# Service Definition

## G-Cloud 13
## Lot 3 – Cloud Support

## Version: 1.0 (April 2022)
## Unrestricted

**Axis Pentest Limited**
**The Maltings**
**2 Anderson Road,**
**Birmingham,**
**West Midlands,**
**B66 4AR**

**info@axispentest.com**
**www.axispentest.com**
**020 8133 9999**

Axis Pentest Limited is Registered in England and Wales
Company Number: 11654892
VAT Registration: 310 9427 27

# Service Definition

## Deliverables

The main deliverable will be the final assessment report. This is a high-quality document which starts with the executive summary. This describes the overall level of risk perceived to result from the findings and the associated business impact.

The report will confirm the testing scope and note any caveats or points of interest to be considered while consuming the report.

Our reports aim to be straightforward and plain. There will necessarily be technical details in the description of each finding discovered. Each issue will be detailed so that technical teams can understand and recreate the finding so that it may be resolved and retested.

Findings will be rated in a 5-level traffic light system from Critical to Informational in. As required, scoring can also be performed with the CVSSv3 rating system.

Remediation recommendations will be provided, where wider lessons can be drawn these will also be highlighted, for example structural deficiencies.

Where successful exploitation necessitates prerequisites, these will be stated so the finding can be put into context.

Where appropriate, the tools or custom scripts used to exploit an issue will be documented or provided in order to foster knowledge transfer.

## Onboarding

The onboarding process sees the signing of a mutual NDA and the subsequent formulation of the first proposal. This is done by conducting the initial scoping exercise to ensure the requirements, objectives and risks are well understood and communicated.

## Ordering and Invoicing

Once the project scope is agreed a valid purchase order will be required in order to commence the project scheduling subsequent delivery processes.

An invoice will be issued after successful delivery to the value agreed and set out in the proposal. Standard payment terms are 30 days from the date of invoice.

## Pricing

Volume discounts can be applied based on the number of days within the contract period.

- Up to 15 days – 0% discount
- 16 to 30 days – 5% discount
- 31 to 50 days – 10% discount

- 51 to 75 days – 15% discount
- 75 days plus – 20% discount

## Contract Termination

Please refer to the Axis Pentest Terms of Business document.

## Customer Responsibilities

Please refer to the Axis Pentest Terms of Business document.

## Service Constraints

While no specific service constraints can be quoted all services are subject to circumstances such as, exact requirements, site locations, skills and technologies.

## Financial Recompense

A formal framework is not defined though one can be negotiated.

## Levels of Data Backup, Restore and Disaster Recovery

N/A.

# Web Application Penetration Testing

## Why Test Your Web Application?

The explosion of the Internet has led web applications to be the ubiquitous gateway to offer services over the World Wide Web. Early platforms and web applications were usually riddled with common web application flaws. Even as platforms and defences have matured over the last 20 years well established classes of security flaws can still readily be found and exploited.

The news regularly brings a flow of compromises and breaches, some resulting from vulnerabilities in web applications that have been exploited to extract databases full of sensitive customer data.

There is no substitute for having your web application periodically manually tested for both common and novel web application security issues.

## How We Work

Each web application test starts with information gathering which includes mapping out the functions from an unauthenticated and authenticated user perspective. The nature and structure of the supporting infrastructure stack and potential defences are also included in early reconnaissance stage. Where multiple user privilege level exist, these are enumerated so that options for privilege escalation can be assessed.

Broadly speaking the OWASP methodology is used to assess web applications, this is applied with the benefit of expert skill and experience.

Options for attack and penetration are guided by a thorough understanding of the application gained during the reconnaissance stage. This can be improved by the inclusion of a source code assisted element, this sees the web application assessed with the knowledge of the application's inner workings.

## What are the Benefits?

The resulting deliverable will highlight risks where they are identified. The exercise will also aim to identify application characteristics and practices which are in line with good security practice. The engagement will identify whether the level of security alerting and monitoring in place are appropriate.

A manual web application test can often lead to the detection of flaws in the common areas of web application security including input validation, session management, error handling, SQL injection, flaws in logic and authentication mechanisms.

The detection and resolution of such issues will make an incremental improvement to the level of security of your web application.

# Internal Penetration Testing

## Why Test Your Internal Infrastructure?

Internal networks are the unseen workhorses of the modern enterprise, security can easily be neglected. Attention and resources can flow to externally facing services which are perceived to be in the direct firing line.

Over time internal networks grow in size and complexity, software and new technologies are added with functionality as the main driver. This complexity comes at a cost, patching, monitoring and security may suffer as the management overhead swells.

Internal systems may often be thought of as ‘safe’, and not liable to malicious interference as they are not subjected to daily probes as external networks are. This can leave internal networks vulnerable from internal hacking or mishaps from users assigned excessive privileges.

Add to this the fact that the internal network may have a wide range of technologies connected to it over time, often with little control over who connects what.

## How We Work

Internal network pentesting can be scoped in a multitude of ways, perhaps as a strictly time-limited exercise or as a wider scale engagement. The target is generally to attain the highest level of privilege possible.

Generally, when targeting the internal network, the consultant will be given physical network access and no more. Key network components will be identified, enumerated and targeted until the objective is reached. The first stepping stone in the chain of compromise will often be to gain a foothold in one service, server or user account. From this point the attacker, in this case the pentester will aim to escalate privileges within the network typically without being detected.

## What are the Benefits?

The resulting deliverable will highlight risks where they are identified. Typically, if the internal network is not suitably hardened the scales will be weighted in favour of the attacker. There may be multiple items of ‘low-hanging fruit’ which are exploitable and lead to the attacker being able to gain the highest privilege available to network administrators in a short timescale.

In these cases, the report will not only be able to identify the key technical points of weakness but also structural failings which lead to the overall result.

Experience shows that over one or two cycles of pentesting and issue mitigation the picture can be much improved. More significantly, the associated structural changes including those in user behaviour can alter the trajectory of a network in terms of security more fundamentally.

Internal network-based engagements are a great channel for knowledge transfer from the testing team to the client and we promote this.

# External Penetration Testing

## Why Test Your External Infrastructure?

Due to its nature, externally facing infrastructure can be the most visible element of the enterprise and the first to come under attack. Internet connected components will be subjected to prods, probes and attacks of all types from attackers with a range of motivations and skill sets.

## How We Work

Once the target IP ranges and the proposed approach is agreed the network fingerprinting can commence. Accurate probing of services and assessment of the underlying systems is key to providing a solid foundation for later work. As the fingerprinting and reconnaissance stages come to an end, the vectors for attack come into focus.

After an analysis stage the identified attack vectors are then executed to their fullest extent. Information gathered in one attack vector is fed through to all others, this may lead to new possibilities for attack becoming available. Open source intelligence (OSINT) may be used to feed into and select attack vectors.

The attack work will be guided by the agreed approach and constant feedback between the engaged team and the client will communicate high risk vulnerabilities as they are identified. This can reduce the time-lag to resolve findings.

## What are the Benefits?

External pentesting gives the enterprise an independent view on the exposed Internet services and the options for attack.

The testing can also be used by network defenders to test and tune their defences to ensure that key events are alerted upon and low-level noise does not distract from higher priority events.

Our manual approach takes the best facets of best of breed automated tools and improves these by removing false positives. A practical approach is taken to rating risks in the context they exist and in relation to the real-world ramifications.

The manual approach taken can chain together seemingly unrelated findings which together can used to forge a chain of attack leading to results which are greater than the individual findings.

# Wireless (Wi-Fi) Penetration Testing

## Why Test Your Wireless Network?

The key feature of wireless networks is also a factor that makes pentesting wireless networks most interesting. Wireless networks can be attacked while remaining physically distant, using commodity hardware and freely available knowledge, all whilst remaining unseen.

## How We Work

The main pre-requisite required from the client is the SSID of each network in scope. These are included in the 'Authorisation to Test' by the client before testing can begin, as with other types of pentest engagement.

Each network in scope is targeted to identify the type and nature of the wireless technology in use. These are then attacked from the perspective of an untrusted party. It is common for wireless testing to be performed where a sample wireless client is provided so that its configuration can be reviewed to ensure it fits with good practice in all areas including authentication and authorisation.

A review of the wireless management console can also be included in the scope. This gives the pentester the ability to switch from an attacking perspective in order to add value to the engagement by conducting an internal configuration assessment of the wireless network infrastructure.

## What are the Benefits?

A thorough independent pentest and review of your wireless network can identify technologies and protocols which are no longer considered to be in line with best practice. These may be vulnerable to practical risk and attack or theoretical attacks which are difficult to exploit in practice.

Practical pentesting can be used to test the configuration to see if, for example guest users are indeed segregated to only those areas which they should rightly be able to access.

Identification and exploitation of weak authentication mechanisms or poor configuration may allow attackers to connect to vulnerable wireless networks. Determined attackers may then be able to target the internal network as if they were directly connected, whilst inside the premises.  This is an example of a finding we have reported in a medical healthcare setting. If exploited by a malicious attacker this could have been catastrophic in terms of reputational damage and risk to information assets.

## Company Profile

Axis Pentest is a cyber security and penetration testing specialist.

Through tailored engagements we simulate adversaries to map your defences and weaknesses allowing security to be bolstered by building layered defences.

We regularly engage in specialised security assessments for government bodies and high-profile commercial clients alike.

Through experience and resourcefulness we keep a step ahead of the landscape.

Our expert team keep pace with industry leading certifications and developments.

All our consultants are qualified with CREST, Cyber Scheme or Tigerscheme certifications. We are dedicated to maintaining and improving the certifications we hold.