Penetration Testing

Many organisations are looking to have some form of penetration testing performed on their systems. This may simply be to evaluate existing security measures and to find gaps where security needs improvement, but increasingly it is performed to comply with security standards when connecting to public sector networks or processing payment details.

What is penetration testing?

Penetration testing is a method for evaluating the security of an information system by simulating the types of attack that are known to occur in the wild. The process can vary widely according to the requirements and purpose of the testing. Even the name given to this type of testing can vary widely - Vulnerability Assessments and IT Health Checks are two common terms.

During testing, assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system or network. This often involves launching attacks on real systems and data that use tools and techniques commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain greater access than could be achieved through a single vulnerability. Penetration testing can also be useful for determining:

- how well the system tolerates real world-style attack patterns
- the likely level of sophistication an attacker needs to compromise the system successfully
- additional countermeasures that could mitigate threats against the system
- defenders' ability to detect attacks and respond appropriately.

What sort of testing do I require?

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. The testing may be needed for connection to a particular network and the precise nature of the testing will depend on the requirements for that network. The depth and breadth of the testing performed will vary according to your requirements so make sure that these are clear before you consider any testing. You may just require a simple vulnerability scan of your external networks, or you may need many hours of involved manual testing. The expenses will vary accordingly.

The industry generally acknowledges three distinct types of testing:

White box

The testing team has complete carte blanche access to the testing network and has been

supplied with network diagrams, hardware, operating system and application details etc. prior to a test being carried out. This does not equate to a truly blind test but can speed up the process a great deal and leads to more accurate results being obtained. The amount of prior knowledge leads to a test targeting specific operating systems, applications and network devices that reside on the network rather than spending time enumerating what could possibly be on the network. This level of information can allow a tester to focus on specific areas of interest and systems that are more likely to be vulnerable to attack. This type of test equates to a situation whereby an attacker may have complete knowledge of the internal network.

Grey box

The testing team would simulate an attack that could be carried out by a disgruntled, disaffected staff member. The testing team would be supplied with appropriate user level privileges and a user account, and access granted to the internal network by relaxation of specific security policies present on the network i.e. port level security. For example, testing using authenticated access to a web application can provide more information on the security of an application than a black box test which may just end up testing the security of your authentication.

Black box

No prior knowledge of a company network is known. In essence an example of this is when an external web- based test is to be carried out and only the details of a website URL or IP address are supplied to the testing team. It would be their role to attempt to break into the company website / network. This would equate to an external attack carried out by a malicious hacker, but due to time constraints this may not be a thorough test of the security of a network or system.

Most companies charge an hourly rate so it is worth remembering that for grey and black box testing, you will be paying testers to discover information that you could have provided them. On a per-hour basis, white box testing is often more cost effective.

Can we perform this testing ourselves?

It is recommended, if you are able to, that you assess and improve the security of your network using the tools and skills available to you before you bring in a third party. By removing some of the more obvious security threats you will get more value for money from the testing.
Where penetration testing is being done solely as part of an internal process to improve the security of your network you could undertake the entire process yourself. If the testing is being done to comply with third party requirements it is almost certain that the requirements will stipulate third party testing.

What are the common standards that require penetration testing?

PCI-DSS (Payment Card Industry Data Security Standard) This standard requires both a wide scoped internal and external vulnerability assessment but also a penetration test that attempts to exploit the vulnerabilities and gain access to systems. The organisation performing the testing need not be the same as your QSA (Qualified Security Assessor) and

may even be an internal team if they can be shown to be independent and suitably qualified.
GSI (Government Secure Intranet) Code of Connection Penetration testing forms part of an ‘IT Health Check’ and is required for connection to Government Secure Networks. It is not required, but strongly recommended that testing is performed by a CESG (Communications-Electronics Security Group) CHECK qualified service provider.

What qualifications should we look for in our penetration testers?

CHECK is a series of qualifications that certify the holder is competent to perform IT Health Checks on government systems. Both individuals and companies can be certified, with individuals being qualified at Team Leader or Team Member status. CHECK holders must also hold at least Security Check (SC) clearance, allowing them to work on systems that process information marked up to CONFIDENTIAL.

CREST provides a series of assessments for penetration testers and has been targeted more at the commercial world. The qualifications are now also valid as an equivalent to CHECK, and holding the relevant CREST accreditations and SC clearance will allow you to be CHECK accredited. CREST provides separate assessments for both web applications and infrastructure, and now offers an entry level ‘registered tester’ status, which is equivalent to the CHECK Team Member qualification.
Tiger Scheme is an industry consortium who provides a number of qualifications with testing managed by the University of Glamorgan. Its qualifications have been recognised by a number of organisations and companies throughout the UK. CESG accept the Senior Security Tester (SST) Tiger Scheme assessment as equivalent to the technical aspect of a CHECK Scheme Team Leader qualification and the Qualified Security Tester - Team Member (QSTM) as the equivalent to the CHECK Scheme Team member qualification.
What do we need to look for in a penetration testing company? Ask other organisations for recommendations of companies they have previously used. Make sure that the company has wide and current experience in your sector and in the type of testing you are looking for. Ask the company for references from recent customers and follow these references up. Some companies may offer discounts for academic and public sector customers.

What information will I need to give our penetration testers?

Many companies offer a range of tests that vary in the amount of information that is provided to them. ‘White box’ testing entails providing full information, while ‘Black box’ testing presumes that the attacker has no privileged knowledge about the systems. Our recommendation is that the former is more beneficial to most organisations and since you are paying for time, it also provides the best value for money.
Typically you will be required to provide as much information as possible on the networks you wish to be tested: IP ranges, domains, URLs of applications, which systems and applications you consider key, and what IP addresses and systems should be avoided.
A main point of contact within the organisation, who is readily available, should also be agreed with the testing team before the testing takes place in case of any problems the tester(s) encounter.

All of the information regarding the testing process should be compiled into a document by the testing company and should be signed off by a person within the organisation with the relevant authority before any testing should take place.

What else do I need to do to prepare?

In preparing for an assessment, users and administrators sometimes modify settings to make their systems more secure, resistant to attack, or compliant with policies and other requirements. While this can be viewed as positive, changes made under these circumstances are often only maintained for the duration
of the assessment, after which the systems are returned to their previous configurations. Providing no advance notice of assessments to users and administrators helps to address this challenge. Many organisations perform occasional unannounced assessments to supplement their announced assessments. As security weaknesses are identified during an assessment, administrators may want to take immediate steps to mitigate them and expect assessors to re-assess the system quickly to confirm that the problems have been resolved. Although this desire for quick mitigation is admirable, assessors should communicate the importance of following the organisation's change management policies and procedures.
Security assessment is often incorporated into development or deployment with little notice and narrow timeframes. With advanced planning it can be made a regular part of the development or deployment cycle.
Time is a challenge when testing critical systems and networks that are in production: if testing techniques have the potential to cause loss of availability or other problems, then systems and networks may need to be tested out of hours. Remember that assessors are often restricted to testing timeframes while real attackers are not limited by such constraints. Similarly, if you use any Intrusion Detection Systems (IDS), make sure that they are disabled, or the testing systems white listed, so that their operation does not impact the testing and prevent the full extent of a vulnerability being explored. Testing of an IDS should normally be considered separately.

During an assessment, the organisation's incident response team may detect an incident. This could be caused by the assessors' actions, or by a real adversary that happens to perform an attack while the assessment is in progress. The incident response team or individual discovering the incident should follow the organisation's normal escalation procedures, and assessors should follow the guidelines set forth by the testing plan. It is recommended that assessors stop assessing the systems involved in the incident while the organisation carries out its response.
If testing is taking place from an external network, make sure that you notify Janet CSIRT and any other network operators involved.

What do I need to tell my users?

Testing often faces resistance. Resistance to assessments can come from many sources within an organisation, including system and network administrators and end users. Reasons may include fear of losing system or network availability, fear of being reprimanded, inconvenience, and resistance to change. Obtaining upper management approval and support will help resolve problems related to resistance. Incorporating security assessments into the organisation's overall security policy will help establish a process that does not surprise administrators and users.

It is imperative that people within the organisation are aware that testing will be taking place.
