BISHOPFOX

METHODOLOGY

CLOUD PENETRATION TESTING METHODOLOGY

APRIL 2021

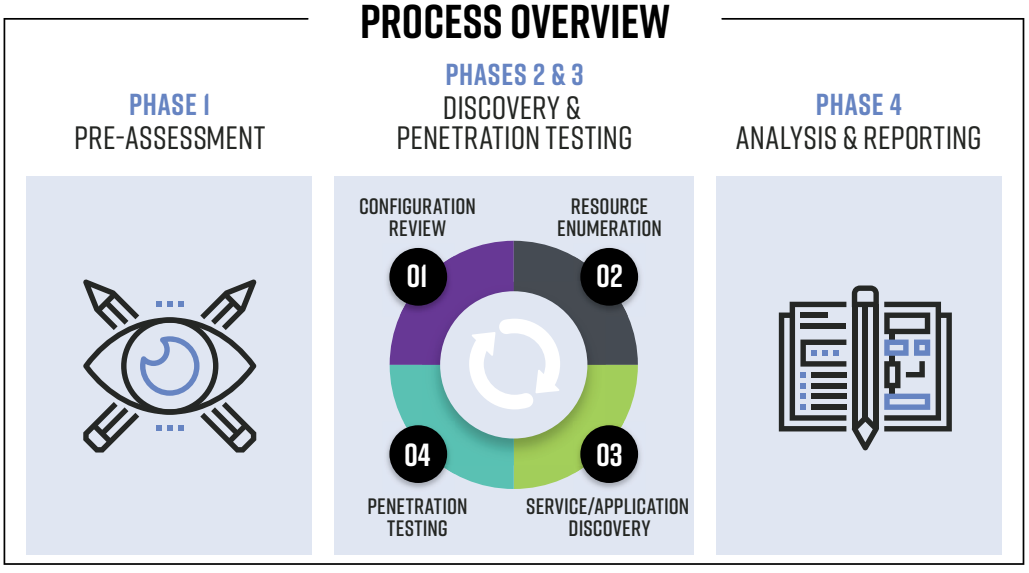
BISHOPFOX

CLOUD PENETRATION TESTING METHODOLOGY

Bishop Fox's cloud penetration testing methodology combines configuration review with penetration testing to identify vulnerabilities in cloud environments, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. These assessments are meant to simulate the threat of someone with access to the client's cloud environment, whether that is a compromised user, a compromised application, or a similar use case.

The assessments are time boxed and focus on demonstrating the real-world impact of misconfigurations. To accomplish this, the team attempts to achieve specific engagement objectives, such as obtaining privileged cloud credentials, gaining control over key services, or acquiring sensitive business data.

For example, the team often demonstrates how role-based access control misconfigurations can provide users with unintended administrative access to cloud resources, or how misconfigured cloud storage buckets can leak sensitive data and secrets that can then be exploited to gain further cloud access. Additionally, the team frequently finds mistakes made by individual operators or teams that impact the larger environment. For instance, a team may deploy an internal application with default credentials or known vulnerabilities. If that application is compromised, the attacker can often gain access to privileged credentials that can then be used to compromise additional cloud services.



PHASE I: PRE-ASSESSMENT

The following assessment requirements must be met to ensure the timely and successful completion of the project.

PRE-ASSESSMENT REQUIREMENTS	
ACCOUNT FOR CONFIGURATION REVIEW	To conduct a configuration review, the assessment team requires cloud account credentials with the following access: • API access to the cloud environment • Graphical user interface (GUI) or console access to the cloud environment • Security audit permissions Bishop Fox's engagement manager will provide specific details on how to set up an account with the correct permissions.
ACCOUNTS FOR PENETRATION TESTING	To conduct penetration testing, the assessment team requires account credentials that mirror a typical user account or a compromised application/microservice. The access should be based on the penetration test's goals or objectives. For example, access may mimic a software developer's account.
ENVIRONMENT ACCESS	The assessment team requires network access to the cloud API and all in-scope services. Access is typically provisioned through one of the following methods: • Client laptop with VPN access • Jumpbox • Direct internet access
OBJECTIVES	Prior to beginning fieldwork, the assessment team works with the client's team to determine primary engagement goals. These goals often include the following: • Compromising trophy targets, such as privileged credentials or customer data • Pivoting to restricted portions of the cloud environment • Exfiltrating data to determine the client's detection capabilities • Acquiring selected levels of access and privileges as a simulated attacker

SCOPE	The assessment team requires a list of in-scope cloud environments such as the following: • AWS accounts • GCP projects • Azure subscriptions
DUE CARE	Throughout the assessment, Bishop Fox attempts to minimize disruptions to network availability, particularly when performing any automated scanning, manual validation, or penetration testing. Prior to testing, the assessment team will discuss risks to environmental stability with the client and identify the escalation path in the event that any disruptions are observed.
AUTHORITY	If any portion of the product or related resources is hosted on a third-party system, a consent to test must be obtained prior to the start of fieldwork.

PHASE 2: INFORMATION GATHERING AND AUTOMATED TESTING

In this phase, the assessment team begins fieldwork by using automated tools and manual techniques to gather and analyze details about the cloud deployment.

DISCOVERY AND ENUMERATION

CONFIGURATION ENUMERATION

The assessment team uses open source and proprietary tools to gather the following configuration information:

- Service configuration details
- Identity and access management (IAM) configuration data
- Resource-level access controls, such as data buckets
- Credentials and other confidential data exposures

The team then uses this information to conduct the following activities:

- Identify potential security misconfigurations
- Enumerate cloud privilege escalation paths
- Map the environment's attack surface

NETWORK DISCOVERY

From a position within the cloud network, the assessment team performs the following activities to identify live hosts on the target network:

- **Cloud Resource Enumeration** — programmatically query the cloud API to identify exposed service endpoints
- **Common TCP Port Scanning** — conduct port scanning to identify specific TCP ports, targeting the subnets associated with the previously identified hostnames and domains

SERVICE AND APPLICATION ENUMERATION

Once live hosts on the target network are identified, the team attempts to enumerate running network services by using the following methods:

- **Detailed Port Scans** — conduct a TCP/UDP port scan against known ports and live hosts
- **Service and Application Enumeration** — attempt to fingerprint and examine running network services and applications

PHASE 3: PENETRATION TESTING

After the configuration review is complete, the assessment team performs the following activities to identify and exploit vulnerabilities within the cloud deployment.

CLOUD PENETRATION TESTING

CLOUD PENETRATION TESTING	The assessment team attempts to compromise in-scope systems and credentials, perform lateral movement, and escalate privileges within the target environment by conducting the following activities: • Traversing cloud privilege escalation paths • Hunting for exposed secrets and credentials • Testing the access of identified credentials • Identifying overly permissive network access controls • Exploiting misconfigured cloud services • Exploiting vulnerable network services and applications • Identifying abandoned subdomains

PHASE 4: ANALYSIS AND REPORTING

Bishop Fox reports contain an executive-level summary of the engagement, which includes the assessment's goals, a synthesis of the highest-impact findings, and high-level recommendations. Within each finding, a vulnerability definition is given along with detailed reproduction steps and tailored recommendations.

For each finding, the assessment team builds a holistic view of the business risk it represents by performing the following activities.

TECHNICAL ANALYSIS ACTIVITIES	
LIKELIHOOD DETERMINATION	**For each vulnerability, the assessment team determines the likelihood that it will be exploited based on the following factors:** • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of controls
IMPACT ANALYSIS	For each vulnerability, the assessment team analyzes and determines the impact of successful exploitation as it affects the organization and its customers in the areas of confidentiality, integrity, and availability.
SEVERITY DETERMINATION	Bishop Fox determines severity ratings using in-house expertise and industry-standard rating methodologies such as the Open Web Application Security Project (OWASP) and the Common Vulnerability Scoring System (CVSS) to evaluate the likelihood and impact of exploitation. The team weighs those factors to classify the overall severity as critical, high, medium, or low. The severity of each finding is determined independently of the severity of other findings.

PHASE 5: REMEDIATION REVIEW (OPTIONAL)

Optionally, the assessment team re-performs scanning and testing of the identified vulnerabilities after the client indicates that the vulnerabilities have been addressed.