NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

Best Practice Guide

Commercially Available Penetration Testing

Issued 08 May 2006

Abstract

This paper provides a technical overview of the different types of penetration test and how these can be used within wider information security assurance activities. It also provides guidance on how organisations should plan for, procure and manage such tests

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the use of information contained in this document or its references.

National Infrastructure
Security Co-ordination Centre
PO Box 832
London, SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@niscc.gov.uk
Web: www.niscc.gov.uk

KEY POINTS

- This document is a guide to the large number of different types of penetration test available, covering different aspects of information security.
- This document is specifically aimed at both non-technical and technical buyers of penetration testing services.
- Penetration testing should be considered as part of a wider programme of information security assurance activities.
- Buyers of penetration tests need to prepare for and manage the performance of penetration tests by third parties in order to obtain value from such tests.
- The frequency of testing should be determined on the basis of risk analysis and when significant changes are implemented.
- High impact systems should be given a priority.
- Penetration testing should be integrated into the system's development lifecycle.
- Test planning should detail the scope and context of the test and consider the assessed threats to the organisation's systems.
- Risk associated with testing should be detailed and managed.
- Remediation should be agreed and project managed.

INTRODUCTION

1. This paper provides guidance on purchasing or managing penetration tests. It also shows how penetration testing fits into a wider range of information security assurance approaches and provides practical, non-technical explanations of testing types and styles. It also provides options for planning tests, including defining objectives, scoping, managing risk (including obtaining test authorisation), provider selection, test management reporting and corrective action identification and implementation.

Definition

2. Penetration testing has been in use for many years and is one of a range of ways for obtaining security assurance. Penetration testing and associated security testing techniques have a variety of definitions, several of which overlap or are used differently by suppliers and buyers of testing.

3. Penetration testing can be defined as the use of techniques and tools to simulate an attack on an organisation's information security. A variety of specific tests can be employed to achieve this, based on an organisation's specific requirements.

4. It is important to understand the difference between penetration testing and vulnerability scanning. Penetration testing uses manual techniques, supplemented by tools, to attempt to penetrate a system. Testing restricted to

vulnerability identification using largely automated tools is generally termed 'vulnerability scanning'.

Assurance approaches

5. Methods of gaining information security assurance include:

- security review of an organisation's Information Security Management System including organisational security strategy, governance approach, policies, standards, staff awareness and assurance and performance management;
- security review of a system's Information Security Management System, including system technical configuration, security procedures, physical security and administrator and user awareness and training;
- security review of the Information Security Management System in operation within an outsourced service provider;
- security review of organisational technical security architectures; and
- technical security review of system configuration of one or more systems.

6. Penetration testing can have a role in any one of these testing approaches – though it is important to understand that security assurance cannot be gained solely through use of penetration testing.

7. Penetration testing can help establish the level of vulnerability that an organisation or system is exposed to while simulating particular threats. Testing therefore provides an important element in understanding overall security risk.

8. While other forms of security assurance provide a theoretical articulation of vulnerability, penetration testing demonstrates actual vulnerability and as such can be more compelling to senior management.

9. Testing can simulate various types of threats by careful scoping, giving an organisation a view of the severity of a particular threat in terms of its ability to exploit actual vulnerabilities in their systems.

Limitations of testing

10. There are several general limitations of testing.

- Technical results can be difficult to interpret in a business context. The nature of testing means that results are often highly technical. Interpreting these in a business context is difficult and requires effective communication between the test provider and the organisation under test. Some penetration testing providers are more capable than others at setting findings and recommendations into a business risk context.
- Commercial considerations mean that test scopes are limited in depth and breadth or timing of the test. A malicious attacker is often not constrained by commercial considerations and can take as much time as necessary to penetrate an organisation or system. Similarly, if an attacker is not able to penetrate a particular system or process, they may simply try another route; depending on the scope of a penetration test this may not be possible.
- Legal considerations will restrain a tester, while a malicious attacker will often do whatever it takes to penetrate an organisation or system. For example, a tester may be limited by the scope to test only systems belonging to the target organisation. A malicious attacker may attempt to attack the business partners, customers or service providers of the target.

- Penetration tests generally do not aim to find all vulnerabilities of a given system. Often they will only discover one possible attack path. Conclusions and resulting corrective actions should take this into account – simply fixing vulnerabilities uncovered by a test could still leave a number of other vulnerabilities present for an attacker to find.

PENETRATION TESTING METHODS

Generic testing methodology

11. Broadly, all forms of penetration testing adhere to the following methodology and tests should progress through these steps in order. The activities performed and amount of time spent on each step will vary depending on the nature of the test and the target.

- Information gathering – background information is gathered from the target, whether the target is a process or a system. An example of this is obtaining public information from the Internet about the target organisation.
- Reconnaissance – positive confirmation of the target is confirmed. Contact is made with the organisation to confirm that targets and security controls are as expected. An example in a physical test would be to visit a target site as a guest or bystander. In a network test, this might be sending traffic to confirm the existence of routers, web servers and email servers.
- Enumeration – establishing the potential points of access being offered by a target. In a network test this will involve scanning for open services on targets or establishing the existence of possible user identification credentials.
- Vulnerability identification – identifying potential vulnerabilities in a target. In a network test this will consist of using tools to test for vulnerabilities on a particular product, for example a router. In a web application test, this may involve finding an input field that does not check for malicious code in the text being entered.
- Exploitation – using identified vulnerabilities to gain unauthorised access to the target. For example, in a web application test, this may involve injecting commands into the application that provide a level of control over the target. Exploitation may require the combination of several sets of information in a creative way.
- Escalation – gaining further access on a target, once an initial level of access has been obtained. For example, in a network test, successful exploitation may allow user or guest access to a system. Escalation through additional exploitation will be required to obtain administrative privilege.
- Advancement – attempting to move on from the compromised target to find other vulnerable systems. For example, in a network test this will consist of "hopping" from one system to another, potentially using the access obtained on the original target to access other systems. In a physical test, this might involve moving from one compromised building to another.

12. With regard to using identified vulnerabilities to perform exploitation, escalation or advancement, there are several methods used by penetration testing providers. These include:

- using third party products containing third party developed exploits;
- using public domain exploit code (eg, that provided by security researchers);

- recoding public domain exploits to achieve slightly different results (eg, recoding an exploit developed for one version of a system so that it also works for other versions of the same system); and
- developing custom exploits for unknown or theorised vulnerabilities.

Test types

13. The table below summarises the types of penetration test that an organisation is likely to conduct:

Category	Type	Description	Benefits	Limitations
Information gathering	Passive research	Passive research is a form of information gathering conducted by analysing information available from public sources of information on the Internet. This can provide considerable detail about an organisation, including its technology environment and its business and security structure.	Passive research involves no, or minimal, communication with a target; it is very unlikely to result in disruption to the target.	Passive research provides no assurance on the actual controls in place in a target organisation. Information may be inaccurate or incomplete.
Infrastructure	External network	A test targeted against externally facing (e.g. Internet or third party) infrastructure such as web servers and email servers. These tests are commonly performed via the Internet. However, tests against infrastructure which is not yet live on the Internet may be performed on site. Tests generally examine only systems owned by the target organisation. Tests of Internet service provider infrastructure will require additional agreements.	Provides a level of assurance on infrastructure that is often exposed to random, or potentially targeted, attacks from malicious software on the internet. External network infrastructure such as public web sites are often important to an organisation's reputation. Network infrastructure is often built on systems with known vulnerabilities. This means that a tester, to some extent, can rely on information in the public domain and on automated tools.	Tests tend to be limited in scope. Associated networks or service provider networks may not be examined and therefore the risks on related critical systems remain unknown. Tests may not provide any assurance on security of internal devices, if such testing was prevented by a border device such as a firewall. Extensive testing can place a load on infrastructure that may impact on performance or disrupt system operations.

Category	Type	Description	Benefits	Limitations
Infrastructure (cont.)	Internal network	This is a type of test targeted against a portion of internal infrastructure. Internal test scopes can be very narrow (e.g. a particular network segment) or very broad (e.g. the entire office network). Tests can be performed by starting with no authorised access to the network, with user access or with privileged (administrator) access, depending on the objective of the test. Internal tests may also include examinations of wireless network infrastructure. These tests are commonly performed on site, although some penetration testing providers have the capability to provide high security remote links.	Internal tests can determine the access a physical intruder or insider might be able to obtain. These tests can also be effective at determining what information different classes of user are capable of accessing. Tests of wireless infrastructure can be effective in determining what information can be accessed by individuals in close proximity to a site.	Extensive testing can place a load on infrastructure that may impact performance or disrupt system operations.
	Voice network	This is a type of test targeted against systems that provide voice telephony infrastructure. Traditionally, this consisted of an attempt to dial a range of telephone and fax numbers offered by the organisation to find and attempt to penetrate attached computer systems and voice mail systems. This is commonly referred to as 'wardialling'. This testing may also now include Voice over IP (VoIP) testing, which overlaps significantly with internal testing in the techniques used.	Voice network tests can determine additional external channels that malicious attackers may use. PABX, modems and remote access systems can be overlooked as tests often concentrate on IP based network infrastructure.	External voice tests can be disruptive as telephone numbers are dialled in sequence. Voice testing is often conducted overnight to minimise disruption although in 24 hour operations, it can be difficult to perform.

Category	Type	Description	Benefits	Limitations
Applications	N/A	This is a type of test targeted against a specific application. Applications are often heavily customised, built on bespoke infrastructure, and may have less priority given to secure coding than the risks might justify. Web applications, and associated databases, are commonly tested as they are often connected to the Internet and considered to carry significant risks. Other applications, such as internal client/server applications or backup applications may also be tested.	Application tests can establish whether an attacker can bypass infrastructure level controls, such as firewalls, and directly compromise sensitive data using application channels.	The custom nature of applications means that testing them is often a highly manual process. However, tools that provide automatic code injection into application fields can be used to ensure testing is rigorous. Application testing can be time consuming and expensive, especially if the test is performed as a 'black box' exercise where no details of the application are provided to the tester. Since a tester is working in the unknown to some extent, there is a possibility that unintentional service disruption may occur.

Category	Type	Description	Benefits	Limitations
Process	Social engineering	Social engineering tests are targeted against staff to extract sensitive information such as passwords. These tests are often performed over the phone although they can be conducted face to face.	Staff are often the weak link in security and can be subjected to persuasion or duress. Social engineering tests can establish where weak points exist within awareness and organisational security procedures.	Social engineering depends on obtaining information from individuals. If successful, this can be very demoralising for the individual and may result in apportionment of blame. Staff morale can be negatively impacted. Social engineering should therefore be deployed carefully.
	Physical	Physical tests are targeted against an organisation's buildings or facilities. Physical controls are often critical to the overall security of an organisation. For example, once physical access to a system is obtained, it is much easier for an attacker to successfully compromise a computer, for example a storage device can be stolen or copied and examined at a later date.	Tests can be used to demonstrate the ease or difficulty with which physical buildings or sites can be penetrated. If combined with other forms of penetration testing, physical tests can also establish the impact of a physical attack, which can be more significant than an organisation may expect.	Staff performing physical tests can be at risk from detention by security guards or arrest by law enforcement. Appropriate authorisation is important for all testing, but this is particularly true for physical testing where the testers could be subject to immediate detention by security guards or law enforcement officials. To some extent, staff morale can be impacted negatively following a successful test.

Category	Type	Description	Benefits	Limitations
Process (cont.)	Response	Response tests are intended to measure how well security detect and respond controls are operating. An example of response testing is an external infrastructure test intended to be detected so as to elicit a response in order to assess the operation of the response process.	Tests can demonstrate the successful operation, or otherwise, of the linkages between technical or physical controls and procedural controls.	Tests are simulations and therefore the response may not be fully equivalent to a real attack. Staff aware of the test may respond in a different way than they would to a real incident.
	Evasion	A test intended to progress as far as possible without being detected by the target organisation. An example would be an external infrastructure test where the presence of IDS is suspected. Tests will be run below the assumed trigger thresholds of the IDS.	Tests demonstrate whether it is possible to evade detection processes while attempting penetration.	Evasion tests can require significant amounts of time to complete as scans and attacks are performed slowly.
	Denial of Service (DoS)	A DoS test is intended to simulate attacks in which a malicious attacker deliberately attempts to disrupt availability.	Tests can establish the effectiveness of processes and technologies intended to provide resilience and continuity.	Certain types of Internet based denial of service attack are nearly impossible to defend against. Simulating these types of attack often adds little value, other than to demonstrate the vulnerability to management.

Category	Type	Description	Benefits	Limitations
Control systems	Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)	Tests against SCADA or DCS infrastructure that operate control or measurement systems. Tests may attempt to discover and penetrate: • SCADA systems from the Public Switched Telephone Network (PSTN); • SCADA systems from the Internet; • SCADA systems from the business premises; • SCADA remote diagnostic systems; • SCADA firewalls; • SCADA hosts; • SCADA gateways; • SCADA Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs); • SCADA Man Machine Interfaces (MMIs) or console systems; and • Telecommunications networks and their network management systems used for SCADA or DCS links.	SCADA or DCS systems are often of the highest criticality to an organisation. They are also often designed with little, or no, consideration given to security. For Critical National Infrastructure organisations in particular, the vulnerability of these systems should be closely examined.	SCADA or DCS systems are often safety critical. Testing should therefore be performed very cautiously. Often paper based tests or tests against exact replica systems are more appropriate. SCADA or DCS systems are often bespoke and highly specialised. Finding a provider with the skills to fully test a system can be difficult.

Category	Type	Description	Benefits	Limitations
Organisational	Integrated test	Performance of a penetration test as part of a series of tests to examine a number of aspects of an organisation's security. Such tests can provide senior management with an overall view of the organisation's security posture and its vulnerability to assessed threats. Such tests are often commissioned by board-level management and are conducted in secrecy, in order to obtain the best possible picture of overall organisational posture.	Provides a very dramatic and understandable picture of security for senior management, often to set the context for a strategic organisational security improvement programme.	Unless managed carefully, these tests can result in senior management overreaction and unpredictability in the event that findings indicate the organisation is at risk. In addition, since many staff will be unaware the tests are being conducted, staff morale may be adversely affected.
Supplier	Integrated Test	Performance of a penetration test as part of a series of tests of the effectiveness of the ISMS (or part of it) operated by an outsourced service provider.	Provides an understandable picture of the security posture of the provider, and can influence security improvements.	Requires supplier permission and cooperation. Many outsourcing service providers are unwilling to permit 3rd party penetration tests on their infrastructure.

TESTING PROCESS

Strategic test planning considerations

Integration with security and assurance framework

14. Penetration testing should form an integral part of an organisation's overall security and assurance framework. This includes a number of aspects:

- penetration testing requirements should be made explicit within organisational or system security policies;
- development processes should include penetration testing requirements as part of the systems development lifecycle;
- ongoing security management processes should include penetration testing requirements; and
- penetration testing should be used as a technique within an overall organisational or system-level assurance plan.

Testing frequency

15. Penetration testing schedules for existing infrastructure should be based on a risk assessment, considering business impact of compromise of the systems to be tested, the assessed level of threat to that system, and the amount of change to which the system is subjected. The schedule should also be influenced by the wider assurance plans for the organisation or systems concerned.

16. Vulnerability scans should be performed more regularly as part of an ongoing process.

17. Penetration tests are recommended when significant changes are made to systems or processes.

18. The organisation should schedule penetration tests as part of an assurance approach which helps ensure that security is maintained at an appropriate level. Organisations should avoid infrequent but dramatic penetration tests which cause security to vary wildly between insufficient security to over-provision of security following a penetration test.

Integrated testing

19. Penetration testing should be integrated into the systems development lifecycle (SDLC) within an organisation. Significant security testing may already be included within an SDLC; penetration testing should form an additional part of the process.

20. Penetration testing should be planned in the early stages of an SDLC where other testing is designed. However, the penetration test should be performed against infrastructure that is close to its live state as changes may invalidate any results that are found, requiring the test to be repeated.

Provider management models

21. Penetration tests are commonly provided by an external organisation using teams who specialise in penetration testing work. Larger organisations tend to maintain varying degrees of in-house capability, although this is often supplemented by external resources. However, the

nature of penetration testing means that it can be expensive to maintain an internal team that is required only periodically. As a result, the provision of penetration testing by an external provider is common practice.

22. The use of external providers can be managed in a number of ways that can be tailored to fit an organisation's style. Use of penetration testing providers tends to fall into the following models.

- Single provision – a single provider is used for all penetration testing. This can be beneficial since it can provide an extensive relationship where the provider is very familiar with your organisation and can therefore provide insightful and practical recommendations. The disadvantages are that a single provider may not be able to provide all types of penetration testing equally well. In addition, over-familiarity may give rise to conflicts of interest.
- Dual provision – two providers are used. Penetration tests are assigned according to the technical speciality of the provider, e.g. one provider for infrastructure testing and one for application testing. This retains the benefits of single provision while also playing to the strengths of the providers. The possibility of over-familiarity remains with this model.
- Testing panel – multiple providers are used. Penetration tests are either assigned in a cyclic fashion or according to technical speciality. The advantages of this model are that over-familiarity is less of a possibility and subsequent penetration tests on systems can be performed by different providers to make testing more thorough. The disadvantages are that the selection, contract maintenance and test management can be complex and expensive. Large organisations may also choose to invite competitive tenders from penetration testing providers to be on a 'call-off' contract framework. They then call off work against the framework, perhaps re-tendering the providers on the call-off framework for larger penetration tests.
- Ad-hoc – various providers are used dependent on the particular penetration test being performed. This model allows for flexibility and the ability to specifically select supplies based on their capability. However, providers are likely to have little or no familiarity with systems.

Test planning considerations

Test objectives, reporting, and expected resulting action

23. When planning a specific test, the scope and context should be carefully considered.

24. The test scope defines the systems or processes to be tested while the context determines the style of test and the types of test deployed.

25. The objectives of the test should be clear - the objective could be one or several of the following:

- provide an indication of the technical security of a system prior to going live;
- provide an indication of the overall security posture of key elements of a system or organisation's ISMS;

- test the technical configuration of a system, its security procedures and the response by a particular service delivery organisation;
- keep an IT organisation 'on their toes' by spot-testing from time to time; or
- cause a 'thunderflash' effect within the organisation's Board or audit committee to raise senior management awareness of the vulnerability of IT systems and the need for security investment.

26. The type of report and resulting action from the test should also be established. Depending on the test objective, the report or output may need to:

- provide a detailed technical report on the vulnerabilities of the system;
- explain the vulnerabilities in a way which is understandable by senior management;
- report the outcome of the test in business risk terms;
- identify short term (tactical) recommendations;
- conclude with and define 'root cause' long term (strategic) recommendations;
- include a security improvement action plan; and
- provide assistance to the organisation in implementing the security improvements.

27. The test objectives can therefore influence greatly the required competencies of the penetration testing service provider, and thereby the choice of the provider organisation.

Threat simulation

28. Test planning should consider the assessed threats to the organisation's information and systems. The results of relevant threat assessments that have been performed will help shape the context of the test. Often it is possible to cover a number of threats within a single penetration test.

29. It is important that the test remains realistic. It is not appropriate to use the most sophisticated possible attacks in a test when the system is assessed to be low business impact in nature, neither attractive nor exposed to attackers with strong motivations and technical capability. Likewise, it is also inappropriate to 'under-test' a high criticality system which faces a highly sophisticated threat.

Intrinsic threats

30. Test plans should be partly driven by the inherent level of threat. Some systems and processes are more exposed by their nature and purpose and therefore present a larger 'attack surface' to an attacker. For example, an Internet server hosting a number of services may be more exposed to attack than an internally facing system with restricted access.

Target criticality

31. The criticality of a particular system to the organisation should also drive test planning. A business impact assessment which evaluates the

requirement for confidentiality, integrity and availability of each candidate system should be performed.

32. ‘High impact’ systems should be given priority for testing.

Testing style

33. Careful consideration should be given to the style of testing that is required, black, grey or white box. The following terms have evolved to describe the testing style:

- ‘Black box’ – no information is provided to the penetration tester;
- ‘Grey box’ – limited information is provided, for example login credentials to an application or visitor access to a site; and
- ‘White box’ – full information is provided, for example network maps or access to development staff.

34. Black box testing is useful to understand what is possible for an uninformed attacker to achieve.

35. Grey box testing is useful to understand the degree of access that authorised users of a system can obtain.

36. White box testing is useful when performing a more targeted test on a system that requires a test of as many vulnerabilities and attack vectors as possible. Such tests are often accompanied by other forms of security review, for example code reviews of applications or system reviews of network infrastructure.

Testing depth

37. Part of the test context should set out the depth to which a penetration test is progressed. The generic testing methodology in section 2.1 shows that a comprehensive penetration test includes a combination of methods, tools and approaches.

38. The depth of a test, i.e. the extent to which the test is progressed through the methodology steps should be defined in advance of testing, with the implications of the approach understood.

39. Test depth can be restricted to vulnerability identification where an organisation seeks to understand the level of vulnerability on a particular set of systems. Where this is performed using largely automated tools, this approach is generally termed ‘vulnerability scanning’. This style of testing will not be able to determine whether manual techniques or attacks against other systems will be successful. This test depth can also result in numerous false positives.

Test risk management

40. There are a number of risks relating to penetration tests which should be managed. The table below sets out the key risks and provides suggested mitigations for these risks.

Risk	Suggested Mitigation
Disruption of safety or business critical systems	Perform tests against an exact replica of the system rather than the live system. Perform inspections of technical configurations, operating procedures and physical security rather than a technical test.
Disruption of systems[1]	Verify the effect of each test exploit against another similar system before using the exploit on a live system. Perform tests out-of-hours or during scheduled maintenance windows. Understand how to engage with service delivery organisations in emergency to restore services. Understand how to engage with organisational crisis management processes in the event of a major disruption. 24*7 contact information should be shared between the customer and the penetration testing provider.
Unclear authority to test	Ensure that the management commissioning the test have the appropriate authorisation to commission the test. Systems located in subsidiaries or joint-venture companies, systems owned or operated by service providers, systems located in other jurisdictions, or subject to other regulations may require other formal consents. Security testing may also require other authorisations within the organisation, such as from the Head of Internal Audit, the IT director, the Director of Security, the Chief Compliance Officer, or the Chief Information Security Officer. A 'Letter of Authority' should be obtained for any penetration test.

[1] Where tests are performed on production systems, it should be noted that a residual risk will remain. This residual risk should be accepted by the customer before the testing commences.

Risk	Suggested Mitigation
Inadvertent incident escalation	If tests are carried out in secret ensure that law enforcement or security authorities are not called by the part of the organisation under attack, believing the test is ‘for real’.
Loss of data	Verify that systems to be tested have been properly backed up, and that restore processes have been tested to work properly.
Inadvertent committing of an illegal act	Verify that the necessary legal risks have been considered, in discussion with the organisation’s Counsel. Areas for focus include, but are not limited to: • human rights legislation; • computer misuse legislation; • regulations governing investigatory powers; and • data protection legislation.
Organisational difficulties	Commissioning such a review may inadvertently trigger internal organisational sensitivities, create organisational tensions, create high emotion, loss of morale or cause difficulties with senior management.
Information sensitivity	Penetration test results can be extremely sensitive and require careful handling and security precautions to prevent unauthorised disclosure, e.g. through use of appropriately security cleared staff.

Penetration test provider selection

41. Selection of a suitable provider is essential to the execution of a successful test plan. Several aspects of a potential provider's profile should be examined before a selection is made.

Supplier capability

42. Penetration testing providers have different capabilities, and their suitability for a given test will depend on the objectives of the test and the required deliverables from the test. Service providers differ in:

- their technical capability in the various areas in which tests may be required (such as application testing);
- their ability to deal with the internal management aspects relating to test setup;
- their ability to resolve issues with IT service providers, and address global risk management issues;
- their ability to engage with senior management and report in business terms;
- their ability to issue an assurance report from which 3rd party reliance or positive assurance may be required;
- their capability to combine penetration testing with other forms of assurance;
- their ability to identify 'root cause' findings, strategically analyse findings in business terms, and co-develop security improvement strategies and programmes; and
- their ability to follow-through with a security improvement programme to address the fundamental 'root cause' issues.

43. Where UK Government systems, eg, those handling protectively marked information, are to be tested the supplier selection process may be narrowed through selecting providers who are members of the CHECK scheme (see Section 0).

44. A clear set of test objectives and requirements should be drawn up, and the capabilities of potential suppliers compared against those objectives and requirements.

45. There are a range of types of penetration testing service provider, including:

- small boutique firms specialising in penetration testing;
- information security consultancies and integrators, with penetration testing teams;
- systems integrators and outsourcing service providers with penetration testing teams; and
- regulated professional services firms, including the 'Big 4' accountancy firms, with penetration testing teams.

Methodologies

46. Examination of a test provider's methodology will provide an understanding of how a provider performs tests. There are a number of open source penetration testing methodologies that can be used as a reference when examining provider methodologies. Examples include:

- OSSTMM - Open Source Security Testing Methodology Manual (http://www.isecom.org/osstmm/); and
- OWASP - Open Web Application Security Project (http://www.owasp.org).

Staff

47. Penetration testing is a highly skilled activity and the quality of a test will depend on the capability of the staff involved in the test. Staff should be able to demonstrate experience in performing testing and technical expertise in a variety of technologies.

48. It may be appropriate to request staff CVs or to perform interviews unless the reputation of the firm itself can be relied upon. In addition, penetration testing staff may gain access to sensitive information and so should be required to demonstrate that they have undergone an appropriate level of security background checking.

Pricing

49. A provider's pricing will be a key factor in selection. An organisation should obtain indicative pricing for the types of test. Clearly prices will vary dependent on:

- the type of test;
- the scope;
- the amount of planning, preparation, and setup required by the service provider;
- the degree to which management of internal issues is to be performed by the service provider;
- the type of reporting required and the number of different reports; and
- the nature of post-test activity, including corrective action strategy co-development and security improvement programme planning.

Risk management

50. The risk management processes of a provider should be clearly understood before a test is undertaken. A provider should be able to explain:

- how tools and methodologies are tested before being used in live tests;
- how their operational risk management works during a test;
- how information is kept secure;
- how they take ownership of and guide customer management in their own internal risk management; and

- how their staff are recruited and subject to security background checks before being permitted to perform testing.

Qualifier tests

51. A useful technique to obtain a view of a provider is to invite them to perform a qualifying test. This is typically a small test of a low criticality or test system to determine how well the provider performs.

CHECK

52. CHECK is a UK government scheme operated by CESG, which is intended to assist public sector organisations and their suppliers in selecting providers and commissioning penetration tests. It was designed primarily for assurance of systems handling protectively marked information.

53. CHECK companies and their individual team members are assessed to ensure that they are capable of providing a high quality service. Members of the team must be British nationals (or as a minimum hold dual British nationality) and be able to obtain and hold an SC clearance. In addition at least one member must have passed the standard Network and Operating Systems Assault Course, which will give the individual Team Leader status. It will also give the company 'Green Light' status. 'Green Light' status means that a company is able to conduct work under the terms and conditions of CHECK. Another category known as 'Red Light' exists but the company does not have a Team Leader who has passed the standard Assault Course and therefore cannot carry out work under the terms and conditions of CHECK.

54. A test performed under CHECK terms and conditions is subject to certain requirements, including notifying CESG that a test is due to commence, that it is being led by a Team Leader who is present for the duration of testing and providing CESG with a copy of the report once the test is complete. CHECK providers are not required to perform all tests under CHECK terms and conditions, nor are customer organisations required to use CHECK terms and conditions for any particular test. However, if CHECK is to be used, potential customers should note that if the information is not Protectively Marked then they do not need to specify membership of CHECK in their invitations to tender, and may be challenged if equally competent non-scheme members are prevented from bidding.

55. Further information on CHECK as well as a list of current providers can be found at: http://www.cesg.gov.uk/site/check/index.cfm.

Test management

Test management role

56. Test management is a significant responsibility, particularly where an organisation performs a large number of penetration tests. It is recommended that the customer to include responsibility for management of testing in the role of a suitable member of staff. The member of staff can then act as a single point of contact for test providers and can help ensure continuity for the testing process.

Contracts

57. Where tests are obtained from an external provider a contract will need to be executed. Further information on the security considerations for outsourcing contacts can be found in the NISCC Good Practice Guide, The Security Governance Framework for IT Managed Service Provision.

58. The nature of the contract will depend on several factors including the provider management model in use, as described above. Contracts are often proposed by the provider and include:

- scope as determined through planning;
- testing style and test depth to be adopted;
- outline of methodology to be used;
- operational risk management considerations:
    - points of contact;
    - agreed hours of testing;
    - explicit exclusions;
    - responsibilities for internal risk management;
    - specific regulations to be complied with;
- reporting and presentation style and timing;
- post-test corrective action strategy and action plan development;
- pricing; and
- terms of business.

59. The contract should always be referred to a legal team to ensure that the terms of business and the detail of the contract and schedule of work are acceptable, as penetration testing providers often caveat risks, require customers to acknowledge that they understand penetration testing involves an element of risk, and seek indemnities from the customer.

Test preparation

60. Preparation by the customer is needed to help ensure the test progresses effectively:

- information such as target addresses and authentication credentials should be supplied in advance of testing;
- target systems should be available for testing when tests are due to start;
- relevant staff should be notified;

- appropriate site access should be arranged;
- relevant authorisations and contracts are in place; and
- physical network access should be available for on-site visits.

Test execution

61. The customer's penetration testing manager should be available to deal with any issues that arise while the test is taking place. The manager should have a senior counterpart they can contact at any time in the penetration testing provider who is accountable for managing the delivery of the test.

Reporting

62. Effective reporting is a critical aspect of penetration testing and its importance is often overlooked. Reporting style should be considered as part of the test planning process and reporting requirements should be written into the contract.

63. Ongoing communication during tests can take the form of regular updates or alerts where a serious vulnerability has been discovered.

64. Written deliverables can consist of reports or presentations. In either case, the deliverable should include the following sections:

- Background – summarising the test plan
- Executive summary – presenting the results in a business risk context, highlighting particular concerns, any patterns, and a high-level statement of the required form of the corrective action.
- Findings table – describing each finding in non-technical, business context.
- Findings table – technical content describing:
  - the vulnerabilities found;
  - the associated technical risk; and
  - remediation steps.
- Test narrative – a description of the process that the tester used to achieve particular results. This can be helpful where an exploit was the result of several vulnerabilities.
- Test evidence – this may be presented as an appendix or only available on request. The evidence should include results of automated testing tools, screen shots of successful exploits or other 'trophies'.

65. It is often helpful to ensure that suppliers use a common reporting template. This enables organisations to more readily compare results from different providers.

Remediation

66. After the test is complete it is often the responsibility of the organisation's test manager to ensure that the results are acted upon. The report should be disseminated to the relevant staff and the remediation of the identified vulnerabilities and associated 'root causes' should begin.

67. Each remedial step should be assigned an owner with an associated expected completion date.

68. In some cases, especially where the issues relate to fundamental ‘root causes’, the test manager may require the penetration testing provider to involve qualified and experienced security professionals to assist the organisation in defining the corrective action strategy and plans.

TERMINOLOGY

69. A number of terms are used related to penetration testing, some of which can cause confusion. This section is intended to clarify some commonly used terms.

General

- Port scanning – part of reconnaissance or enumeration during a network infrastructure test. A tool is used to establish the services (such as file sharing, web or email) being offered by a system.
- Vulnerability scanning – identifying vulnerabilities using automated tools that search for known problems.

‘Boxes’

- Black-box – testing with no knowledge of the target.
- Grey-box or translucent box – testing with partial knowledge of the target.
- White-box or crystal box – testing with complete knowledge of the target.

‘Teams’

- Tiger team – originally a term to describe coordinated penetration test teams, often performing physical tests against military installations. Now sometimes used to describe security incident response teams.
- Red team – a penetration test. The term can be used to describe a particularly aggressive testing style or tests where only senior staff are aware of testing.
- Blue team – a security review to determine the existence of policies, plans, processes, and procedures. The term can be used to describe those responding to attacks during a test, such as IDS analysts.
- White team – a security review to determine the completeness and implementation of policies, plans, processes, and procedures. The term can be used to describe the “referees” of a test that capture the process and outcomes, though this is rare.