Track 1: Local Testing Environment

- Create Vagrant file for Windows Server VM
- Set up local Active Directory in VM
- Practice AD management tasks locally
- Test Ansible playbooks against local VM

Track 2: AWS Infrastructure

- Write basic Terraform config for VPC
- Add security groups and subnets
- Create Windows Server EC2 instance
- Test connectivity and access

Track 3: Automation Development

- Write Ansible playbooks for Windows setup
- Create AD installation and configuration scripts
- Develop user and group management automation
- Test automation scripts locally first

2.3 Integration Points

Key moments where different tracks come together:

- When local AD setup works, move configurations to AWS
- Test Ansible playbooks on AWS instances
- Combine Terraform and Ansible for full automation

2.4 Learning Notes

Things to document as I go:

- Tool installation steps and issues faced
- Common AWS and AD configuration problems
- Successful configurations and why they work

3 Resources & References

TOOLS

- Attacking Active Directory
- SIGMA detection rules for SIEM
- InSpec: Infrastructure Testing Framework
- Official VMware Automation Collection for Ansible
- Ansible Best Practices and Standards
- Setting Up Ansible Test Environment on Windows
- AWS AD with MFA using Terraform

EXAMPLES

- AD Delegation Lab
- AD Lab
- AD Lab with Attack Scenarios
- Automated AD Lab Deployment using Ansible
- Multi-Platform AD Environment with Ansible
- AD Setup with Groups and Users
- Automated Windows Server Deployment in vSphere

DOCS

- Terraform Documentation
- Vagrant Documentation
- Ansible Windows Integration