G-Cloud 15 Service Definition

Accenture CHECK & CREST Approved Penetration Testing and Red Team Activities

Jan 2026

accenture

Contents

1.0 Scope of our services

Service introduction

Penetration testing aims to uncover security weaknesses in IT systems based on specific needs and targeted scope. We offer a range of offensive security testing services. From traditional penetration testing focused on individual applications, networks or services, to phishing simulations and in-depth simulated attacks. We can also undertake specialist configuration review when required. We are flexible to any bespoke requirements for example physical intrusion scenarios.

Service features

- On shore security cleared team
- CHECK & CREST approved
- Application pen-tests typically covering Web and API interfaces
- Also cover bespoke thick client applications
- Infrastructure pen-tests cover physical and virtual hardware
- Also, software defined services including fabric, network and server infrastructure
- Bespoke simulated phishing exercises designed specifically for your organisation threat-profile
- Our simulated attack & Red Team exercises are designed to replicate capabilities and methods of advanced persistent threat actors targeting your organisation
- Reporting: CVSS standard with flexibility to conform to any bespoke-reporting requirements
- Provision of embedded testing resources into your project team to accelerate delivery
- All our testers are certified: CREST, Offensive-Security, Cybersphere and SANS-accreditations

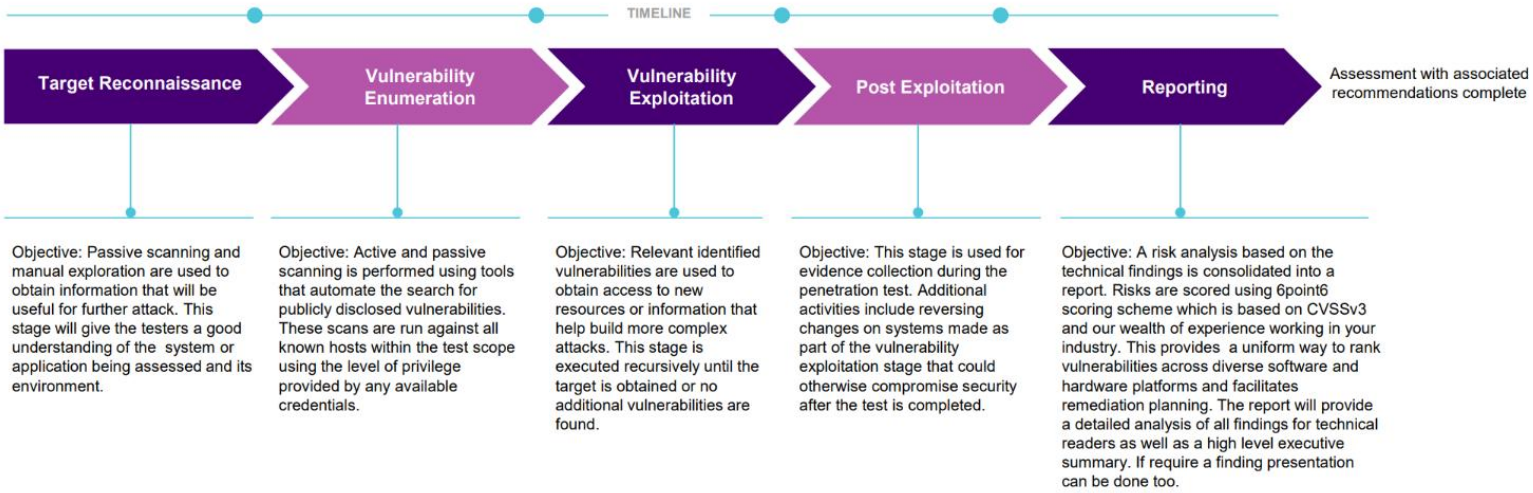
Service benefits

- Identify and mitigate complex security vulnerabilities before an attacker exploits them
- Understand how an attacker is most likely to target your organisation
- Get an independent view of your organisations IT security exposure and how it compares with the rest of your industry
- Allow your security teams and controls to practice against a real adversary in a controlled way
- All our testing is supported by our internal research and development

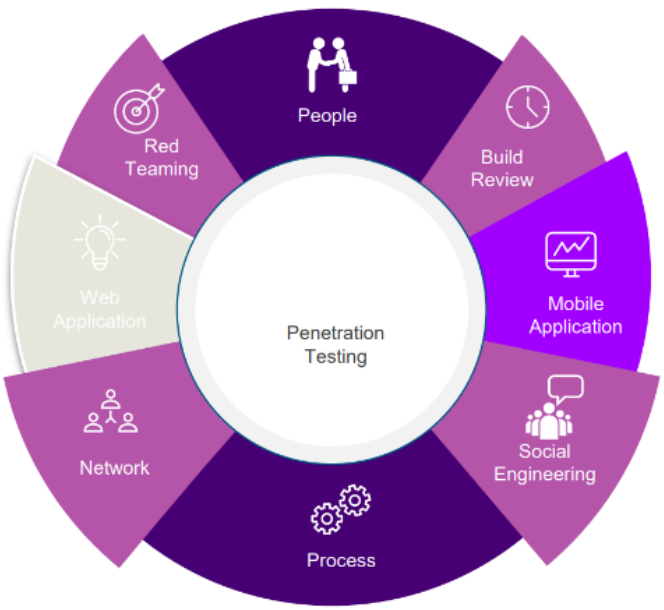
- Exercise the robustness of your IT-security-controls
- Phishing simulations test the cyber awareness of your employees
- Supported and derived from the Research & Development activities of our Lab
- Accelerated project delivery and 'shift-left' of vulnerability identification
- Cyber-risk assessment against your applications (web/mobile/thick-client), infrastructure (Cloud/On Prem-hosted)
- Exercise the maturity of your incident-response-plans

2.0 Service Implementation

Penetration tests are tailored to an organisation's specific environment and needs, in order to appropriately assess the aspects and state of the security programme as well as critical systems. We use people and technology in order to deliver enhanced findings. Unlike other testing companies we can provide more aftercare including a presentation of the results to relevant stakeholders.



Example Tests



3.0 Build Review

DESCRIPTION A authenticated security review of a system. This test type will not attempt to exploit any vulnerabilities so can be done on live systems with no risk. Typically build reviews are done on; firewall configuration files, user devices or a cloud management console but we can perform a build review on most types of assets.

OBJECTIVE Evaluate how well locked down a device or system is. A build review can be performed on all kinds of assets from laptops and phones to firewall configurations and cloud hosted networks.

BENEFITS Discover new security controls that can be applied to your company assets. These will reduce your security exposure in a cost effective and unrestrictive way.

TEST TYPE White box, authenticated test.

LIMITATIONS Findings are not confirmed through exploitation.

TYPICAL VULNERABILITIES Lack of hard drive encryption, overly permissive firewall rules and missing security settings.

Mobile Application

DESCRIPTION Penetration test with a clearly defined scope covering a mobile application and its associated back-end infrastructure. This will involve looking for and exploiting security vulnerabilities in the target scope. This test is sometimes done together with a build review of the infrastructure.

OBJECTIVE Fully explore all security issues that could be present in your mobile application. Your application will be reverse engineered and security tested on a rooted/ jailbroken as well as non-rooted/jailbroken device. We can test both android and iOS mobile applications.

BENEFITS Uncover security vulnerabilities in your mobile application that can expose your application data to malicious applications or users. Clear and concise remediation advice will be given for each vulnerability.

TEST TYPE Grey box authenticated and unauthenticated testing.

LIMITATIONS Potentially destructive tests will be run so it is a good idea to perform this testing on a non-prod environment if the application can upload data to TYPICAL VULNERABILITIES Lack of certificate pinning, overly permissive authentication controls rules and no root/jailbreak detection.

Social Engineering

DESCRIPTION A simulated social engineering campaign could involve physical security checks such as tailgating attempts or just consist of a phishing campaign depending on the client's requirements. Phishing is by far the most common way for hackers to compromise a network, our phishing campaigns are usually run in stages to cover several attack vectors including fake login, malicious attachments and links.

OBJECTIVE Evaluate how susceptible to social engineering attacks your organisation is and exercise any anti-social engineer controls that might be already in place.

BENEFITS An understanding of how strong the cyber awareness within your organisation is. You will get a breakdown by department of which users are most vulnerable to these types of attacks so targeted training can be run.

TEST TYPE Black box, unauthenticated testing.

LIMITATIONS This engagement type focuses on employee cyber awareness rather than technical security misconfigurations. The impact of a successful attack is not explored in as much details as the likelihood.

TYPICAL VULNERABILITIES Lack of cyber awareness mean employees in HR are highly susceptible to phishing, Lack secure email gateway.

Network Infrastructure

DESCRIPTION Penetration test with a clearly defined scope covering some cloud hosted infrastructure, this could be standard corporate office infrastructure or a more bespoke production network. This will involve looking for and exploiting security vulnerabilities in the target network. If testing is done on a live environment care will be taken with any potentially destructive attacks.

OBJECTIVE Discover any security vulnerabilities on your locally hosted network infrastructure. Testing will utilise a mix of cutting-edge automated tools and manual testing expertise.

BENEFITS Understand the risks to your network from threats that are acting from outside and inside your network. Clear and concise remediation advice will be given for each vulnerability.

TEST TYPE Grey box authenticated and unauthenticated testing.

LIMITATIONS The **scope of the testing is strictly limited.**

TYPICAL VULNERABILITIES Credentials sent in clear text, Overly permissive firewall rules, DNS zone transfer.

Web Application

DESCRIPTION Penetration test with a clearly defined scope covering a web service. This could be a normal website for human users or an API. This will involve looking for and exploiting security vulnerabilities in the target scope, so it is recommended to conduct the test in a non-production environment if possible. This test type is often done together with a build review of the infrastructure.

OBJECTIVE Comprehensively assess a web application or API for vulnerabilities that can lead to unauthorised access or data exposure. All web focused testing covers the standard OWASP web testing practices.

BENEFITS Understand the potential security risks of any systems that are exposed to the internet. Then get remediation advice for any risks that have been found.

TEST TYPE Grey box authenticated and unauthenticated testing.

LIMITATIONS The scope of the testing is fairly strictly limited.

TYPICAL VULNERABILITIES SQL injection User enumeration Credentials sent in clear text, Weak ciphers, Stored cross site scripting.

Red Teaming

DESCRIPTION Pulling all the testing services together, a Red Team engagement will target all systems in your organisation using any kind of attack possible. These are typically much longer and larger in scope than other test types.

OBJECTIVE Run a simulated attack against your whole organisation. Attacks against applications, system infrastructure and social engineering will all be considered. This will allow you to discover the most likely attack paths a hacker will follow when attacking your organisation. Additionally, you can evaluate how effective your security operations team currently are.

BENEFITS Exercise your security team against a real attacker in a controlled way. If your security operations team are unaware of the red team, you get a clear view of how they will respond in the case of a real attack. Discover security vulnerabilities in your organisation, clear and concise remediation advice will be given for each vulnerability.

TEST TYPE Black box, unauthenticated testing.

LIMITATIONS The wide scope of this engagement type requires many man hours.

TYPICAL VULNERABILITIES Poor network segmentation, Improper access controls Missing critical OS patches Directory Traversal Remote code execution Social engineering awareness.

Key Differentiators

Outcomes of Our Penetration Tests

- Non-technical summary for executives and senior-level management
- Technical details that include enough information to recreate our attacks
- Fact-based risk analysis to define the criticality of each finding in the context of your environment
- Tactical and strategic recommendations for immediate and longer-term improvement

Benefits of Our Penetration Tests

- We will Identify complex security vulnerabilities and show you how to mitigate them before an attacker can exploit them

- We understand how the most sophisticated attackers operate based on intelligence gained from our years working in the most secure environments in the country
- Our team of penetration testers are Crest certified professionals and work in a multidisciplinary team to ensure you get the best person for the job

4.0 Pricing

Please refer to the associated pricing document/ rate card relevant for this service.

5.0 Contacts

Email: UK.TenderMonitoring@accenture.com

Telephone: +44 (0) 20 7844 4444

6.0 About Accenture

Accenture is a leading global professional services company that helps the world's leading businesses, governments and other organisations build their digital core, optimise their operations, accelerate revenue growth and enhance citizen services—creating tangible value at speed and scale. We are a talent- and innovation-led company with approximately 799,420 people serving clients in more than 120 countries. Technology is at the core of change today, and we are one of the world's leaders in helping drive that change, with strong ecosystem relationships. We combine our strength in technology and leadership in cloud, data and AI with unmatched industry experience, functional expertise and global delivery capability. We are uniquely able to deliver tangible outcomes because of our broad range of services, solutions and assets across Strategy & Consulting, Technology, Operations, Industry X and Song. These capabilities, together with our culture of shared success and commitment to creating 360° value, enable us to help our clients reinvent and build trusted, lasting relationships. We measure our success by the 360° value we create for our clients, each other, our shareholders, partners and communities