Awesome Cloud Security Labs

A list of free cloud native security learning labs. Includes CTF, self-hosted workshops, guided vulnerability labs, and research labs.

Sorted by Technology and Category

Name	Technology	Category	Author	Notes
CloudFoxable	AWS	Self-hosted CTF Challenge	Seth Art	Create your own vulnerable by design AWS penetration testing playground
The Big IAM Challenge	AWS	Author-hosted CTF Challenge	Wiz	CTF challenge to identify and exploit IAM misconfigurations
CloudSec Tidbits	AWS	Self-hosted Challenge	Doyensec	Three web app security flaws specific to AWS cloud, self-hosted with terraform
Pentesting.Cloud	AWS	Self-hosted, Author-hosted CTF labs	Nicholas Gilbert	17 free labs, requires registration, some labs are bring your own AWS

Name	Technology	Category	Author	Notes
				account and use cloudformation to create
AWS CIRT Workshop	AWS	Self-hosted, guided lab	AWS CIRT	Build with Cloudformation, explore 5 common incident response scenarios observed by AWS CIRT
CloudGoat	AWS	Self-hosted, guided vulnerability lab	Multiple, Rhino Security Labs	Python orchestration of terraform
Attacking and Defending Serverless Applications	AWS	Self-hosted, guided vulnerability workshop	Ryan Nicholson	Attack and defend a Lambda that you build in your own AWS account with author provided terraform
IAM Vulnerable	AWS	Self-hosted, guided vulnerability lab	Seth Art	IAM-focused priv esc playground with 31 pathways, create in your own AWS account using terraform, solid docs
flaws.cloud	AWS	Author-hosted, CTF challenge	Scott Piper	Challenge style with levels and clues
flaws2.cloud	AWS	Author-hosted, CTF challenge	Scott Piper	Challenge style Attacker and Defender paths
CI/CDon't	AWS	Self-hosted CTF walkthrough	Nick Frichette	Host with terraform in your own AWS account, vulnerable CI/CD CTF infrastructure
AWSGoat	AWS	Self-hosted, attack and defense manuals	Multiple, ine-labs	Bring your own aws account, Build with terraform, two modules, provides attack and defense manuals

Name	Technology	Category	Author	Notes
Sadcloud	AWS	Self-hosted	Multiple, NCC Group	Terraform code; not guided like CloudGoat
DVCA	AWS	Self-hosted demo lab	Maxime Leblanc	Deploy a Damn Vulnerable Cloud Application in your own AWS account to practice privilege escalation
lambhack	AWS	Self-hosted lab	James Wickett	Deploy a very vulnerable AWS lambda serverless application in your AWS account
BadZure	Azure	Self-hosted lab	Mauricio Velazco	Powershell Graph SDK script that spins up your own Azure AD (Entra ID) lab with attack paths. Currently no walk through or guide.
Broken Azure	Azure	Author-hosted, CTF challenge	Secura	Provides hints, optionally self-host in your own Azure account using terraform
PurpleCloud Azure AD Workshop	Azure	Self-hosted, guided vulnerability workshop	Jason Ostrom	Guided vulnerability workshop requires PurpleCloud and terraform; username and password is `sec588`
Mandiant Azure Workshop	Azure	Self-hosted, guided commands	Multiple	Vulnerable by design Azure lab with two scenarios; build with terraform
AzureGoat	Azure	Self-hosted, attack and defense manuals	Multiple, ine-labs	Bring your own Azure tenant, Build with terraform, one module,

Name	Technology	Category	Author	Notes
				provides attack and defense manuals
XMGoat	Azure	Self-hosted, guided labs	Multiple	Build with terraform, 5 scenarios, solution docs provided
CONVEX	Azure	Self-hosted, CTF	Multiple	Spin up three Capture the Flag environments in your Azure tenant using powershell
GCP Goat (Josh Jebaraj)	GCP	Self-hosted, mdbook lab guide	Josh Jebaraj	Host in your own GCP account, build with provided scripts, nice guided lab workbook
GCPGoat (ine-labs)	GCP	Self-hosted, attack and defense manuals	Multiple, ine-labs	Bring your own GCP account, Build with terraform, one module, provides attack and defense manuals
Thunder CTF	GCP	Self-hosted, CTF	Multiple	Bring your own GCP account, 6 levels, practice attacking vulnerable cloud projects on GCP
Bustakube	Kubernetes	Self-hosted, import VMs	Jay Beale	Vulnerable K8S cluster, Download the VMs to build cluster and import into VMWare, run it
Kubernetes Goat	Kubernetes	Self-hosted, multi-cloud, K3S	Madhu Akula	Create and host in your own cloud account (GKE, EKS, AKS) or K3S and attack, has a guided workbook
Kubecon NA 2019 CTF	Kubernetes	Self-hosted in GKE	Multiple	Create GCP account, has a guided workbook with

Name	Technology	Category	Author	Notes
				two attack and defense scenarios plus bonus challenges
Kube Security Lab	Kubernetes	Local, kubernetes in docker	Rory McCune	An awesome local lab to create 14 vulnerable Kubernetes clusters using Docker, Ansible, and Kind. Attack them after building, then destroy. Includes walkthroughs.
Container Security 101	Container	Self-hosted, guided workshop	Jon Zeolla	A guided vulnerability workshop, host in your AWS account, provided CloudFormation
Contained.af	Container	Author-hosted Challenge	Jessie Frazelle	A container escape challenge, break out of it and email the author
TerraGoat	Terraform	Self-hosted multi-cloud (AWS, Azure, GCP)	Multiple, Bridgecrew	Vulnerable by design terraform repository
PurpleCloud	Azure	Research Lab	Jason Ostrom	Using python and terraform, build your own Azure security lab
SimuLand	Azure	Research Lab	Roberto Rodriguez	Using Azure RM templates, create your own Azure security lab
CNAPPgoat	AWS, Azure, GCP	Research Lab	Ermetic Research	Using Pulumi, modularly provision vulnerable-by-design components in AWS, GCP, Azure
CI/CD Goat	CI/CD	CTF, local docker	Palo Alto	Deliberately vulnerable CI/CD environment,

Name	Technology	Category	Author	Notes
				hacking CI/CD pipelines with CTF. Host locally with docker.
Github Actions Goat	CI/CD	Self-hosted Github	StepSecurity	Deliberately vulnerable Github Actions CI/CD environment, hosted in your own Github account. Includes threat scenario descriptions mapped to vulnerabilities.

AWS

CloudFoxable: Create your own vulnerable by design AWS penetration testing playground.

The Big IAM Challenge: CTF challenge to identify and exploit IAM misconfigurations.

CloudSec Tidbits: Three web app security flaws specific to AWS cloud, self-hosted with terraform.

Pentesting.Cloud: 17 free labs. Requires site registration.

AWS CIRT Workshop: Build in your own AWS account and explore 5 common incident response scenarios as seen by the AWS CIRT team.

CloudGoat: Vulnerable by design AWS security labs with guided walkthrough.

Attacking and Defending Serverless Applications: Attack and defend a Lambda that you build in your own AWS account with author provided terraform and scripts. Very educational with workshop style feel.

IAM Vulnerable: Use Terraform to create your own vulnerable by design AWS IAM privilege escalation playground with 31 privilege escalation attack pathways. Very solid documentation.

flaws.cloud: Challenge style with levels and clues.

flaws2.cloud: Challenge style with both Attacker and Defender paths.

CI/CDon't: A vulnerable CI/CD CTF challenge hosted in your aws account with terraform. Includes a walkthrough.

AWSGoat: A damn vulnerable AWS infrastructure with two attack and defense manuals.

Sadcloud: Create vulnerable AWS services without a guide showing vulnerabilities.

DVCA: Deploy a Damn Vulnerable Cloud Application in your own AWS account to practice privilege escalation.

lambhack: Deploy a very vulnerable AWS lambda serverless application in your AWS account.

Azure

BadZure: Powershell Graph SDK script that spins up your own Azure AD (Entra ID) lab with attack paths. Currently no walk through or guide.

Broken Azure: A vulnerable by design Azure infrastructure that you can attack.

PurpleCloud Azure AD Workshop: Guided vulnerability workshop simulating an enterprise Azure customer. It requires PurpleCloud and terraform; username and password is `sec588`

Mandiant Azure Workshop: Vulnerable by design Azure lab with two scenarios that you build in your own Azure tenant.

AzureGoat: Build one module with terraform and walk through the provided attack and defense manuals.

XMGoat: Build 5 scenarios in your Azure tenant and walk through solution docs provided.

CONVEX: Spin up three Capture the Flag environments in your Azure tenant using powershell.

GCP

GCP Goat (Josh Jebaraj): Host in your own GCP account and build with provided scripts. It has a nice guided lab workbook.

GCPGoat (ine-labs): Bring your own GCP account and build one module with terraform. Provides attack and defense manuals.

Thunder CTF: Bring your own GCP account, 6 levels, practice attacking vulnerable cloud projects on GCP.

Kubernetes

Bustakube: Download a vulnerable K8S cluster as VMs that you can import and run locally in VMWare.

Kubernetes Goat: Create and host in your own cloud account (GKE, EKS, AKS) or K3S and attack. Includes a guided workbook.

Kubecon NA 2019 CTF: Awesome CTF that you create in your GCP account. Has a guided workbook with two attack and defense scenarios plus bonus challenges.

Kube Security Lab: An awesome local lab to create 14 vulnerable Kubernetes clusters using Docker, Ansible, and Kind. Attack them after building, then destroy. Inludes walkthroughs.

Container

Container Security 101: A guided vulnerability workshop that is hosted in your AWS account. Author has provided a nice lab you follow on the webpage and you build a VM with CloudFormation and then create a container.

Contained.af: A container escape challenge, break out of it and email the author.

Terraform

TerraGoat: Vulnerable by design terraform repository.

Research Labs

PurpleCloud: Using python and terraform, build your own Azure security lab.

SimuLand: Using Azure RM templates, create your own Azure security lab.

CNAPPgoat: Using Pulumi, modularly provision vulnerable-by-design components in AWS, GCP, Azure. The vulnerabilities are modular scenarios with no guided walkthrough existing yet.

CI/CD

CI/CD Goat: Deliberately vulnerable CI/CD environment, hacking CI/CD pipelines with CTF. Host locally with docker.

Github Actions Goat: Deliberately vulnerable Github Actions CI/CD environment, hosted in your own Github account. Includes threat scenario descriptions mapped to vulnerabilities.