Penetration Testing

G-Cloud 15 Service Definition

1. Summary

We operate a CREST-accredited penetration testing service focused on education and research sectors. We identify vulnerabilities, help assess risks, and recommend mitigation to protect against relevant threats. Our experienced and certified in-house cyber security experts conduct tests across numerous areas, including network infrastructure, applications, social engineering, build image review, and Active Directory.

A foundation of strong communication and collaboration will help you understand and remediate any findings and develop processes to stay on top of issues in an ongoing manner.
Normal

1.1 Benefits

Penetration testing takes the approach of simulating an attacker, looking for ways to circumvent your security systems and data using common tools and techniques.

While the specifics of a test vary based on the goals and targets involved, the general goal is to identify weaknesses in the tested system. This allows you to assess and understand your cyber security posture, and to find and fix flaws before threat actors or malicious users can do so.
We then provide a comprehensive report, helping you to determine:

- Where your vulnerabilities lie – including how well your systems tolerate real-world attacks and how successfully you detect and respond to them.
- What impact these vulnerabilities may have - and how likely they are to be exploited.
- What actions you can take to improve your security posture.

All work is carried out by our in-house cyber security experts -– who are experienced, trained and certified.

As a trusted partner to member organisations, Jisc can draw on insights and best practices from across the UK education sector.

- Our foundation of communication in consultancy ensures results are well-understood
- Working exclusively in Education, we deeply understand the sector's needs
- Our day-rate pricing model maximises effective use of testing time
- Our testing benefits from access to Jisc's organisation-wide expertise

- Optional free post-test call is available to discuss results
- Optional half-day retesting included free of charge
- Supporting skills sharing with your team for ongoing security
- We can carry out onsite and remote testing

1.2 Features

Why Use Jisc?

- We offer very competitive rates compared to commercial equivalents.
- We have experience and expertise in testing the applications and systems our customers commonly use, such as specific Virtual Learning Environment platforms.
- We feed back our anonymised threat findings to the sector for the benefit of the whole community.
- Where appropriate, we will communicate with software vendors and service providers so remediation can take place quickly and fixes can be rolled out across the area/sector.
- Deep knowledge of sector-specific information technology and threat landscapes. We understand the security challenges faced across the sector, such as devolved IT departments and legacy systems and software.
- Our security experts can offer workshops as part of an engagement to upskill your internal staff and enhance your testing and security capability for the future.
- Consultation-led, bespoke test scoping for white, grey and black-box testing.
- External and internal network infrastructure, applications and attack modelling.
- Active Directory and build image review, privilege escalation, lateral movement.
- Desktop and Web applications, API testing, role-based authenticated testing.
- Social engineering, phishing simulation, onsite physical security and covert infiltration.
- Wi-Fi secure configuration assessment, access to Eduroam expertise.
- Manual testing and automated vulnerability assessment using industry-recognised scanning tools.
- Flexible customer-focused approach including technical skills and knowledge sharing.
- Direct, frequent communication with testers resulting in a tailored report.

2. Service Definition

2.1 Core Service Offering

2.1.1 Conduct varying tests according to your needs and budget

Because this is a flexible service, we offer a customised scope and depth of penetration testing, making the service cost-effective for you. Our service could range from a straightforward evaluation of your external networks to many hours of involved on-site manual testing. Alternatively, you may simply be looking to have the security of an individual system or application tested before it is deployed, or you may be interested in the wider security of your network.

Before testing begins, we can advise you on the level of service you are likely to need.
We regularly carry out penetration tests of various scopes, such as:

2.1.1.1 External and Internal Infrastructure Testing

The infrastructure testing and scanning tasks include internet-facing hosts, servers, end-user devices, and network devices such as firewalls and access points. Test activities that would be carried out to achieve this include:

- Automated and manual port scanning of all targets and ranges.
- Vulnerability scanning of all targets.
- Use of credentials for authenticated access where provided.
- Enumeration of services and host information across targets, including information available from sources other than the target (such as DNS and certificate information, or leaked credentials).
- Investigation of services identified, including manual testing for vulnerabilities and verification of detected issues.
- Light-touch testing where specified.
- With appropriate approval, demonstrating exploitation of vulnerabilities and investigating the impact of an attack.

2.1.1.2 Web Application Testing

Test activities for executing web application tests include:

- Crawling and fingerprinting of all in-scope applications to the required depth.
- Investigation of page functionality, through normal and abnormal use.
- Review of headers for information gathering and potential exploitation.
- Use of credentials for authenticated access where provided.
- Testing to bypass or undermine authentication processes.
- Attempting to send text and file payloads to execute code or bypass restrictions.
- Fuzzing of user inputs to verify correct handling of data.
- Attempt to exceed user privileges, such as bypassing access restrictions and reading/writing areas outside of user permissions.
- Exclusion of specified forms (e.g. avoiding sending significant volumes of traffic through an automated form).

2.1.1.3 Build Reviews

Build review activities assess the ability of a malicious user to carry out unintended functionality based on the way a baseline system image is implemented. Testing activities include:

- Reviewing and enumerating the configuration of the representative system (such as users and policies present), and AD configuration where relevant.
- Identifying issues such as misconfigured services, or the ability to run certain commands.
- Use of user credentials for information gathering, such as requesting information from the domain.
- Searching for the presence of sensitive information, such as readable or easily cracked user or service passwords.
- Identification of resources, software and services that can be installed and manipulated.
- Attempting to escalate privileges from a normal user perspective. For example, using a software packaged to access PowerShell restrictions, then using a malicious script to harvest administrator credentials.

2.1.1.4 Dedicated Active Directory Testing

- Dedicated testing efforts focused on the Active Directory include the following, across multiple levels and configurations of user permission based on provided credentials:
- Investigation focused on identifying and exploiting issues within the domain.
- Review of the domain configuration and how it's used, through user requests and discussions with administrators.
- Mapping of relationships between domain objects such as groups.
- Identification and exploitation of vulnerabilities to demonstrate lateral movement or privilege escalation within the domain.
- Use of techniques focused on the interaction between permission/authentication systems and processes.

2.1.1.5 Wi-Fi Testing

Testing the Wi-Fi security involves an onsite visit to a location where the in-scope SSIDs (Service Set Identifier) are in use, and includes:

- Use of specialised Wi-Fi cards to attempt to capture and manipulate Wi-Fi traffic.
- Assessment of visible networks and their resilience to types of attack such as handshake capturing, credential theft, and evil twin attacks.
- Where handshake capture is achieved, attempted cracking against common and specialised wordlists to assess the passkey complexity.

2.1.1.6 Social Engineering and Physical Testing

Testing the operational security and response of staff to security threats. This can consist of a variety of activities at different levels, tailored to the needs of the test, such as:

- Sending phishing emails to gather information or capture user credentials. This can be a targeted attack, with the intent to use captured credentials as part of further testing, or a general phishing exercise to assess the overall risk of the organisation. This can be carried out in combination with existing training materials.
- Using social engineering techniques, such as phone calls, to gain access to systems. For example, calling IT and requesting a password reset for a different user.
- Attempting to gain unauthenticated physical access to sensitive areas such as executive offices or server rooms. Non-destructive testing, which can either be carried out as part of technical testing, or under an "assumed breach" method.
- Where handshake capture is achieved, attempted cracking against common and specialised wordlists to assess the passkey complexity.

2.1.1.7 Purple Team and Information Sharing

Working alongside your defensive team to test detection and prevention methods, and share knowledge:

- Executing specific types of attack to measure detection and response, and to demonstrate what an attack might look like in Realtime on the network.
- Attempting to evade defensive measures, while sharing information about what is being done.
- Sharing tools and techniques for attacks to allow your staff to carry out ongoing checks.
- Using social engineering techniques, such as phone calls, to gain access to systems. For example, calling IT and requesting a password reset for a different user.

- Attempting to gain unauthenticated physical access to sensitive areas such as executive offices or server rooms. Non-destructive testing, which can either be carried out as part of technical testing, or under an "assumed breach" method.
- Where handshake capture is achieved, attempted cracking against common and specialised wordlists to assess the passkey complexity.

These tests can help to assess the effectiveness of operational controls, such as sign-in procedures, or whether unknown individuals without ID cards are questioned. It can be effective to test with "presumed access"; for example, the tester having a legitimate key, which they use after pretending to manipulate a lock for some time.

3. Service Level Description

At Jisc, our penetration testing service is designed to provide organisations with cybersecurity solutions tailored to their unique needs. Our service level description outlines the key components and commitments associated with our service offerings:

Initial Consultation

- Response Time: Within 2 business days of initial enquiry.
- Assessment Duration: Variable, depending on the complexity of the organisation's cybersecurity requirements.
- Deliverables: Once the tests have been completed, a fully comprehensive report will be delivered to the Customer. A post assessment call can then take place to go over the findings.

Bespoke Solutions

- Response Time: Tailored solutions provided based on client requirements and feedback.
- Implementation Duration: Variable, depending on the scope and complexity of customised solutions.
- Deliverables: Customised cybersecurity solutions addressing specific security needs, challenges, and compliance requirements.

Trusted Partnership:

- Response Time: Ongoing support and communication provided throughout the engagement.
- Duration: Continuous partnership maintained to address evolving cybersecurity threats and requirements.
- Deliverables: Dedicated pen tester, regular updates, and proactive recommendations to enhance cybersecurity posture and resilience.

3.1 Customer Responsibilities

Active Participation	Customers are expected to actively participate in initial consultations, assessments, and ongoing communications throughout the penetration testing engagement. What information would you need to provide? Different forms of penetration testing mean you need to provide different levels of information about your systems. These include: • White box testing – where you provide full network information. • Grey box testing – where you allow the attacker user-level privileges. • Black box testing – where you provide no privileged information. Typically, you will be required to provide information such as IP ranges, domains, URLs of applications, key systems and applications, and IP addresses and systems that should be avoided. Depending on the test, it may be necessary to provide accounts with appropriate permissions, and remote access to testing machines on the network to support remote.
Resource Allocation	Customers must allocate necessary resources, including personnel and time to support the penetration testing effort effectively.
Feedback and Collaboration	Customers are encouraged to provide feedback, insights, and collaboration to improve the effectiveness and efficiency of our services and support ongoing cybersecurity initiatives.

3.2 Support

We are committed to providing comprehensive support throughout the penetration testing process. Our dedicated team of testers are available to assist customers at every step, ensuring a smooth and successful assessment journey. Support includes:

3.2.1 Advice and Guidance

Our experts offer personalised advice and guidance to help customers understand assessment requirements, assess their cybersecurity readiness, and develop an effective strategy for achieving a robust cybersecurity posture.

3.2.2 Technical Assistance

Our team provides technical assistance to help customers implement and configure security controls, address vulnerabilities, and optimise their cybersecurity infrastructure to meet assessment requirements.

3.2.3 Response and Communication

We maintain open lines of communication with customers, promptly addressing enquiries, providing updates on assessment progress, and ensuring alignment with customer timelines and expectations.

3.2.4 Issue Resolution

In the event of any challenges or issues encountered during the assessment process, our team works diligently to identify solutions, mitigate risks, and facilitate timely resolution to minimise disruption and ensure progress towards a robust cybersecurity posture.

3.2.4 Training and Education

We offer training and educational resources to empower customers with the knowledge and skills necessary to maintain cybersecurity best practices, address emerging threats, and sustain compliance with cybersecurity standards beyond the assessment.

3.2.5 Continuous Improvement

Our commitment to continuous improvement drives us to seek feedback from customers, evaluate our processes and services, and implement enhancements to deliver an exceptional assessment experience and support ongoing cybersecurity initiatives effectively.

At Jisc, our support extends beyond the assessment process to empower customers with the confidence, knowledge, and resources needed to strengthen their cybersecurity defences and navigate the evolving threat landscape with resilience.

4. Service Management

At Jisc, we prioritise effective service management to ensure the successful delivery of the penetration testing service. Our service management approach encompasses various aspects, including:

Service Design and Planning

We meticulously design and plan our penetration testing service to align with customer requirements, industry best practices, and cybersecurity standards. Our team evaluates customer needs, defines service offerings, and establishes clear objectives and deliverables.

Service Transition

During the service transition phase, we facilitate a seamless transition from the initial engagement to the engagement process. This involves coordinating with customers to gather necessary information, conduct assessments, and prepare for the penetration testing engagement, while ensuring minimal disruption to ongoing operations.

Service Operation

Our service operation phase focuses on the delivery of the penetration testing process efficiently and effectively. We leverage our expertise, resources, and technology infrastructure to guide customers through each stage of the assessment, monitor progress, and address any issues or concerns that may arise.

Incident and Problem Management

In the event of incidents or problems encountered during the assessment process, our incident and problem management processes come into play. We promptly identify, assess, and resolve issues to minimise impact and ensure the timely completion of assessment activities.

Change Management

Throughout the assessment process, we adhere to robust change management practices to manage changes to customer requirements, scope, or timelines effectively. We assess the

impact of changes, obtain necessary approvals, and implement changes in a controlled and transparent manner.

Service Improvement

Continuous service improvement is integral to our approach. We regularly evaluate our service delivery processes, solicit feedback from customers, analyse performance metrics, and implement enhancements to optimise service quality, efficiency, and customer satisfaction.

Customer Relationship Management

At Jisc we thrive on building and maintaining strong customer relationships. We encourage, transparent and collaborative communication with customers, ensuring customers' needs are met and understood. Expectations are managed effectively.

Risk Management

We proactively identify, assess, and mitigate risks associated with the testing process to safeguard customer interests and ensure the successful completion of the penetration tests. Our risk management practices encompass risk identification, analysis, treatment, and monitoring throughout the service lifecycle.

With our robust service management practices in place, we are committed to delivering a penetration service that meets the highest standards of quality, reliability, and customer satisfaction.

Our focus on service excellence enables us to empower organisations with the confidence, resilience, and assurance needed to navigate the complex cybersecurity landscape effectively.