Cloud Penetration Testing

Risk Advisory Services

INTRODUCING OUR COMPREHENSIVE CLOUD PENETRATION TESTING SERVICE

In today's digital landscape, ensuring the security of your cloud infrastructure is paramount. Our expert team conduct thorough penetration tests to identify vulnerabilities and potential threats in your cloud environment. We simulate real-world attacks to provide you with actionable insights and recommendations, helping you fortify your defences and protect your valuable data. Trust us to safeguard your cloud assets and maintain the integrity of your business operations. Choose our Cloud Penetration Testing Service for peace of mind and robust security.

SERVICE FEATURES

- Scan and test your cloud infrastructure, leaving no stone unturned
- Adjust the testing approach based on the cloud characteristics, complexity and sensitivity
- Simulate realistic and relevant attack scenarios that match your threat profile and industry
- Receive a report that gives you the insights, recommendations and steps to improve your cloud security

WHAT WE DO

- Identifying cloud services and vulnerabilities from an anonymous perspective
- Identifying cloud services and vulnerabilities from an authenticated perspective, with a customer-provided account
- Iterative performance of the following activities as required during each portion of the assessment:

Intelligence Gathering

- Username/email harvesting
- Query breach databases for exposed credentials

Host Discovery

- Port scanning
- Service identification
- Service enumeration
- Web directory brute forcing
- Critical data exposure identification

Exploitation

- Payload generation
- Vulnerability exploitation
- Exploitation through manual and automated attacks
- Password spraying attacks (cloud infrastructure)

Post-exploitation

- Persistence
- Privilege escalation
- Defence evasion
- Credential access
- Discovery
- Lateral movement
- Execution
- Collection
- Simulated data exfiltration
- Command and control

Report consisting of:

- An executive summary of the work carried out and results of the test
- A review of test findings
- A review of remediation recommendations

EXCLUSIONS

- Social engineering
- Active denial-of-service testing
- Migration, maintenance or configuration of any data, applications, systems or services
- Remediation of any previous compromise or clean-up from any non-testing activities
- Unless otherwise purchased, re-testing of the system or environment is not included

PRE-REQUISITES

- Signed rules of engagement (consent) document
- Approval from required third parties to execute the scope of work
- Provide a list of target IPs and/or URLs, SSIDs and locations
- Allowlist CDW-provided IP addresses and/or domains on IDS/IPS/WAF systems which could impede testing activities
- The customer should provide credentials for an account principal with the following permissions:
  - Azure: An account with Global Reader permissions (including reader and security reader roles). Additionally, the customer must have an Azure tenant with active subscriptions.

WHY CDW?

Leverage adversarial emulation (CDW's Red Team), vulnerability and penetration testing services with consultants who have best-of-industry offensive security certifications such as OSCE, OSCP, OSWE, OSWP, CEH and CRTP, in addition to networking and general security certifications such as CISSP, CISM, GSEC, Network+ and Security+

These are the applicable SKUs for the service described in this document:

Service Name	SKU/EDC
Azure Cloud Penetration Test	8053034
Cloud Penetration Test Ad-On - VA Scanning 1-100IPs	8053040
Cloud Penetration Test Ad-On - VA Scanning 101-250IPs	8053044
Cloud Penetration Test Ad-On - VA Scanning 251-500IPs	8053051
Cloud Penetration Test Ad-On - VA Scanning 501-1000IPs	8053055

Engage your account representative to discuss your desired timeline to start, deadline and the scope.

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca/security.