BISHOPFOX

METHODOLOGY

Cloud Penetration Testing

Bishop Fox's Cloud Penetration Testing goes beyond cloud configuration review to reveal security issues across the entire cloud ecosystem. Applying open-source and proprietary discovery techniques, Bishop Fox's cloud penetration testing methodology is purpose-built to systematically uncover a comprehensive set of cloud based weaknesses and vulnerabilities such as unintended entry points, IAM privilege escalation paths, insecure credential storage, and vulnerable applications and services. The methodology outlined in this document provides a detailed look at the step-by-step process and delineation of responsibilities that are critical to accomplishing predetermined objectives.

Summary of Engagement

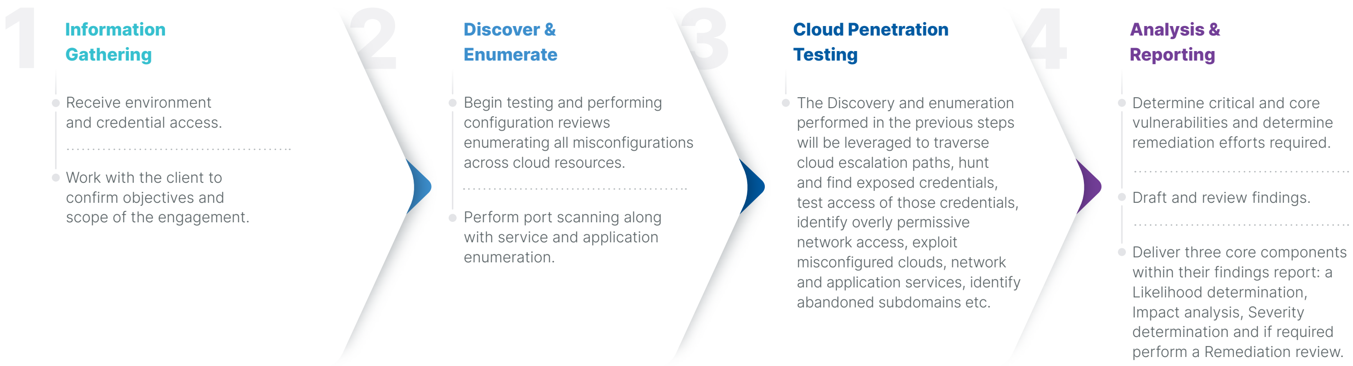
Before the engagement can begin, Bishop Fox's consultants require credentialed access to the cloud environment. In addition, Bishop Fox consultants meet with all invested stakeholders to understand and confirm the objectives and scope of the engagement.

Once access has been obtained and objectives are determined, Bishop Fox consultants perform full discovery and enumeration of all in-scope cloud exposures. From these findings, we leverage our in-depth configuration review to simulate the threat of someone with access to the 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 in your cloud environments.

The team attempts to achieve specific engagement objectives, set out by the initial agreements with stakeholders during scoping and objective setting. These objectives could be situations like 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.

Once weaknesses have been discovered, consultants document initial discovery and enumeration findings including successful exploitation. Remediation steps applicable to each threat are outlined in detail and reviewed with stakeholders for feedback and clarification. Once feedback has been applied, reports are finalized and communicated to all parties. It is important to note that the primary outcome of this engagement is ensuring your security teams understand all cloud exposures and prioritization of remediation against the likelihood of attack, business impact, and required resource allocation.

High-level Process



1 **Information Gathering**

- Receive environment and credential access.
- Work with the client to confirm objectives and scope of the engagement.

2 **Discover & Enumerate**

- Begin testing and performing configuration reviews enumerating all misconfigurations across cloud resources.
- Perform port scanning along with service and application enumeration.

3 **Cloud Penetration Testing**

- The Discovery and enumeration performed in the previous steps will be leveraged to traverse cloud escalation paths, hunt and find exposed credentials, test access of those credentials, identify overly permissive network access, exploit misconfigured clouds, network and application services, identify abandoned subdomains etc.

4 **Analysis & Reporting**

- Determine critical and core vulnerabilities and determine remediation efforts required.
- Draft and review findings.
- Deliver three core components within their findings report: a Likelihood determination, Impact analysis, Severity determination and if required perform a Remediation review.

Methodology Details

Phase 1: 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 if 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.

	Bishop Fox	Client
Identify and Meet with Security Team and Business Stakeholders	✓	✓
Provision Accounts for Configuration Review		✓
Provision Accounts for Penetration Testing		✓
Provision Credentials and Environment Access		✓
Set Objectives and Scope	✓	✓

Phase 2: Information Gathering & 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.

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

	Bishop Fox	Client
Gather Configuration Information	✓	
Gather Configuration Data on Identity and Access Management (IAM)	✓	
Discover Resource-level Access Controls (i.e. Data Buckets)	✓	
Expose Credentials and Other Confidential Data	✓	
Identify Potential Security Misconfigurations	✓	
Enumerate Cloud Privilege Escalation Paths	✓	
Attack Surface Mapping	✓	
Enumerate Cloud Resources Identifying Exposed Endpoints	✓	
TCP Port Scanning Identifying Specific Ports for Targeting	✓	
Conduct TCP/UDP Scans Against Known Ports and Live Hosts	✓	
Enumerate Service and Applications to Fingerprint 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	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

	Bishop Fox	Client
Traverse Cloud Privilege Escalation Paths	✓	
Hunt Exposed Secrets and Credentials	✓	
Test Identified Credential Access	✓	
Identify Overly Permissive Network Access Controls	✓	
Exploit Misconfigured Cloud Services	✓	
Exploit Vulnerable Network Services and Applications	✓	
Identify Abandoned Subdomains	✓	

Phase 4: Analysis & Reporting

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

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.

	Bishop Fox	Client
Likelihood Determination	✓	
Impact Analysis	✓	✓
Severity Determination	✓	

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.

Appendix

Delineation of Responsibilities	Bishop Fox	Client
Phase 1: Pre-assessment Requirements		
Identify and Meet with Security Team and Business Stakeholders	✓	✓
Provision Accounts for Configuration Review		✓
Provision Accounts for Penetration Testing		✓
Provision Credentials and Environment Access		✓
Set Objectives and Scope	✓	✓
Phase 2: Information Gathering & Automated Testing		
Gather Configuration Information	✓	
Gather Configuration Data on Identity and Access Management (IAM)	✓	
Discover Resource-level Access Controls (ie Data Buckets)	✓	
Expose Credentials and Other Confidential Data	✓	
Identify Potential Security Misconfigurations	✓	
Enumerate Cloud Privilege Escalation Paths	✓	
Attack Surface Mapping	✓	
Enumerate Cloud Resources Identifying Exposed Endpoints	✓	
TCP Port Scanning Identifying Specific Ports for Targeting	✓	
Conduct TCP/UDP Scans Against Known Ports and Live Hosts	✓	
Enumerate Service and Applications to Fingerprint Running Network Services and Applications	✓	
Phase 3: Cloud Penetration Testing		
Traverse Cloud Privilege Escalation Paths	✓	
Hunt Exposed Secrets and Credentials	✓	
Test Identified Credential Access	✓	
Identify Overly Permissive Network Access Controls	✓	
Exploit Misconfigured Cloud Services	✓	
Exploit Vulnerable Network Services and Applications	✓	
Identify Abandoned Subdomains	✓	
Phase 4: Analysis & Reporting		
Likelihood Determination	✓	
Impact Analysis	✓	✓
Severity Determination	✓	