

# INFOSEC Boot Camps

CERTIFICATION TRAINING 

Get live, expert instruction from anywhere.



## Cloud Penetration Testing Boot Camp

Learn how to conduct penetration tests on cloud services and applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend cloud infrastructure components with a combination of hands-on labs and expert instruction.

### Course description

Infosec's Cloud Penetration Testing Boot Camp is a practical, hands-on training focused on teaching you the skills, tools and techniques required for conducting comprehensive security tests of cloud servers and applications.

You will learn the secrets of cloud penetration testing in an immersive environment, including exploiting and defending AWS and Azure services, building your pentesting toolbox in the cloud, and diving deep into security features and vulnerabilities of cloud infrastructure. You will also learn how to deal with the unique challenges presented by cloud pentesting, such as multi-tenant environments and pivoting. The boot camp also prepares you to earn the Certified Cloud Penetration Tester (CCPT) certification.

### Who should attend

- » Penetration testers
- » Cloud and system administrators
- » Application developers
- » DevSecOps engineers
- » Security consultants
- » Security analysts

### Boot camp at a glance



#### What you'll learn

- ✓ Cloud pentesting process and requirements
- ✓ Attacking AWS and Azure
- ✓ Attacking containerized and serverless applications



#### Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite



#### Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp
- ✓ 90-day extended access to all boot camp materials

## The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.



### Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.



### Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.



### Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.



### 700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

## What's included

- » Five days of expert, live CCPT training
- » Exam Pass Guarantee
- » Exam voucher
- » Unlimited practice exam attempts
- » 100% Satisfaction Guarantee
- » Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- » 90-day extended access to all boot camp video replays and materials
- » Pre-study learning path
- » Hands-on cyber ranges and labs
- » Knowledge Transfer Guarantee

### Prerequisites

Familiarity with cloud and penetration testing concepts and at least one year in an information security role, or equivalent experience, is recommended.

## Cloud Pentesting exam overview

This boot camp provides hands-on cloud infrastructure penetration testing experience and prepares you to earn the CCPT certification. You will leave with skills and in-depth knowledge of the five CCPT domains:

- » Common vulnerabilities in cloud environments
- » Security features of popular cloud platforms
- » Cloud pentesting process and requirements
- » Cloud pentesting tools
- » Reporting cloud pentest findings and providing recommendations

## Hands-on labs

Get hands-on penetration testing experience in our custom-built cloud-based lab environment. You will practice using OSINT tools and techniques to gather information about target services and public buckets, abusing metadata endpoints, stealing credentials from cloud instances, attacking storage and database service misconfigurations, and more. You will also learn remediation steps so that the cloud service provider can properly close the security hole.

## Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

## Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest CCPT exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

## Skill up and get certified, guaranteed



### Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.



### 100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.



### Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

# What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

**Michelle Jemmott**

Pentagon

---

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

**John Peck**

EPA

---

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

**Sylvia Swinson**

Texeltek

---

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

**Erik Heiss**

United States Air Force

---

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

**Robert Caldwell**

Salient Federal Solutions

**INFOSEC Boot Camps**

CERTIFICATION TRAINING 

Enroll today: 866.471.0059 | [infosecinstitute.com](https://infosecinstitute.com)

# Cloud Penetration Testing details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5
Morning session	Introduction Cloud pentesting process and requirements	Attacking AWS	Attacking Azure	Attacking containerized and serverless applications	Reporting
Afternoon session	Reconnaissance in the cloud	Attacking AWS	Attacking Azure	Attacking containerized and serverless applications	Take CCPT exam
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study		

*Schedule may vary from class to class*

## Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

## During your boot camp

### Cloud pentesting process and requirements

- » The need for cloud pentesting
- » Cloud architecture fundamentals
- » Cloud security responsibilities (within service models)
- » Unique challenges for cloud pentesting
- » Multi-tenancy considerations (data privacy, legal requirements, rules of engagement)
- » Cloud attack surface
- » Virtualization concepts
- » Pentesting methodologies
- » Cloud pentesting process

- » Pentesting tools: traditional and cloud-specific
- » Setting up a cloud pentesting environment

### Reconnaissance in the cloud

- » OSINT techniques
- » Azure and AWS IP ranges
- » Tools for obtaining IP and host information (Shodan, Censys, Google dorks)
- » Enumerating access with Nimbostratus, ScoutSuite and Prowler
- » Finding exposed buckets
- » Bucket enumeration with Slurp
- » Service discovery

### Attacking AWS

- » AWS security features
- » AWS Console overview
- » Working with AWS CLI
- » Exploiting remote access protocols (SSH , RDP)
- » Exploiting application security misconfigurations

- » Abusing EC2 metadata
- » Stealing IAM credentials
- » EC2 IMDSv2
- » Attacking lambda endpoints
- » Assessments with AWS Inspector
- » Attacking misconfigured S3 buckets
- » Discovering and stealing EBS snapshots
- » Recovering data from EBS snapshots
- » Exploiting AWS RDS misconfigurations
- » RDS data pilfering with AWS CLI and Amazon API
- » Persistence

## Attacking Azure

- » Understanding Azure Services
- » Mapping Azure Services to AWS Services
- » Attacking Azure Virtual Machines
- » Attacking Azure Blob Storage misconfigurations
- » Extracting data from disk snapshots
- » Subdomain takeover via Azure App Services
- » Gaining shell access with Azure run command
- » Finding and examining Azure SQL Database servers

## Attacking containerized and serverless applications

- » Understanding containers
- » Working with Docker
- » Container breakout
- » Exploiting misconfigured containers
- » Trojanized Docker images
- » Understanding Kubernetes
- » Attacking deployed applications
- » Attacking Kubernetes clusters

- » Understanding AWS Lambda
- » Attacking serverless applications

## Reporting

- » Cloud security frameworks and best practices
- » Collecting and reporting evidence in cloud accounts, aliases, metadata, keys and AMIs
- » Developing and communicating follow-up items

## After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

## About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at [infosecinstitute.com](https://infosecinstitute.com).