Penetration testing

How to get the most from penetration testing

Introduction

Penetration testing is a core tool for analysing the security of IT systems, but it's not a magic bullet.

This guidance will help you understand the proper commissioning and use of penetration tests. It will also help you to plan your routine security measures so that you gain maximum benefit from this powerful but expensive operation.

What is penetration testing?

For the purposes of this article, we will define penetration testing as: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."

Penetration testing should be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities.

A penetration test should be thought of as similar to a financial audit. Your finance team tracks expenditure and income day to day. An audit by an external group ensures that your internal team's processes are sufficient.

Pen-testing: the ideal

In an ideal world, you should know what the penetration testers are going to find, before they find it. Armed with a good understanding of the vulnerabilities present in your system, you can use third-party tests to verify your own expectations.

Highly experienced penetration testers may find subtle issues which your internal processes have not picked up, but this should be the exception, not the rule. The aim should always be to use the findings of a penetration test report to improve your organisation's internal vulnerability assessment and management processes.

What should a penetration test tell you?

Typically, penetration tests are used to identify the level of technical risk emanating from software and hardware vulnerabilities. Exactly what techniques are used, what targets are allowed, how much knowledge of the system is given to the testers beforehand and how much knowledge of the test is given to system administrators can vary within the same test regime.

A well-scoped penetration test can give confidence that the products and security controls tested have been configured in accordance with good practice and that there are no common or publicly known vulnerabilities in the tested components, *at the time of the test*.

What sort of system should be tested?

Penetration testing is an appropriate method for identifying the risks present on a specific, operational system consisting of products and services from multiple vendors. It could also be usefully applied to systems and applications developed 'in-house'.

For product-specific testing, it is not an appropriate technique.

Using penetration testing effectively

A penetration test can only validate that your organisation's IT systems are not vulnerable to *known issues on the day of the test*.

It's not uncommon for a year or more to elapse between penetration tests. So, vulnerabilities could exist for long periods of time without you knowing about them if this is your only means of validating security.

Third-party penetration tests should be performed by qualified and experienced staff only. By their nature, penetration tests cannot be entirely procedural, an exhaustive set of test cases cannot be drawn up. Therefore, the quality of a penetration test is closely linked to the abilities of the penetration testers involved.

The NCSC recommends that HMG organisations use testers and companies which are part of the CHECK scheme.

Types of testing

Penetration testers can be used to perform a wide-range of testing. The following list is illustrative, not comprehensive.

+ Show All

1. Test basis

+ Show

Tests can be carried out by testers armed with varying amounts of information about your system:

- ***Transparent or Open box testing*** - Full information about the target is shared with the testers. This type of testing confirms the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems.
- ***Opaque or Closed box testing*** - No information is shared with the testers about the internals of the target. This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets. This more accurately models the risk faced from attackers that are unknown or unaffiliated to the target organisation. However, the lack of information can also result in vulnerabilities remaining undiscovered in the time allocated for testing.

2. Test type

+ Show

Each of the tests described below can be run as either a opaque/closed box or transparent/open box operation:

- ***Vulnerability identification in bespoke or niche software*** - Most commonly used in web applications. This type of testing must give feedback to developers on coding practices which avoid introducing the categories of vulnerability identified.
- ***Scenario driven testing aimed at identifying vulnerabilities*** - The penetration testers explore a particular scenario to discover whether it leads to a vulnerability in your defences. Scenario's include: Lost laptop, unauthorised device connected to internal network, and compromised DMZ host, but there are many others possible. You should consider, based on previous incidents, which scenarios are most relevant to your organisation.
- ***Scenario driven testing of detection and response capability*** - In this version of scenario driven testing, the aim is to also gauge the detection and response capabilities your organisation has in place. This will help you understand their efficacy and coverage in the particular scenario. This is an area of current work by the NCSC, further information will be available shortly, please contact us if you have a particular need in this area.

Note

If you have a particular scenario that requires additional assurance, a specifically targeted penetration test may be a good way to obtain that assurance. A suitably qualified penetration testing team will be able to guide you through the selection and scoping process required in this case.

Your testing regime

It's critically important to note that a planned penetration test doesn't mean your normal testing regime should cease to include security tests on the target system. Functional testing of security controls should still occur.

Assessing whether defined security controls are functioning is not a valuable use of penetration testing resources.

A functional testing plan should always include **positive tests** (such as 'The logon box comes up every time you try to log in and you aren't just allowed in').

Negative testing may be included in your functional testing plan where the skills to perform it are available within your organisation (for example, verifying that 'You can't log in without the correct password').

A model penetration test engagement

A typical penetration test will follow this pattern: Initial engagement, scoping, testing, reporting and follow up. There should be a severity rating for any issues found.

For this model we assume that:

- you wish to know what the impact of an attacker exploiting a vulnerability would be, and how likely it is to occur
- you have an internal vulnerability assessment and management process

Initial engagement of the external team

You should ensure that the external team has the relevant qualifications and skills to perform testing on your IT estate. If you have any unusual systems (mainframes, uncommon networking protocols, bespoke hardware etc.) these should be highlighted in the bid process so that the external teams know what skill sets will be required.

+ Show All

Scoping + Show

Scoping a penetration test should involve:

- all relevant risk owners
- technical staff knowledgeable about the target system
- a representative of the penetration test team

Where the goal of the test is to ensure good vulnerability management:

- risk owners should outline any areas of special concern
- technical staff should outline the technical boundaries of the organisation's IT estate
- the penetration test team should identify what testing they believe will give a full picture of the vulnerability status of the estate

Assuming you have one, a current vulnerability assessment should be shared with the testers at this stage. Testing can then be designed to support a reasonable opinion on the accuracy and completeness of the internal vulnerability assessment.

Special requirements

During scoping, you should outline any issues which might impact on testing. This might include the need for out-of-hours testing, any critical systems where special handling restrictions are required, or other issues specific to your organisation.

Plan of action

The output of the scoping exercise should be a document stating:

- the technical boundaries of the test

- the types of test expected
- the timeframe and the amount of effort necessary to deliver the testing - usually given in terms of resource days
- depending on the type of approach agreed, this document may also contain a number of scenarios or specific 'use cases' to test
- the penetration testing team's requirements - this will allow you to do any necessary preparation before the date of the test (for example, by creating test accounts or simply allocating desk space)
- any compliance or legislative requirements that the testing plan must meet
- any specific reporting requirements, for example the inclusion of CVSS scores or use of CHECK severity levels
- any specific time constraints on testing or reporting, that a penetration testing company will need to consider when allocating resources

Testing

+ Show

Staying in contact

During the test phase, you should ensure that a technical point of contact is available at all times. The point of contact does not need to spend all their time working with the test team but should be available at short notice. This allows the test team to raise any critical issues found during testing, and resolve problems which are blocking their testing (such as network misconfiguration).

Taking care

The testers should make every effort to avoid causing undue impact to the system being tested. However, due to the nature of penetration testing, it's impossible to guarantee that no unexpected reactions to testing will occur.

Changing scope

During a penetration test or security assessment, the testing team may identify additional systems or components which lie outside of the testing scope but have a potential impact on the security of the system(s) which have been defined as in scope.

In this event, the testing team may either suggest a change to the scope, which is likely to alter testing time frames and cost, or they may recommend that the exclusion of such components be recorded as a limitation on testing.

The decision on which would be the preferred option will generally be down to the risk owner, with the penetration team responsible for clearly articulating the factors to consider.

Reporting

+ Show

The test report should include:

- any security issues uncovered
- an assessment by the test team as to the level of risk that each vulnerability exposes the organisation or system to
- a method of resolving each issue found
- an opinion on the accuracy of your organisation's vulnerability assessment
- advice on how to improve your internal vulnerability assessment process

A debriefing can also be useful. At this meeting the test team run through their findings and you can request further information or clarification of any issues.

Severity rating

+ Show

When rating vulnerabilities it is common for penetration testers (often at customer behest) to use the Common Vulnerability Scoring System which attempts to give a numerical score identifying the severity of a vulnerability.

To simplify this measurement, CHECK reports are required to state the level of risk as HIGH, MEDIUM, LOW or INFORMATIONAL in descending order of criticality. For CHECK reports, scoring systems such as CVSS may be used in addition to (but not in place of) this.

Whilst vulnerabilities are ordinarily categorised at one of these levels in a consistent manner, exceptions can sometimes occur. For example, other mitigating controls in place could minimise the effectiveness of a vulnerability, or the presence of additional vulnerabilities could have a synergistic effect.

Any deviation from associating a vulnerability with its standard rating should be documented and justified by the penetration testing team.

Follow up on the report

+ Show

1. Do your own assessment

The penetration test report should be assessed by your organisation's vulnerability management group in a similar manner to the results of an internal vulnerability assessment.

The penetration test team will have rated each issue found and given a potential solution. However, it's important to note that *risk assessment and decisions on the application of fixes are your responsibility.*

The test team may not have had access to all details about a specific system or the potential business impact of the exploitation of a vulnerability. Consequently, they may rate issues either lower or higher than you. This process of assessing vulnerability levels should not be used to downplay issues - it should be a process of looking at issues and identifying the risk to your organisation.

2. Previously unknown vulnerabilities

Any vulnerabilities identified by the penetration test which you did not previously know about should be given special attention, with the aim of identifying ways in which you might go about spotting such issues in future.

3. Choosing solutions

The solutions proposed by your penetration testers may not be the only ones possible. You should take advice from your own technical staff and suppliers on alternatives.

As an example, imagine your pen testers have suggested patching a piece of software. You should ask yourself, *'Is this the only solution to the problem?'* It may be possible to simply uninstall the software if it's not actually required, or other controls could be put in place to limit exposure to the vulnerability. It may even be that additional monitoring of the vulnerable component is sufficient to reduce the risk to an acceptable level.

Vulnerability risk assessment and mitigation is a business process and should not be wholly outsourced to the test team.

PUBLISHED

8 August 2017

REVIEWED

10 January 2022

VERSION

1.0

WRITTEN FOR

Cyber security professionals Large organisations Public sector Small & medium sized organisations