AWS PENETRATION TESTING

Stay ahead of Vulnerabilities in Cloud Configuration

Penetration testing (or pentesting, for short) on the AWS cloud is unique, bringing its own set of security factors. While some vulnerabilities are mitigated through Amazon security measures, the complexity of these services leaves many companies exposed.

Rhino Security Labs' AWS penetration testing services are aimed at specifically these needs, identifying the configuration and implementation flaws which often go unchecked.

TRADITIONAL INFRASTRUCTURE VS AWS PENTESTING

Traditional security infrastructure and AWS clouds differ in various ways. From setup and configuration to identity and user permissions, the technology stacks could not be more distinct.

The most noticeable difference is the ownership of the systems, meaning Amazon requires formal permission for penetration testing, carried out on approved dates. The purpose of this policy is since the testing is affecting Amazon-owned infrastructure, the attacks of 'ethical hacking' would violate acceptable use policies (and may provoke incident response actions by the AWS team).

By making these testing windows clear, we ensure both a thorough and safe security assessment.

Also distinct is the architecture of Amazon Web Services and its set of powerful API's. Deeply integrated into the AWS ecosystem, our security engineers test for a range of AWS-specific tests.

AWS Assessment Techniques

- *Probe IAM Permissions for exploitable misconfigurations*
- *Enumerate EC2 'User Data' fo credentials*
- *Abuse EC2 Systems Manager for remote access to instances*
- *Escalate AWS privileges through IAM misconfigurations*
- *Backdoor Lambda functions for environment persistence*
- *Evade CloudTrail / GuardDuty through various techniques*

AWS ATTACK VECTORS - COMMON SERVICES

IAM

- Analyze permissions for privilege escalation paths (through services like Lambda, EC2, etc.)
- Checking for misconfigured roles, attempting to access them
- Establish persistence through backdoor users/roles

EC2/VPC

- Enumerating Instances, Security Groups and AMIs to stage EC2 attacks
- Abusing Simple Systems Manager for remote access to instances
- Analyzing EC2 User Data for secrets or system credentials
- Identifying routes between VPCs for lateral movement and escalation

S3

- Check for misconfigured buckets (unauthenticated)
- Once authenticated, check access to S3 buckets for sensitive files and data
- Leverage existing S3 buckets to exfil data or stage further attacks

Lambda

- Analyze code and configuration for sensitive information disclosure
- Privilege Escalation through Lambda IAM Roles and SDK’s
- Data exfiltration through modification of data-processing functions
- Create new Lambda functions for alerting attackers to blue team activities (such as removal of previous AWS backdoors)

RDS

- Modifying/evading Security Group rules to access RDS databases
- Bypassing RDS authentication through copy of backups and RDS password change
- Exfiltration of RDS data through cross-account C2 channel

CloudTrail / GuardDuty

- Various methods of trying to evade detection, cover tracks, and generally stay under the radar
- Downloading logs to get a better idea of common activity in the environment and creating a lay of the land

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.