AWS Inspector Basic Lab Workshop

Step-by-Step Guide

Table of Contents

1. Prerequisites
2. Lab Overview
3. Step 1: Environment Setup
4. Step 2: Enable AWS Inspector
5. Step 3: Launch EC2 Instances
6. Step 4: Configure Inspector Assessment
7. Step 5: Run Vulnerability Scan
8. Step 6: Analyze Results
9. Step 7: Remediation
10. Step 8: Cleanup
11. Additional Resources

Prerequisites

Required Knowledge

- Basic understanding of AWS console navigation
- Familiarity with EC2 instances
- Understanding of IAM roles and policies
- Basic Linux command line knowledge

Required Access

- AWS Account with administrative privileges
- Access to the following AWS services:
  - Amazon Inspector
  - Amazon EC2
  - AWS IAM
  - AWS Systems Manager

Estimated Time

Total Duration: 2-3 hours

Lab Overview

What You'll Learn

- How to enable and configure Amazon Inspector
- How to scan EC2 instances for vulnerabilities
- How to interpret Inspector findings
- How to implement basic remediation strategies
- Best practices for ongoing vulnerability management

What You'll Build

- A vulnerable EC2 instance for testing
- Inspector assessment configuration
- Vulnerability scanning workflow
- Remediation plan based on findings

Step 1: Environment Setup

1.1 Access AWS Console

1. Navigate to AWS Management Console
2. Sign in with your AWS account credentials
3. Ensure you're in your preferred AWS region (e.g., us-east-1)

1.2 Verify Required Permissions

1. Navigate to **IAM** → **Users** → Your username
2. Verify you have the following managed policies attached:
   - `AmazonInspectorFullAccess`
   - `EC2FullAccess`
   - `IAMFullAccess`
   - `AmazonSSMFullAccess`

1.3 Create IAM Role for Inspector

1. Go to **IAM** → **Roles** → **Create role**
2. Select **AWS service** → **EC2**

3. Attach the following policies:
    - `AmazonSSMManagedInstanceCore`
    - `AmazonInspectorAssessmentAgent`
4. Name the role: `InspectorEC2Role`
5. Click **Create role**

Step 2: Enable AWS Inspector

2.1 Navigate to Inspector Service

1. In the AWS Console, search for "Inspector"
2. Click on **Amazon Inspector**
3. If this is your first time, you'll see the welcome screen

2.2 Enable Inspector

1. Click **Get started** or **Enable Inspector**
2. Choose **Enable Inspector** for your account
3. Select the types of resources to scan:
    - ✅ **Amazon EC2 instances**
    - ✅ **Amazon ECR container images**
    - ✅ **AWS Lambda functions**
4. Click **Enable Inspector**

2.3 Configure Inspector Settings

1. Go to **Inspector** → **Settings**
2. Configure the following:
    - **Auto-enable**: Turn on for EC2 instances
    - **Scan frequency**: Continuous monitoring
    - **Finding aggregation**: 24 hours

Step 3: Launch EC2 Instances

3.1 Launch Primary Test Instance

1. Navigate to **EC2** → **Instances** → **Launch Instance**
2. Configure the instance:
    - **Name**: `Inspector-Test-Instance-1`

   - **AMI**: Amazon Linux 2023 (latest)
   - **Instance Type**: t3.micro
   - **Key Pair**: Create new or use existing
   - **Security Group**: Create new with SSH (port 22) access
   - **IAM Role**: Select `InspectorEC2Role`
3. In **Advanced Details**:
   - **User Data**: Add the following script:

```bash
#!/bin/bash
yum update -y
yum install -y httpd php mysql
systemctl start httpd
systemctl enable httpd
# Install some intentionally vulnerable packages for testing
yum install -y vsftpd telnet-server
```

4. Click **Launch Instance**

3.2 Launch Secondary Test Instance

1. Repeat the process above with:
   - **Name**: `Inspector-Test-Instance-2`
   - **AMI**: Ubuntu Server 22.04 LTS
   - **Same configuration** as above
   - **User Data** for Ubuntu:

```bash
#!/bin/bash
apt update -y
apt install -y apache2 php mysql-client
systemctl start apache2
systemctl enable apache2
# Install vulnerable packages
apt install -y vsftpd telnetd
```

3.3 Verify Instances

1. Wait for both instances to reach **Running** state
2. Verify they have the **InspectorEC2Role** attached

3. Note down the instance IDs for later reference

Step 4: Configure Inspector Assessment

4.1 Verify Auto-Discovery

1. Go to **Inspector** → **Findings**
2. Click on **Inventory** tab
3. Verify your EC2 instances appear in the inventory
4. This may take 5-15 minutes after instance launch

4.2 Configure Assessment Templates (Classic Inspector)

If using Inspector Classic:

1. Go to **Inspector** → **Assessment templates**
2. Click **Create assessment template**
3. Configure:
   - **Name**: `Basic-Vulnerability-Assessment`
   - **Target**: Select your instances
   - **Rules packages**: Select all available
   - **Duration**: 1 hour
4. Click **Create**

4.3 Set Up Findings Filters

1. Go to **Inspector** → **Findings**
2. Click **Create filter**
3. Configure filters for:
   - **Severity**: High, Critical
   - **Resource type**: EC2 Instance
   - **Status**: Active

Step 5: Run Vulnerability Scan

5.1 Initiate Manual Scan

1. Navigate to **Inspector** → **Assessments**
2. Select your assessment template

3. Click **Run assessment**
4. Monitor the assessment progress

5.2 Monitor Scan Progress

1. Check **Inspector** → **Assessment runs**
2. View real-time progress
3. Estimated completion time: 15-60 minutes

5.3 Verify Systems Manager Integration

1. Go to **Systems Manager** → **Inventory**
2. Verify your instances appear and are managed
3. Check **Compliance** dashboard for patch status

Step 6: Analyze Results

6.1 Review Findings Overview

1. Go to **Inspector** → **Findings**
2. Review the dashboard showing:
    - Total findings count
    - Severity distribution
    - Resource breakdown
    - Trending information

6.2 Examine Individual Findings

1. Click on a **Critical** or **High** severity finding
2. Review the following details:
    - **Title**: Brief description of the vulnerability
    - **Description**: Detailed explanation
    - **Severity**: Risk level assessment
    - **Affected Resource**: Specific instance/component
    - **CVSS Score**: Numerical risk rating
    - **Remediation**: Suggested fix actions

6.3 Generate Assessment Report

1. Go to **Inspector** → **Assessment runs**

2. Select your completed assessment
3. Click **Download report**
4. Choose format: **HTML** or **PDF**
5. Review the comprehensive report

6.4 Key Findings to Look For

Common vulnerabilities you might find:

- Outdated software packages
- Missing security patches
- Insecure service configurations
- Network exposure issues
- Compliance violations

Step 7: Remediation

7.1 Prioritize Findings

1. Sort findings by **Severity** (Critical → High → Medium → Low)
2. Focus on findings with:
   - CVSS score > 7.0
   - Network-accessible vulnerabilities
   - Known exploits available

7.2 Implement Fixes via Systems Manager

1. Go to **Systems Manager** → **Patch Manager**
2. Create a **Patch Baseline**:
   - **Name**: `Critical-Security-Patches`
   - **Operating System**: Linux
   - **Approval rules**: Auto-approve critical/security patches
3. Create **Maintenance Window**:
   - **Name**: `Security-Patching-Window`
   - **Schedule**: Weekly during off-hours
   - **Duration**: 4 hours

7.3 Manual Remediation

For instances requiring manual fixes:

1. **Connect via SSH**:

```bash
ssh -i your-key.pem ec2-user@instance-public-ip
```

2. **Update packages**:

```bash
# Amazon Linux
sudo yum update -y

# Ubuntu
sudo apt update && sudo apt upgrade -y
```

3. **Remove vulnerable services**:

```bash
sudo systemctl stop vsftpd
sudo systemctl disable vsftpd
sudo systemctl stop telnet
```

7.4 Verify Remediation

1. Wait 24 hours for Inspector to rescan
2. Check **Inspector** → **Findings** for status updates
3. Verify critical findings show as **Resolved**

Step 8: Cleanup

8.1 Stop Assessment

1. Go to **Inspector** → **Assessment runs**
2. Stop any running assessments
3. Delete assessment templates if no longer needed

8.2 Terminate EC2 Instances

1. Go to **EC2** → **Instances**

2. Select your test instances
3. Click **Instance state → Terminate**
4. Confirm termination

8.3 Clean Up IAM Resources

1. Go to **IAM → Roles**
2. Delete the `InspectorEC2Role` if created specifically for this lab
3. Review and remove any temporary policies

8.4 Inspector Settings

1. If this was a test environment, consider:
    - Disabling auto-enable for future instances
    - Adjusting scan frequency settings
    - Configuring appropriate finding filters for production

Additional Resources

AWS Documentation

- Amazon Inspector User Guide
- Inspector API Reference
- Inspector Classic User Guide

Best Practices

1. **Regular Scanning**: Enable continuous assessment
2. **Integration**: Connect with AWS Security Hub
3. **Automation**: Use EventBridge for automated responses
4. **Compliance**: Map findings to compliance frameworks
5. **Remediation**: Implement automated patching workflows

Troubleshooting Common Issues

Inspector Agent Issues

- Verify IAM role permissions
- Check Systems Manager agent status
- Ensure network connectivity

No Findings Appearing

- Wait for initial discovery (up to 24 hours)
- Verify resource tags and filters
- Check service enablement status

Assessment Failures

- Review CloudTrail logs
- Verify resource accessibility
- Check assessment template configuration

Cost Optimization

- Use resource tags to control scope
- Schedule assessments during off-peak hours
- Leverage AWS Config for compliance checking
- Implement automated remediation to reduce manual effort

Lab Completion Checklist

□ Successfully enabled Amazon Inspector
□ Created and configured EC2 test instances
□ Ran vulnerability assessments
□ Analyzed findings and generated reports
□ Implemented basic remediation steps
□ Understood Inspector integration with other AWS services
□ Cleaned up lab resources
□ Reviewed additional learning resources

Congratulations! You have successfully completed the AWS Inspector Basic Lab Workshop. You now have hands-on experience with vulnerability assessment and management using Amazon Inspector.

For advanced scenarios, consider exploring:

- Multi-account Inspector deployments
- Integration with AWS Security Hub
- Automated remediation with AWS Systems Manager
- Custom Inspector rules and policies

Document Version: 1.0

Last Updated: September 2025

Lab Duration: 2-3 hours