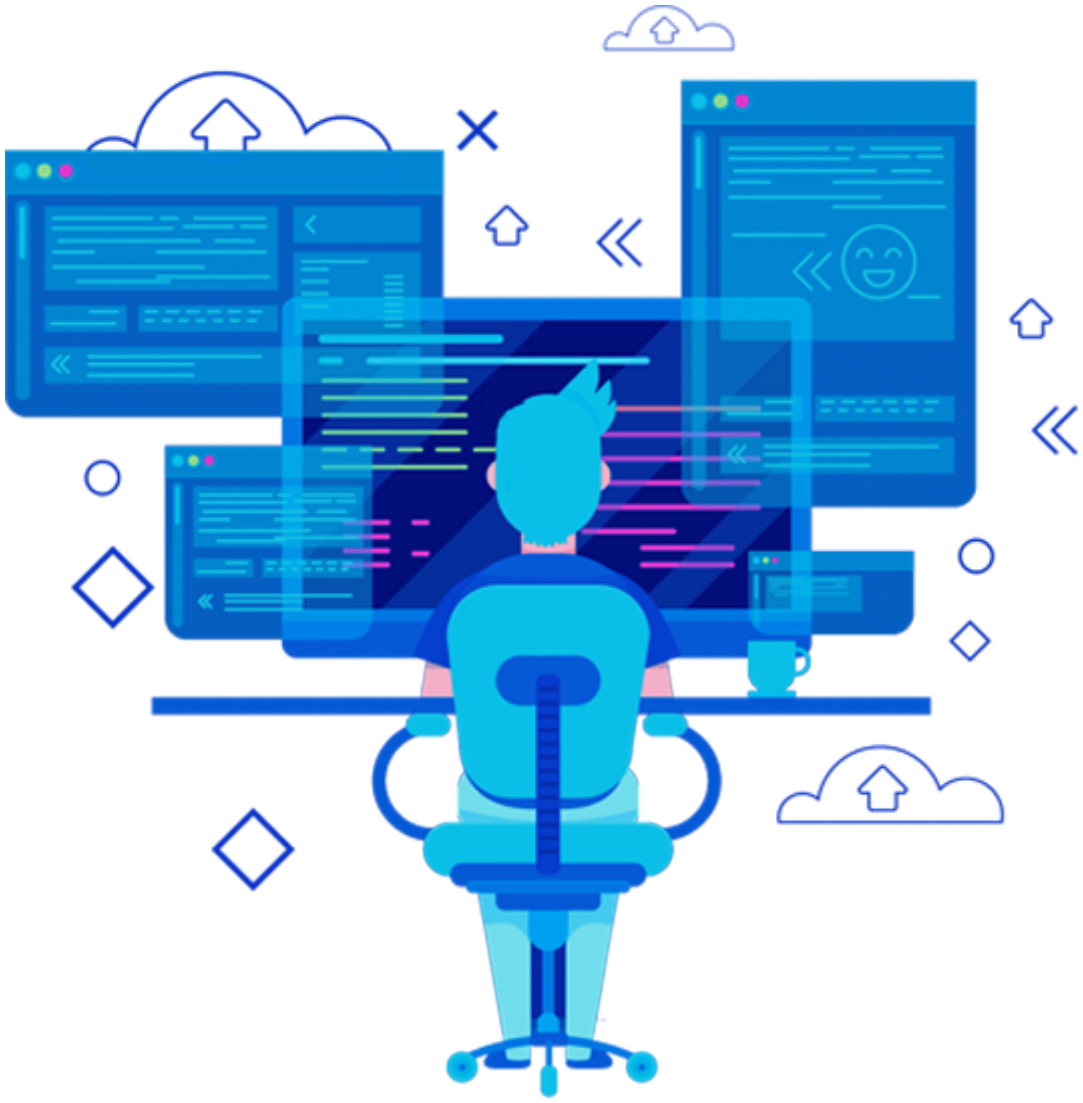
BREACHLOCK™

Dummies guide to AWS Penetration Testing

REQUEST A QUOTE



04 FEB, 2019

Dummies guide to AWS Penetration Testing

Last year, there have been many AWS breaches exposing various types of vulnerabilities including leaking S3 buckets, compromised AWS environments and misconfigurations. Now more and more organizations are moving to the cloud and adapting modern technologies into their development operation. Organizations are trying to improve their security and decrease the chance of a cybersecurity breach so this post will help them understand AWS security and penetration testing.

Why pen testing AWS is important for an organization

The following scenarios give an overview of why penetration testing in and on AWS environments is essential for an organization to maintain security and build the trust of the users:

1. Organization misunderstands the 'shared responsibility model' which leads them to underestimate the risk that they are responsible for.
2. Not doing proper and time-to-time security configuration assessment of the AWS console after setting up their web application.
3. Not implementing multi-factor authentication.

AWS security implementation in the cloud should be part of a complete security plan. AWS also understands the requirement of pen testing the application, instance and an operating system so that's why AWS established a program to permit penetration testing.

Traditional pen testing versus AWS pen testing

Traditional pen testing and AWS pen testing is very different because of the AWS ownership of the infrastructure. Pen testing on the AWS infrastructure or hosted application without permission is a violation of the AWS acceptable use policy. When pen testing AWS environments

there are various perspectives we should consider while security assessment like web application, external infrastructure and some specific to the cloud environment.

Let's see how cloud pen testing is different from traditional pen testing. Below are the different types of testing we can do according to various scenarios.

1. Testing on the Cloud: testing the web application that is hosted merely on the cloud environment which is publicly accessible.
2. Testing in the Cloud: in this scenario testing the environment that is hosted on the cloud like Amazon Virtual Private Cloud (VPC) or equivalent and not directly accessible from outside. Testing web application running on the private cloud and the supporting infrastructure setup including different AWS services in the structure.
3. Testing the Cloud Console: this scenario is very different from the traditional pentesting, examining the whole cloud console configurations like user accounts, permissions, e.g., IAM policies, security groups which is already configured in the AWS console.

Some vulnerabilities to test for in AWS

Below are vulnerabilities we see while AWS penetration testing:

1. S3 bucket configuration and S3 bucket permission defects
2. Compromising AWS IAM keys and permission
3. Establishing private-cloud access through Lambda backdoor functions
4. Cloudfront Misconfiguration Bypasses
5. An IAM privilege escalation pathfinder and abuser
6. Cover tracks by obfuscating Cloudtrail logs

Performing AWS pen test

Security testing for User-Operated Services is authorized by AWS, which is created and configured by the user. Pen tests involving Vendor Operated Services, which are owned and offered by the third-party vendor, are prohibited.

EC2 and S3 bucket is an AWS service which is usually pen tested.

Performing a pen test inside the cloud needs adequate planning and skilled information. General steps and preparation that ought to be taken before the pen test begins to include:

1. The most crucial initial step is defining the scope, as well as the AWS environment and target systems
2. Determine the type of pen test you would like conducted (e.g., black box, white box, gray box)
3. Setting a timeline for the technical assessment to occur
4. Obtaining approval to perform the pen test from AWS
    - Sign in to your AWS account using root credentials
    - Fill out the Vulnerability / Penetration Testing Request Form
    - Inform AWS about the dates that testing will take place
    - Inform AWS about the IP Address range the scan or penetration testing will come from
    - Inform AWS about the scope you will test like IP Address range

---

Category

AWS Penetration Testing	4
Cloud Penetration Testing	5
DAST-Dynamic Application Security Testing	9
DevSecOps	6
GDPR	1
HIPAA	3
Infographics	3
network penetration test	1
OSINT Penetration Testing	1
PCI DSS Compliance	2
Penetration Testing as a Service	10
Uncategorized	2

Recent Post

Importance of Black Box Penetration Testing in Application Security

16 JUL, 2019

Benefits of Automated Penetration Testing

13 JUL, 2019

Vulnerability Scanning and Penetration Testing For HIPAA [Infographic]

12 JUL, 2019

Security Testing

Penetration Testing Service

Continuously find and fix your security gaps.

Application Penetration Testing

Conduct manual penetration tests on applications to achieve compliance

DAST

Dynamic application security testing

IOT Penetration Testing

Check Our IoT Penetration Testing expertise

Social Engineering

Our unique OSINT and Phishing Exposure Assessment

Web Application Penetration Testing

OWAS compliant Web Penetration Testing Services

DevSecOps

Find vulnerabilities fast and early, empower your DevOps

Network Penetration Testing

External and Internal Penetration Testing

Cloud Penetration Testing

Benefit from our Cloud Penetration Testing expertise

Vulnerability Assessment

Benefit from our Vulnerability Assessment expertise

Compliance

Vendor Assessments

Respond to Vendor Security Assessments with confidence

PCI DSS

PCI DSS Penetration Testing and ASV Scans

HIPAA

HIPAA Risk Assessment and Penetration Testing

GDPR

GDPR Compliance with BreachLock™ Security Testing

Follow us

Tell us about your requirements. We respond the same business day.

Fill out the form below to let us know your requirements. We will contact you to determine if BreachLock™ is right for your business or organization.

Once you do, we'll reach out to:

- Ask you a few questions
- Understand your scope and timeline
- Determine if there's a good fit
- Provide a competitive quote within 24 hours

Name

Phone Number

Email

Security needs, scoping details, etc

GET A QUOTE

Menu

How It Works

Cloud Platform

FAQ

Company

Blog

Contact

Privacy Policy

Terms Of Use

Contact

BreachLock Inc.
276 5th Avenue
Suite 704 – 3031
New York NY 10001

E: sales@breachlock.com

P: +1 917-779-0009

F: +1 302 516-7152