CYBERSRC® CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

# AWS CLOUD SECURITY TESTING SERVICES

# AWS CLOUD SECURITY TESTING SERVICES

## OVERVIEW

Most of the web applications are moving to cloud technology. While this enhances the application functionality, it also introduces security issues. Since everything is virtual in case of a cloud hosting, it is difficult to gain fine grain control of the "data at rest" and "data in transit".

Cloud computing technology offers three basic models of implementation. Infrastructure as a service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS). Securing cloud environments is a sweeping proposition that touches on the topics of virtualization security, access control, data protection and a host of other areas.

# MAJOR VULNERABILITIES FOUND IN CLOUD ENVIRONMENT INCLUDE

## MULTI TENANCY ATTACKS

Most SaaS-based archiving vendors, including email archiving vendors, have a multi-tenancy architecture and store archived data in public clouds. That means your data is stored on servers in public clouds owned by very large cloud technology platform providers that rent space to tens or even hundreds of other cloud SaaS vendors.

## PRIVILEGE ESCALATION

With privilege escalation, the hacker gains illegal access to the system and engages in activities that capitalize on lax employee security procedures, programming errors, and weaknesses of the system. These activities enable the intruder to achieve a higher level of access to the main platform, its security resources, other tenant instances, and each tenant's data.

## SQL INJECTION

A hacker uses this type of attack to remotely inject a file onto a web application server. This can result in the execution of malicious scripts or code within the application, as well as data theft or manipulation.

## REQUEST FORGERY

A successful SSRF attack means that the attacker would be able to query the instance and retrieve AWS EC2 specific information and in the worst case, temporary credentials attached to the AWS EC2.

# CHALLENGES IN AWS PENTESTING

1. **Flawed understanding of the 'shared responsibility model' leading organizations to underestimate the risk that they are responsible for.**

2. **Failures across fundamental AWS security checks including 'open-wide security groups' and excessive permissions.**

3. **Addressing zero-day vulnerabilities. Identification and remediation of the zero-day vulnerabilities is an essential part of maintaining good security posture in the cloud.**

4. **Failures in multi-factor authentication requirements, implementation or operation. The latter is particularly vexing when you consider how effective social engineering attacks, credential sharing and privilege escalation are.**

5. **Extending compliance requirements, reporting, and visibility to the cloud. To maintain compliance efforts that impact the data center (specifically Fed RAMP, HIPAA, PCI-DSS, etc.), organizations must take steps to highlight, resolve, and remediate any compliance gaps that effect their applications, infrastructure, and operating systems.**

# OUR DETAILED APPROACH

**Following are the Security Assessment that are performed on an AWS environment**

## TESTING APPLICATIONS HOSTED ON CLOUD

Consider your web application hosted on a VPS or dedicated server and later moved to the cloud platform in which only your developed web application is considered in the scope.

## TESTING INTERNAL APPLICATIONS HOSTED ON CLOUD

This type of cloud assessment is performed where in the cloud system cannot be accessed externally and is private which has firewall to prevent direct access and can only be accessed by a bastion host.

## CONFIGURATION REVIEW OF CLOUD CONSOLE

Testing the cloud console for any misconfigurations such as the created user accounts and their permissions, implemented ACL, etc. This is more of a configuration review verifying standards policies have been implemented while creating accounts. We can identify different techniques to perform privilege escalation.

## TESTING THE CLOUD NETWORK INFRASTRUCTURE

Testing the cloud infrastructure for any unused open ports, vulnerable services running and unpatched softwares.

## CLOUD INSTANCE HARDENING

This adds an extra layer of security to your instance/ server and protects it from outside attacks. It checks the policies used, configurations of the instance.

## SOME OF THE TOOLS USED

- NMAP
- PACU
- AWS Inspector
- AWS CLI
- ScoutSuite

# KEY AREAS COVERED IN AWS CLOUD PENTESTING

1. **Testing S3 bucket configuration and permissions flaws.**
2. **Targeting and compromising AWS IAM keys.**
3. **CloudFront/WAF Misconfiguration Bypasses.**
4. **Establishing private-cloud access through Lambda backdoor functions.**
5. **Cover tracks by obfuscating CloudTrail logs.**

# CASE STUDIES

## Background

- Client is one of the leading E sign service provider
- The client has been in the industry for over 10 years with a global presence including India, California and New Jersey
- Cloud VAPT and configuration helps organization recognize configurations error and loopholes that lead to cyber attack

## Objectives

- Assessment of the AWS Infrastructure and configuration review
- Identification of the malicious file/ backdoor/ Service in Network of AWS infrastructure and safeguard the remaining data and systems
- Identification of the improper configurations of AWS console
- Expert recommendations and guidance to cover up gaps and improve information security posture

## Challenges

- The client did not have any expertise for cloud VAPT and configuration review
- The client lacked required knowledge of tools used for VAPT of cloud

## Our Role

- Cloud VAPT for the companies AWS infrastructure using AWS exploitation tools like PACU
- Cloud configuration review of the company's AWS console using automated scanners like ScoutSuite.
- Retesting of cloud infrastructure
- VAPT reporting and legal advisory

## Result/ Benefits

- Organization gain comprehensive knowledge on the threat action in their cloud environment
- Detailed report of VAPT and recommendation with preventive measure
- Detailed report of AWS console configuration review
- Consultancy on action items required to cover up identified gaps

### Industry Sector

**E-Sign Service Provider**

### Service Utilized

**Cloud VAPT**

**Configuration Review**

### Business Areas Challenges

**IT & Technology (cloud)**

## HOW CyberSRC® HELP?

We primarily follow the Open Web Application Security Project (OWASP) guidelines as a benchmark. However, over time we have developed our own Hybrid Methodology that brings together the best of OWASP, OSSTM, WASC and NIST standards. This hybrid methodology involves a set of comprehensive checks which ensure that no vulnerabilities are missed during testing.

The process involves an active analysis of the application for any weaknesses, technical flaws, or vulnerabilities. Any security issues that are found are presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.

CyberSRC possesses years of security experience ranging from corporate networks to recent customers requiring cloud computing security. Unlike most other security consultancy offerings, in case of cloud security the approach is purely from design perspective. We deep dive into the cloud architecture, and identify various attack vectors which range from network layer of cloud design, to the cloud aware applications running on virtual data centres or virtual development centres. Cloud security also includes that of web authentication portals which call the cloud service providers API calls.

## ABOUT US

CyberSRC® forays into domains of Cyber Security, Data Privacy, Assurance and Governance. Our aim is to assist enterprises, MSMEs, SMEs & others enhance their capabilities for cybersecurity defence, minimise enterprise security and assurance risks, manage security operations and achieve regulatory compliance. Our team consists of several consultants and advisors. We have collaborated with multi-partners in order to provide support for end-to-end security solutions and implementation support.

## WHY CYBERSRC®?

We are team of qualified professionals with rich experience of multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others. Our consultants are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (Coe) and, we have end-to-end capability for Program Build – Operations – Transformation. We have the ability to jump start and execute projects in Managed Services mode globally and flexible delivery models. Our Vision is to be one of the World's most trusted advisory & solution provider for Cyber Security, Data Protection an Assurance practices.

## WHAT WE DO

### SECURITY ASSESSMENT SERVICES

**1. Vulnerability and Penetration Testing Services**

- Web Application VA/PT
- Mobile Application VA/PT
- Network Security VA/PT
- Database Security Assessment
- Cloud Security Assessment
- Wireless/WIFI Devices Assessment
- API & Web Services

**2. Source Code Review**

**3. Configuration Review and Hardening Testing**

**4. Firewall/ Network Devices Security Review**

### SPECIALISED CYBER SECURITY SERVICES

**1. External Threat Intelligence**

- Phishing Domain Detection
- Rogue Applications Detection
- Source Code Leaks
- Social Media Abuse
- Brand Abuse
- Dark Web Monitoring
- Take Down support

**2. Phishing Campaigns/ Stimulation**

- Phishing
- Smishing
- Vishing

**3. Incident response & Malware Analysis**

**4. Forensics Analysis**

**5. Root Cause Analysis**

**6. Red Teaming Exercise**

**7. Honeypot as Service**

- Web Attack Mitigation
- Network Attack Mitigation
- Shadow Surveillance

## CONSULTING, COMPLIANCE AND & AUDIT SERVICES

### 1. ISO Compliance

- ISO 27001 ISMS
- ISO 9001 QMS
- ISO 27701 PIMS

### 2. Information System Assurance & Audit

- **RBI**
  - Payment & Settlement Systems (PSS)
  - NBFC
  - Co-Operative Banks
  - Prepaid Payment Instruments PPI
  - CISA
  - P2P Lending
- **IRDA ISNP**
- **SEBI**
- **AADHAAR**
  - UIDAI AADHAAR
  - ESIGN ASP
- **OTHER**
  - GST SUVIDHA PROVIDER
  - NPCI

### 3. Regulatory Compliance

- PCI DSS
- SOX
- SOC 1, SOC 2 & SOC 3

### 4. Privacy Compliance

- General Data Protection
- Regulation (GDPR)
- ISO 27701 PIMS
- California Consumer Privacy Act (CCPA)
- Brazilian General Data Protection Law (LGPD)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- Singapore Personal Data Protection Act (PDPA)
- Health Insurance Portability and Accountability Act (HIPAA)

### 5. Risk Management

- Virtual Chief Information Security Officer (V-CISO)
- Third Party Risk Management
- IT Risk Management

# CONTACT US

CYBERSRC®
CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

☎ **+91 9718933141, 0120-4160448**

✉ **info@cybersrcc.co**

🌐 **www.cybersrcc.com**

📍 **Head Office:** Unit 605, 6th Floor, World Trade Tower, Sector 16, Noida (UP)- 201301
**Other Office:**
**London (UK):** Kemp House 152-160 City Road, London, UK (EC1V 2NX)