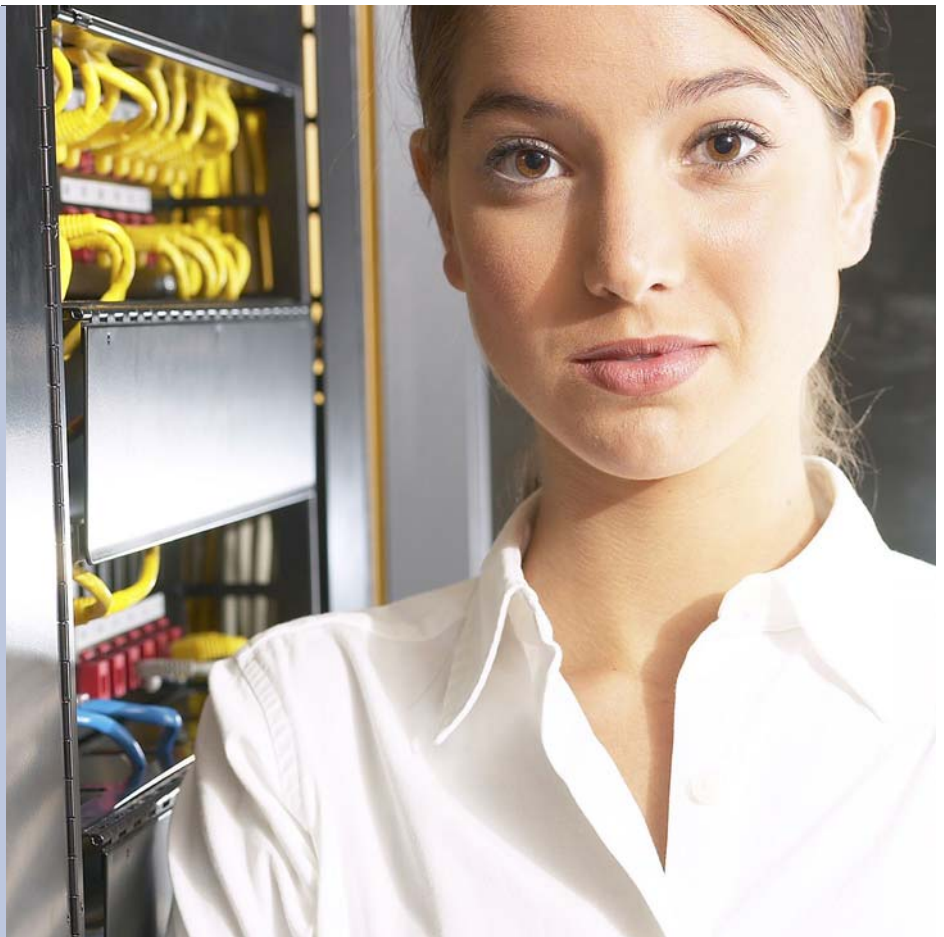


# Penetration Testing



## Why a methodical and proven approach to penetration testing is essential in formulating an effective security testing strategy

This white paper explains the methodology and ethos behind penetration testing. It discusses why penetration testing is not merely the serial execution of automated tools and generation of technical reports that it is frequently viewed as.

It also illustrates why professional penetration testing can provide substantial value to an organisation by providing clear and concise direction on how to secure an IT infrastructure from real world attacks.

### **Establishing objectives**

The goal of penetration testing is to identify the exploits and vulnerabilities that exist within an organisation's IT infrastructure and to help confirm the effectiveness – or ineffectiveness – of the security measures that have been implemented.

Indeed, there is rarely a better way to justify additional funding for security controls than by physically demonstrating the flaws that exist in operational systems. A board of directors will instantly appreciate the value of security once

they've witnessed the exposure of confidential information by a successful penetration test.

It's important, though, that penetration testing should model real world attacks as closely as possible. In practice, whilst a real world attacker would typically spend many months researching a target, a penetration tester will rarely be afforded this luxury. They need to complete, in several days, the activities that a real attacker would spend considerably longer conducting.

This is why it is both useful, and good practice, to examine the internal configuration of systems before attempting an external penetration test. It enables the tester to quickly gain an insight into an organisation's IT infrastructure and to model the months of research an attacker would expend on creating a knowledge base about a potential target.

### **Threats and attack profiles**

Threats come from many different sources. In practice, around 70% are either internal incidents or are accidental or

malicious in nature. The remaining 30% are the result of externally-related incidents.

The most serious security breaches are, more often than not, carried out by insiders who have taken advantage of their intimate knowledge of a company's systems.

Penetration testing should, therefore, model the attack profiles of potential threat sources in order to accurately determine the possibility of an attack succeeding. These are often split down into several, clearly defined categories and are listed below in *Figure One*.

Each of the individuals described have different attack profiles and these have to be carefully modelled in order to re-create attack scenarios that are as realistic as possible.

### Testing models

There are two distinct models for penetration testing - the *Zero Knowledge* test and a *Full Knowledge* test. With the former, the tester is given no insight into the target systems under investigation. With a *Full Knowledge* test, however, the tester is given complete information about them.

Zero Knowledge tests are useful when trying to ascertain how vulnerable

**Script Kiddie** Has limited or no knowledge of how computer systems work. They rely on pre-written exploits and vulnerability scanners to find and realise vulnerabilities.

**Master Cracker** Has intimate knowledge of IT technology and system code. They find original vulnerabilities, write customised exploits and spend much of their time learning and finding flaws in new technology.

**Malicious Insider** Does not necessarily know much about IT systems but does know a lot about YOUR system. This enables them to attack a system at its most vulnerable point.

**Naive employee** Generally damages IT systems through an inability to correctly operate even the most simplest applications.

Figure One: Profiles of potential attackers

systems are from the attack profile of the Script Kiddie. These are the most common type of attackers and are generally regarded as no more than Internet vandals. They typically attack the easiest targets they can find and with complete disregard. They rarely conduct any research and normally start an attack as soon as the target is acquired.

A Full Knowledge attack sets out to accurately model the attack characteristics of a Master Hacker or Malicious Insider. This is because both of these individuals will already know a great deal about an organisation's systems (Malicious Insider) or will carry out extensive research (Master Hacker) in order to identify the best ways of attacking a system.

### Method

All penetration tests use a similar methodology regardless of the actual attack profile that is being simulated.

Target acquisition is the process by which the tester gains as much information about a target as possible. This can be done in several ways such as scanning a web site for names, photographs or contact telephone numbers.

The use of online whois databases can often retrieve vast amounts of information such as system administrator IDs and network addresses. Services such as Companies House can also offer pertinent information regarding management employees.

Once the network location has been identified, the tester can then utilise port and network scanners to identify available services and the topology of a network. Tools such as *nmap*, *fping* and *icmpquery* provide a plethora of information which can additionally be used to develop a plan of the network.

Nmap provides the functionality for TCP fingerprinting and can be used to help identify the operating system running on a particular network server. It can often even reveal the release version that is currently in use.

Enumeration is the process of attempting to obtain user names, network share and application version information from the services running on a server (eg. Apache 1.3.X, BIND 8.2.1). It's achieved through

the interrogation of network systems and banner grabbing or may involve the use of tools such as *gnit* and *netcat* in order to more intrusively retrieve system information from hosts.

### Exposing vulnerabilities

Once the tester has built up a satisfactory library of system information, the vulnerabilities have to be found. This can be performed by manually matching the applications present to publicly available vulnerability lists such as CERT (Computer Emergency Response Team) and Bugtraq.

Using this manual method results in a long and drawn out procedure. Automated tools such as ISS's vulnerability scanner are available, however, and these can rapidly provide a comprehensive list of the vulnerabilities that exist on a target system.

Whilst useful, tools such as these are unlikely to identify the most critical vulnerabilities that affect a specific system. After all, every IT system is unique and vulnerability scanners rarely take this into account. What this means in practice, is that the value of automated tools is superseded by the experience and guile of an experienced penetration tester.

### Stepping outside of the box

Automated tools are designed to operate under the same set of rules as the test target. It is only by stepping outside of this environment that it becomes possible to find 'holes' in a system. The penetration tester must, therefore, be prepared to step outside of the problem rather than merely operating within it.

This, in fact, is one of the main differences between Script Kiddies and penetration testers. Script Kiddies will often pass over this aspect of testing by adopting a 'shotgun' approach compared to the 'scalpel' technique of the penetration tester. Script Kiddies will utilise every resource at their disposal without any concern as to whether they work. As long as one of the scripts succeeds, they rarely care about the rest.

The penetration tester, however, has a full list of potential vulnerabilities and

system information and this can be used to select exploits that will be run against the target system. The user names and passwords – collected at the enumeration stage – now become useful as they can be employed to gain access to the target.

Once the penetration tester has access to a system, other vulnerabilities that exist within the operating system can be used to gain root or administrator privileges. Once this is achieved, the tester can procure a suitable 'trophy' to illustrate the impact of a potential intrusion.

### Not a panacea

Organisations should always realise the limitations of penetration testing. The results of a test only provide a snapshot of a system's security at a given time. New vulnerabilities appear with alarming frequency and regular testing needs to be undertaken.

Furthermore, a penetration test is only as good as the tester conducting it and a services provider should be chosen wisely to ensure a consistent and high level of service. Conversely, organisations should not necessarily criticise a tester that fails to achieve any results. After all, the best outcome of a test is one that confirms that system security cannot be compromised.

### Conclusions

No matter what the threat, a professional penetration test should accurately model the attack characteristics of the profiles discussed. A methodical and scientific approach should be used to successfully document a test and create reports that are aimed at different levels of management within an organisation.

Finally, penetration testing should never be regarded as a one-off service. Systems change, threats emerge and business strategies evolve. Testing should be repeated at frequent intervals and particularly following major changes to an IT infrastructure. It's also important to remember that penetration testing is but just one form of testing and any organisation should develop an overall security testing strategy that is tailored to the threat models and security policies of their organisation.

