QUALYSEC
BEYOND CYBERSECURITY

METHODOLOGY

CLOUD

PENETRATION TESTING

SUMMARY OF ENGAGEMENT

Qualysec's Cloud Penetration Testing is a comprehensive approach to identifying security concerns in the cloud environment. They use open-source and proprietary methods to uncover a wide range of cloud-based vulnerabilities. This engagement requires credentialed access to the cloud environment and meets with stakeholders to understand and confirm the objectives and scope of the engagement. The team then performs discovery and enumeration of all in-scope cloud exposures and simulates the threat of someone with access to the cloud environment. The primary outcome of this engagement is to ensure your security teams understand all cloud exposures and prioritize remediation based on the likelihood of an 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 & Enumerat e

- 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 previoussteps will be leveraged to traverse cloud escalation paths, hunt and find exposed credentials, test accessof 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

To guarantee the project's timely completion and success, the necessary assessment requirements must be fulfilled.

PRE-ASSESSMENT REQUIREMENTS	
ACCOUNT FOR CONFIGURATION REVIEW	In order to access the following: • API access to the cloud environment • Graphical User Interface (GUI) or Console access to the cloud environment • Security Audit permissions Qualysec's engagement manager will give specific instructions on how to establish an account with the appropriate permissions
ACCOUNTS FOR PENETRATION TESTING	To conduct penetration testing, the assessment team needs account credentials that resemble a standard user account or a breached application/microservice. The access should align with the objectives of the penetration test. For instance, the access may imitate an account of a software developer.
ENVIRONMENT ACCESS	To conduct the assessment, the team needs network access to the cloud API and all relevant services. This access is usually provided through one of the following methods: • A client laptop with VPN access • A Jumpbox • Direct internet access
OBJECTIVES	Before starting the fieldwork, the assessment team collaborates with the client's team to establish the main engagement objectives. These objectives commonly include: • Achieving high-value targets, such as privileged credentials or customer data • Expanding the attack to restricted areas of the cloud

PRE-ASSESSMENT REQUIREMENTS

OBJECTIVES	•Stealing data to evaluate the client's detection abilities • Obtaining specific levels of access and privileges as a simulated attacker.
SCOPE	To conduct the assessment, the team needs a list of cloud environments that are in scope, such as: • AWS accounts • GCP projects • Azure subscriptions
DUE CARE	Throughout the assessment, Qualysec endeavors to reduce disruptions to network availability, especially during automated scanning, manual validation, or penetration testing. Before testing, the assessment team will talk about the risks to the environmental stability with the client and establish the escalation process in case any disruptions are noticed.
AUTHORITY	Before the beginning of fieldwork, written consent to test must be obtained from the third-party system host if any part of the product or associated resources is located on a third-party system.

	Qualysec	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

During this stage, the evaluation group commences on-site work utilizing both automated tools and manual methods to collect and examine information regarding cloud implementation.

PRE-ASSESSMENT REQUIREMENTS	
CONFIGURATION ENUMERATION	The evaluation group employs both open-source and proprietary tools to acquire the following configuration details: • Service configuration information • Identity and access management (IAM) configuration data • Resource-level access controls, such as data buckets • Credentials and other confidential data exposures The team then employs this information to carry out the following tasks: • Detect possible security misconfigurations • List cloud privilege escalation routes • Chart the environment's attack surface.
NETWORK DISCOVERY	From a location within the cloud network, the evaluation group executes the following actions to locate active hosts on the target network: • Cloud Resource Enumeration - Utilize cloud API to find exposed service endpoints • Common TCP Port Scanning - Conduct port scanning to locate specific TCP ports, focusing on the subnets linked to the previously recognized hostnames and domains.
SERVICE AND APPLICATION ENUMERATION	Once active hosts on the target network are found, the group attempts to list running network services by implementing the following techniques: • Detailed Port Scans - Perform a TCP/UDP port scan on known ports and live hosts • Service and Application Enumeration - Attempt to identify and inspect running network services and applications.

	Qualysec	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 completing the configuration review, the evaluation group carries out the following actions to detect and take advantage of vulnerabilities within the cloud implementation.

PRE-ASSESSMENT REQUIREMENTS	
CLOUD PENETRATION TESTING	The evaluation group endeavors to infiltrate in-scope systems and credentials, move laterally, and increase privileges within the target environment by undertaking the following actions: • Traversing Cloud Privilege Escalation Paths • Searching for Exposed Secrets and Credentials • Verifying the Accessibility of Identified Credentials • Identifying Excessively Permissive Network Access Controls • Taking advantage of Misconfigured Cloud Services • Exploiting Vulnerable Network Services and Applications • Finding Unused Subdomains

	Qualysec	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

Qualysec reports providing an executive summary of the engagement, including assessment goals, high-impact findings, and recommendations. Each conclusion includes a vulnerability definition, replication steps, and tailored advice. The assessment team evaluates the business risk of each finding.

LIKELIHOOD DETERMINATION	For each vulnerability, the evaluation group evaluates the probability of it being exploited, taking into account: • Threat-source Motivation and Capability • Characteristics of the Vulnerability • Presence and Efficiency of Controls
IMPACT ANALYSIS	The evaluation group examines and assesses the consequences of the successful exploitation of each vulnerability on the organization and its customers in terms of confidentiality, integrity, and availability.
SEVERITY DETERMINATION	Qualysec assigns severity ratings by utilizing internal expertise and commonly used rating methodologies such as OWASP and CVSS to evaluate the probability and impact of exploitation. The group considers those factors to categorize the overall severity as critical, high, medium, or low. The severity of each finding is determined separately from the seriousness of the other conclusions.

	Qualysec	Client
• Likelihood Determination	✓	
• Impact Analysis	✓	
• Severity Determination	✓	

PHASE 5: REMEDIATION REVIEW (OPTIONAL)

Upon request, the evaluation group repeats scanning and testing of the identified vulnerabilities after the client confirms that the vulnerabilities have been resolved.

APPENDIX

Delineation of Responsibilities	Qualysec	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 RunningNetwork 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	✓	