



**Penetration Testing – How to Obtain a Real Security
Dividend**

Safecomms White Paper

Prepared by Nick Gifford

Managing Director

(02) 8234 4000

nick.gifford@safecomms.com.au

Sydney, 20th February 2005

Version 1

Table of Contents

Table of Contents.....	2
Introduction.....	3
What Value Should Penetration Testing Bring?	5
Targeting The Right Assets.....	7
Online Share Trading Company.....	7
The Pharmaceutical Company	8
The Internet Services Provider ("ISP").....	8
Using The Same Approach As A Black Hat Hacker.....	10
Network Attacks.....	10
Web Application Attacks.....	10
Wireless Attacks.....	11
Social Engineering	11
Physical Security Attacks.....	12
Telephony Systems Attacks.....	12
The Compromise.....	12
Hacking Skills Equivalent To A Real Attacker.....	13
Script Kiddies.....	13
Sophisticated Hackers	14
The Cost Dimension.....	16
Diminishing Returns.....	16
Identifying The "Acceptable Risk" Point.....	16
Indicators Of Time Frames For Penetration Tests.....	17
Educated Attacks and Blind Attacks.....	18
Differential Tests.....	18
After The Test Is Done.....	20
The Executive Summary.....	20
Remediation Treatments.....	20
Conclusion.....	22

Introduction

Penetration Testing (or “ethical hacking” as it is sometimes called) is the act of testing the security of your information assets by inviting a trusted third party to try to breach that security using the same techniques that an authentic hacker would use. The aim of this process is to ensure that potential weaknesses in your security are identified and can therefore be addressed before your security is compromised for real by an attacker.

Whilst obtaining hard data on hacking is notoriously difficult (many organisations who are victims of hacking are reluctant to disclose any details), there is nonetheless sufficient information from government surveys, police anti-fraud investigative bodies and other special interest groups to draw a reasonable picture of current trends. Whichever surveys you read and whoever you talk to in the IT sector, there is a strong consensus on the following points:

- There has been a very significant increase in hacking activity over the last 18 months
- Whereas hacking was previously mainly carried out by “script kiddies” out to cause mayhem and embarrassment, things have recently taken a far more sinister turn as the criminal fraternity has worked out that “you can now steal more with a computer keyboard than you can with a firearm”
- Whilst traditionally attacks were randomly targeted, making all Internet citizens potential targets, hacking is now far more likely to be specifically targeted at a particular organisation

“Making sure we do not get hacked” is therefore a major priority these days for most CIO’s and IT Managers. In this climate, you would therefore expect that penetration testing, which is specifically designed to proactively thwart hackers, would be a core activity in most organisations – but it’s not. Why is this so?

The truth is that many CIO’s and IT Managers regard the value of penetration testing as highly questionable. In particular, a frequently recurring sentiment is summarised in the following statement:

“I’ve spent quite a lot of money on having a penetration test, and I’ve fixed the vulnerabilities that they found, but I still don’t know whether my organisation is secure – and the blokes who did the test can’t give me any guarantees either.”

This statement raises several fundamental issues, and by analysing those issues we will answer the following key questions:

- What value should a penetration test bring to the organisation?
- What are the limitations of penetration testing?
- How do you maximise the probability that you will significantly increase the security of your organisation through penetration testing?

As we develop the arguments set out in this White Paper, we will simultaneously seek to demystify the whole subject of penetration testing. By and large, the information security industry has done a poor job in explaining what penetration testing is, how it works, and how the organisation and the tester should best work together to ensure a valuable result. It is high time this omission was addressed.

What Value Should Penetration Testing Bring?

We are all familiar with the old cliché that “security is not an absolute”. Any organisation that plays in the online world is ultimately at risk of having their security compromised – no matter how diligent they are in implementing security measures. “Zero day exploits” and human weaknesses ensure that there will always be a possibility of a security breach in even the best run organisations. (It is for this reason that organisations must concentrate on having a layered security approach, assuming that breaches will occur, and focused on the containment of these breaches).

However, whilst a state of “guaranteed” security can never be attained, organisations do need to get their security to a level where the level of risk is acceptable for that organisation. In other words, whilst no CIO or IT Manager can look their CEO in the eye and say “I can guarantee you we are totally secure”, they should be able to say “we have taken the right steps to ensure that the probability of our organisation being successfully hacked is very low, and we regard the residual risk level as acceptable”.

Penetration testing has a key role to play in minimising the risk of an organisation’s online presence. However, in order to do so it is necessary that:

- The penetration testing is risk focused, specifically targeting those assets that represent the greatest risk to the organisation
- The penetration testing is conducted in the same manner that would be utilised by a would-be attacker
- The penetration testing is carried out by an ethical hacker who is at least as skilled as a future would-be attacker

If these three conditions are met, then once the testing has been completed and appropriate measures have been taken to deal with the weaknesses identified, the CIO or IT Manager should be able to feel a high level of confidence that:

- the likelihood of the organisation being successfully hacked is sufficiently low that the risk is acceptable; and
- that if an attack is successful, the consequences of that attack will be sufficiently minor so as to render the risk acceptable.

Of course, there is an additional dimension that has to be constantly taken into account – cost. Properly conducted penetration testing requires the time and expertise of highly skilled professionals and can be costly as a result. The size (and therefore the cost) of the penetration test needs to be commensurate with the level of risk faced by the organisation, and needs to be

affordable. This in turn means that the money must be spent on testing the areas that are most at risk, and focused on testing the methods most likely to be utilised by today's hackers.

It is worthy of note that poorly conducted penetration tests can in fact increase the levels of risk an organisation faces, as they can create a false sense of security.

If these principles were universally understood and acted upon, penetration testing would undoubtedly be a very effective weapon in the fight against the hacker, and would be regarded as an essential cornerstone of just about every organisation's security strategy.

In the next sections of this White Paper we explain how to apply the principles identified above.

Targeting The Right Assets

The first step in scoping a penetration test must be to determine which information assets are most at risk. This can be viewed from two different perspectives:

- which information assets, if compromised, would cause greatest loss or damage to the organisation?; and
- which information assets are hackers most likely to attack?

In the vast majority of cases these two questions will yield the same answers, but this will not always be true. From a prioritisation (and therefore cost management perspective) it is important to focus primarily on the assets which, if compromised, would cause most damage to the organisation.

This does not need to involve a complex risk assessment exercise: in most organisations it is blindingly obvious what the biggest risk areas are and most CIO's and IT Managers would be able to state this off the top of their heads. For example, consider the following different types of organisation:

Online Share Trading Company

If the web applications which enable an online share trading company's clients to transact were compromised (eg. a hacker succeeding in taking over clients' trading accounts to commit fraudulent transactions) then the entire business would be in jeopardy due to the loss of trust in the market about the security of the company.

The impact of such an incident would be far greater than (eg.) an incident where a hacker managed to break into some back office systems and compromise the payroll. Of course, the online share trading organisation would be seriously concerned if the payroll system was compromised, but the overall risk to the business (and therefore the risk weighting of such an incident) would be significantly less than an incident with the online applications.

Therefore, the first priority for such an organisation in terms of penetration testing would be a rigorous probing of the web applications where the clients' financial transactions occurred, because that is where the greatest business risk exists.

Coincidentally, this would also be the point where the greatest risk occurs in terms of where a hacker would be most likely to attack, as it is widely recognised amongst hackers that web applications are often the Achilles heel of an organisation's security, and (as web applications) will by definition be exposed to the Internet.

Of course, such an organisation may well have a large security budget, however if this was not the case the organisation should focus their penetration testing on their web applications to obtain the greatest “security dividend” from their investment.

The Pharmaceutical Company

Unlike the online share trading company, the pharmaceutical company will probably have a relatively “inert” web site used primarily for providing information about the company and its products. Whilst it would be embarrassing and a nuisance if (for example) the web site was defaced by political activists such as animal rights groups, it is extremely unlikely that such an occurrence would pose a major threat to the business.

However, if the confidential plans and test data for the next generation of “wonder drug” (stored in systems on the company’s networks) were to be accessed by a hacker, this could have a massive negative impact on the pharmaceutical company’s business.

Therefore, the first priority for such an organisation would be to protect the confidentiality of its “crown jewels” – the data held on the internal network. In this scenario, penetration testing would be best focused on preventing unauthorised access to internal systems both via the Internet gateway and also from within.

The Internet Services Provider (“ISP”)

ISP’s (particularly those serving the small business and home user market) operate in a fiercely competitive environment where customers are likely to “take their business elsewhere” at the drop of a hat – particularly if there are service availability problems.

The critical information risks faced by the ISP are the non-availability of its web services due to a denial of service attack or the loss of confidentiality of their customer information. It is in fact foreseeable that an ISP could go completely out of business if they suffered ongoing availability concerns, or if a competitor proactively poached customers.

As with the online share trading organisation and the pharmaceutical company, other types of attack may well be damaging and disruptive – but are comparatively relatively low risk in terms of overall business impact.



SAFECOMS

A risk driven approach to penetration testing will therefore focus initially on probing how robust the ISPs service delivery platform is to these forms of attack in order to achieve the greatest "security dividend".

Using The Same Approach As A Black Hat Hacker

Penetration testing is only valuable to an organisation if the tester uses the same types of techniques that a real “black hat” hacker is likely to use on your organisation. If you were going to buy a 4 wheel drive which you were going to use for serious off road work, you would not test it by driving sedately down a suburban street: similarly, there is little point in testing the security of an organisation without subjecting it to the same kind of “treatment” it will receive from a real hacker.

Like anyone else on a mission to succeed, hackers are in a hurry and are on the look out for the line of least resistance. Once they decide to target an organisation they will rapidly look for any obvious potential “soft spots” that the organisation may have, and devise a way of exploiting that weakness.

In particular, they will not necessarily limit their activities to network-based techniques. If the most efficient entry method is via weaknesses in physical security or through social engineering, then that is exactly what a determined attacker will do.

Depending on what they are attempting to achieve and the characteristics of your organisation, hackers are likely to attempt some or all of the following ways of breaking your security:

Network Attacks

Identifying ways to penetrate the network through Internet facing hosts is a natural starting point for most hackers. The range of techniques employed is considerable. These can include:

- Scanning for known vulnerabilities
- Password cracking through brute force attacks
- Attempting to bypass access control lists
- Network eavesdropping
- Trojan attacks
- Exploitation of buffer overflows

Web Application Attacks

It is increasingly recognised that web applications are often an “open window” into the IT infrastructure of many organisations. This is because very few web applications are developed with security in mind, and very few developers understand web application security techniques. Hackers will therefore attack these applications either as an end in itself (eg. to perpetrate fraud via an

insecure financial service application) or to seek to use the web application as a soft entry point into the organisation's other systems.

Web application attacks will typically involve:

- SQL injection
- Cross site scripting attacks
- Exploitation of authentication, access control and authorisation issues
- Exploitation of session management problems
- Exploitation of web server configuration issues

Wireless Attacks

A surprisingly large number of organisations who have been diligent in establishing a secure traditional wired infrastructure suddenly throw caution to the winds when they roll out wireless. If a hacker knows (or can easily find out) that your organisation uses wireless technology, the hacker will almost certainly attempt to break your security through the wireless network, using techniques such as:

- Locating or establishing an unauthorised wireless access point
- Eavesdropping and exploiting weaknesses in network encryption
- Exploiting weaknesses in network access control

Social Engineering

Hackers use a wide variety of social engineering techniques in an attempt to elicit passwords (and other information that might assist an attack) from staff by covert means.

The methods used are many and various, but frequently involve telephoning a junior employee, posing as a member of the IT department and requesting that person's user ID and password so as to perform some remote diagnostic tests.

Physical Security Attacks

Hackers are aware that whilst many organisations have invested heavily in creating a sophisticated logical security infrastructure, this is frequently undermined by holes in the physical security. Hackers will therefore often attempt to breach the physical security of a site through a number of techniques. These can include:

- Stealing laptops (particularly where, for example, the sales force are known to congregate in a particular pub after work and carry their laptops with them)
- Obtaining access to a building through false pretences (eg. by posing as maintenance staff) and
 - stealing assets containing confidential data; or
 - furtively setting up a rogue wireless access point; or
 - looking out for passwords and user names written down on pieces of paper
- Exploiting weaknesses in building access control devices to gain after hours access or access to data centres

Telephony Systems Attacks

Telephonic communication systems and computer systems are nowadays highly integrated, and in many organisations the telephone network is effectively an extension of (or some would say a part of) the computer network. Not surprisingly, hackers can and do use weaknesses in telephony systems to break into organisations. Techniques used by hackers include

- War dialling (for the identification of remote access points)
- Attacking remote access port vulnerabilities
- Brute force attacks (for gaining access to remote access ports)
- PABX attacks (modifying PABX settings to (eg.) re-route calls)

The Compromise

In an ideal world, any penetration test would include all of these activities since a real hacker is likely to try all of them (depending on what they are trying to achieve). However, this would make the cost of a penetration test unrealistic for most organisations, and an intelligent compromise must be reached when defining the scope of the testing. This is considered further in **The Cost Dimension** below.

The important thing to note at this stage is that a penetration test will only make your organisation more secure if the tester uses the same techniques that a black hat hacker is most likely to use on your organisation.

Hacking Skills Equivalent To A Real Attacker

Like practitioners of any “art”, hackers vary enormously in their skill levels. At one end of the spectrum are the relatively unsophisticated “script kiddies”, whose capability is essentially limited to

using pre-made scripts designed to exploit known vulnerabilities. At the other end of the spectrum are the experienced and sophisticated hackers (increasingly being used by organised crime syndicates) who have the technical skills to outfox world class security set ups. In between there is an army of people whose skills are better developed than the average script kiddy and who have the capability (for example) to successfully launch a custom made SQL injection attack on a poorly designed web application, but who would not be likely to break a well designed system.

When having a penetration test conducted on your organisation, it should always be remembered that – given that the object of the exercise is to identify security weaknesses before a real “black hat” hacker does – the skills of the penetration tester need to be on a par with those of the type of hacker who is likely to be taking an interest in your organisation. This raises the question “who is likely to attack my organisation?”

Script Kiddies

Any organisation is likely to be attacked by a script kiddy, since their attacks are typically randomly and targeted at known vulnerabilities. Script kiddies typically have no idea who they are attacking – and generally they will not care. The only thing they are interested in is that you are vulnerable, and therefore potentially open to exploitation by them.

It should therefore be taken as a given that the skills of your penetration tester must be at least on a par with the average script kiddy.

Sophisticated Hackers

In general terms, the more attractive your organisation appears to hackers, the higher the calibre of hacker that is likely to have a crack at you – and the skills of your penetration tester need to reflect this reality.

Sophisticated hackers are in practice only likely to spend their time crafting attacks against major corporations (particularly those in the financial sector) or important government agencies. At this high end of the spectrum hackers may invest months of their time in crafting extremely esoteric and original attacks, resulting in a constant battle of wits between security departments in target organisations and top level hackers. These organisations are often in an almost constant state of penetration testing, with different aspects of their systems being tested by extremely experienced “white hat” hackers on an ongoing basis. They need to invest in the services of the very best penetration testers as the stakes at this level are extremely high.

Whilst not many organisations are operating at this level of threat, a large number of organisations are at threat from hackers whose skills are beyond that of script kiddies. If your organisation fits any of the following criteria then there is a strong likelihood that you will attract the targeted attention of a real hacker whose skills are some way above those of a script kiddy:

- Engaged in the financial services industry at any level
- Offering online credit card transactions with your customers
- Federal, state or local government agency
- Telecommunications company
- Defence sector organisation
- Engaged in the health sector and likely to be holding records about patients
- Publicly listed on any stock exchange
- Internet Service Provider
- High profile organisation of any type (perceived as potentially open to extortion in return for not launching denial of service attack or public defacement of website)
- Engaged in design and manufacturing of leading edge products in any sector (particularly pharmaceuticals, IT, electronics, anything related to defence)
- Part of the “extended enterprise” with a direct link into the trusted networks of any of the above

Of course, this list is not exhaustive: given the widely differing agendas of hackers any organisation is capable of attracting the attention of a real hacker. However, if your organisation fits any of the profiles listed above then it is strongly recommended that any penetration testing is conducted by testers with strong skills in all of the areas referred to in the section **Using The Same Approach As A Black Hat Hacker** above. Simply using standard tools to run network scans and identify known vulnerabilities will not make your organisation more secure.

The Cost Dimension

The cost of a penetration test is generally a function of the time taken to do it and the skill level of the tester (just as a senior counsel costs more than a journeyman barrister, the same applies with penetration testers). So how long should a test take, and who should you employ to do it?

Diminishing Returns

Most people are familiar with what economists call the “law of diminishing returns” – ie. there comes a point when the value add of additional activity is insufficient to justify the additional investment. In everyday speak, we often refer to the 80 / 20 rule which is a similar concept.

These concepts are particularly applicable in the field of penetration testing. Provided your penetration tester is properly skilled, there is a direct correlation between the amount of time allocated to the testing and the level of increased security that you should achieve. As a penetration test progresses, the rate at which security is being improved slows, and there comes a point in a penetration test where it is no longer efficient to continue the penetration test.

The objective is to test to the point where the level of residual risk is considered acceptable (ie. it is recognised that the risk of an attack still exists, but estimated that the likelihood and consequence of an attack is acceptable to your business).

Identifying The “Acceptable Risk” Point

In the previous sections of this White Paper we discussed the main principles to be applied in ensuring that a penetration test really made you more secure. These were:

- The penetration testing is risk focused, specifically targeting those assets that represent the greatest risk to the organisation
- The penetration testing is conducted in the same manner that would be utilised by a would-be attacker
- The penetration testing is carried out by an ethical hacker who is at least as skilled as a future would-be attacker

Applying these principles to your organisation will enable you to quickly determine what the scope of the penetration test should be (what aspects of the IT infrastructure should be tested, what kinds of tests should be carried out) thereby defining the acceptable risk point. Quotations can then be obtained from suitably qualified testers to test to this point.

It is possible that the costs of testing as far as the “acceptable risk point” are in excess of your budget – in which case you can scale back the scope of the testing accordingly. Having been through the mental process of identifying the biggest risks to the organisation and the approaches most likely to be used by a hacker against an organisation of your profile, you can scale back in accordance with a clear set of priorities so that – if necessary in order to accommodate budget constraints – the scope of the penetration test is cut right back to a hard core irreducible minimum.

Of course, this kind of budget driven compromise will increase your level of risk but that then becomes an informed calculated risk – you remain in control, and decide how to play the odds.

Indicators Of Time Frames For Penetration Tests

The cost of a penetration test is typically linked to the time that a penetration tester will require to complete the testing. Based on the experience of conducting numerous penetration tests for a wide variety of different profile organisations, we offer the following table as approximate indicators of typical time frames for penetration testing. Of course, these are approximate guidelines only and will vary from case to case depending on the complexity of your organisation and IT infrastructure and a number of other variables. However, they should provide a helpful ball park indication:

Activity	Timeframe
On Site Scoping Activities	1 Day
Information Gathering	1 Day
Network Enumeration and Fingerprinting	1 Day
Mail Server Testing	1/4 Day (per server)
Name Server Testing	1/4 Day (per server)
Firewall Testing	1/2 Day (per gateway)
Remote Access Testing (e.g. Citrix Metaframe)	1 Day (per device)
Web Server Testing	1/2 Day (per server)
Web Application Testing (Smaller Sites)	1 Day (per web application)
Web Application Testing (Medium Sized Sites)	2 Days (per web application)
Web Application Testing (Large Sites)	3 Days (per web application)
Physical Security Testing	1 Day (per site to be tested)
Social Engineering Exercises	1 Day
Report Writing and Management Presentation	2 Days

Educated Attacks and Blind Attacks

It will be noted from the table above that some time is allocated to information gathering, network enumeration and fingerprinting. This raises the question of whether a “blind” or “educated” attack is more appropriate for your organisation.

A black hat hacker will gather as much intelligence as possible about his intended target prior to conducting an attack, and this is reflected in the preparatory intelligence gathering activities referred to above. However, in order to short circuit the process (thereby saving time and money) some organisations provide the tester with significant amounts of information at the outset of the test, enabling the tester to then focus their efforts straightaway on developing and executing attacks – the so called “Educated Attack”. Other organisations prefer to keep things more “realistic” by providing the tester with no information at all, effectively putting the tester in the same situation as a real arms length hacker. This is the so called “Blind Attack”.

There are arguments either way as to which is the better model. Those who favour the “Educated” attack make the point that a real black hat hacker will almost certainly be able to work out this information anyway, so why pay a penetration tester to verify that this is indeed the case? Additionally, the point is also made that many attacks are from people who already have a fair level of knowledge of the organisation (eg. ex employees, current employees etc.). However, those who favour the “blind attack” believe that there is real value in seeing how much information that would be useful to a hacker can be gained by the tester in a day or so of activity, as this will often point to sloppy internal practices and help the organisation make life that much more difficult for the hacker.

Our recommendation is that if you can possibly afford it, there is significant value in getting the penetration tester to gather his own intelligence, as this will often reveal ways in which security can be tightened up (it can also be a suitably chastening experience for the IT staff to learn just how much information they thought was “internal” or “company confidential” can actually be gathered in the public domain simply by making use of search engines and very basic hacking tools and techniques).

Differential Tests

Another cost related issue is the frequency with which tests should be conducted. The IT infrastructures of most organisations are dynamic and in a constant state of change. Therefore the results of a Penetration Test undertaken today are theoretically of limited validity tomorrow. However, other than in the most extreme secure set ups it would clearly be inappropriate to be in a constant state of Penetration Testing.



Increasingly, organisations are starting to have a rolling program of testing based around (typically) a “full” Penetration Test at quarterly intervals, coupled with monthly “differential” tests. The results of the most recent “full” test are used as a baseline of the state of security, and deviations or differentials from that baseline are identified. This kind of program is more cost effective for the organisation whilst still ensuring that key threats are consistently monitored, and it is a model that is likely to be adopted by more organisations.

After The Test Is Done

So far we have focused on how to ensure that real value is obtained from a penetration test by looking at how (and by whom) the test should be conducted. However, an equally critical issue is what happens after the testing has been completed.

The output from a penetration test should be a written report documenting the following:

- Executive summary
- Description of testing methodology
- Detailed findings including an evaluation of risk
- Recommended risk mitigation techniques

The Executive Summary

It is particularly important that the report contains an Executive Summary aimed at non-technical senior management.

In our experience, the majority of properly conducted penetration tests will identify several high risk findings (ie. security weaknesses that could currently be exploited by a hacker resulting in access to internal or confidential systems). It is obviously important that this information is presented to senior management clearly and concisely (without excessive technical detail) so that the leadership of the organisation will allocate resources and budget (if necessary) to ensure that appropriate remediation treatments are implemented.

The findings need to be presented from a risk perspective (typically using a high / medium / low grading convention) based on likelihood and consequence. It is important that the organisation conducting the penetration test includes people with business management experience who are able to interpret the results and ascribe the appropriate risk rating finding. Failure to do so can lead to incorrect prioritisation in the risk mitigation exercises that follow a penetration test. It is rare to find a penetration tester who also understands business risk, so be sure that the organisation you choose to deliver penetration testing services includes properly skilled business risk analysts.

Remediation Treatments

A penetration test will only make your organisation more secure if the risks identified are subjected to remediation treatment. That may sound like a statement of the obvious, but it is remarkable how many organisations commission a penetration test, receive a report detailing several major risks, and then fail to do anything about them.

Failing to deal with security issues identified in a penetration test could well result in legal exposures for the organisation, if the weaknesses are subsequently exploited by a hacker. When organisations are hacked, the fall out will often adversely impact third parties (customers, suppliers, business partners etc.) and – in our increasingly litigious society – legal action is on the cards. That action may well be based on the common law tort of negligence, and if the claimant can show that the loss they suffered arose from a security weakness that had been pointed out but not fixed, then there is obviously a greatly increased likelihood that the claim for negligence will succeed.

The moral of the story is therefore clear: do not waste time and money on a penetration test if you are not prepared to follow through with rectifying any major risks that are found.

Conclusion

Penetration testing should be a central plank of the information security strategy of any organisation that is at risk from attack as a result of having Internet facing information assets. However, penetration testing will only yield a strong security dividend if

- The testing is risk focused
- The testing is conducted using the same comprehensive range of techniques that a real hacker would use
- The testing is conducted by a tester with skills at least equal to those of the probable profile of hacker that will be interested in your organisation
- The results of the testing are presented in a way that enables senior management to truly understand the risks that they are currently subject to
- The organisation has the will to implement the remediation strategies necessary to deal with the risks that are identified.

A suitably qualified organisation should be appointed to undertake the activity. That organisation needs to be able to demonstrate a sound understanding of the principles set out in this White Paper, whilst simultaneously providing reasonable value for money.

About Safecomms

Safecomms is a specialist information security services and consultancy organisation. Safecomms has performed extensive penetration tests for a wide variety of different profile organisations, including large multinational corporations, smaller private sector bodies, government agencies and local councils. Safecomms is widely recognised as a leader in penetration tests, particularly in the specialist field of web applications.

Safecomms can be contacted at any time:

Tel: (+61) 02 8234 4000

Fax: (+61) 02 8234 4099

Email: info@safecomms.com.au

On the Web: <http://www.safecomms.com.au>