IPF

encription
ethical hacking services

Security, Trust and Risk
Why Ethical Hacking?

A whitepaper by encription limited

Campbell Murray

encription limited
The Stables
White Lodge
Bevere
Worcester
WR3 7RQ
www.encription.co.uk

IPF

encription
ethical hacking services

Security, Trust and Risk – Why Ethical Hacking?

Introduction

There are many different terms used for security testers, specifically those who perform intrusive testing which is intended to compromise and analyse your security. Penetration testing, ethical hacking, tiger teaming, red teaming, blue teaming, information or digital assurance testing and vulnerability analysis are just some buzzwords to describe essentially the same thing. The list is nearly as long as the variations in products and tests. This document will attempt to shed some light on what you should expect from an ethical hacker, why you would want to use one and to give you guidance on how to project manage a successful security test.

Having a regular ethical hack performed is required to obtain and maintain BS7799 and ISO27001 standards and it is also recommended for connection to Government Connect. The payment card industry also recommends that all companies taking credit card payment obtain PCI compliance or in other words, have an ethical hack performed.

Ethical hacking is a key component of risk assessment, audit, counter fraud, best practice and good governance. Not only will ethical hacking identify risks and highlight remedial actions it will reduce your ICT costs long term by resolving those vulnerabilities and reducing support issues. It is also a requirement for many financial and insurance organisations regulated by the FSA and increasingly the data protection act presses a multitude of organisations to demonstrate data security. The upshot of this is that the number and variety of ethical hackers has mushroomed in the last few years which raise several hurdles for the purchasers.

In such a new market, what do you look for to ensure you get value for money and a quality product? In order to answer these questions it is important firstly to understand what an **ethical** hacker is, and is not.

IPF

encription
ethical hacking services

What is an ethical hacker?

In simple terms an ethical hacker is an individual with the same tools and knowledge as a malicious hacker but rather than break into systems for criminal gain an ethical hacker will do this by invitation for a fee.

An ethical hacker must be **authorised** to perform any tests on your systems. This is done by defining the scope of the test, what is to be tested and how it will be tested. The test team will also require a disclaimer stating that they are legally authorised to carry out this activity on your property.

The ethical hacker performing the test must not test anything beyond the agreed scope, to do so would be unethical. This brings me to my next point. An ethical hacker must be **trusted**. Does your ethical hacking supplier perform background checks on their employees? During any security assessment it is highly likely that the test team will encounter sensitive, possibly restricted data. Do you trust your ethical hacker with this information? How is your test result stored? Securely we would expect and with a minimum of 256 bit encryption!

In such a highly specialised field the ethical hacker has to be **expert** in all domains of security from the physical to having an encyclopaedic knowledge of network devices and infrastructure as well as being an expert in every web and server programming language. How can you guarantee that your ethical hacker will have this knowledge? Well you can certainly check their certifications and there are plenty to choose from; CEH, CFEH, GSIH etc but the real measure of an ethical hacker's metal is their depth of experience.

You will gain a far better picture of how an organisation performs by taking up references from within your sector from others who have used the same supplier. You may also consider requesting CV's of the test team to see who they have worked with and in what capacity.

In this rapidly expanding market you could fall foul of the ethical hacker or established company that has chosen to enter this field having passed the exams but without hands on experience the value of the test should be considered limited. Emerging accreditation processes such as the TIGER Scheme will measure ethical hackers not just on their technical skills but also their ability to report findings in plain English. TIGER also allows potential clients to securely view the experience of an individual ethical hacker. You should also establish if they follow an accepted methodology for testing. There are several unofficial but widely recognised standards available, OSSTMM being the most popular and comprehensive at present.

Finally your ethical hacker must be **independent**. It is recommended that your own in house IT staff gain knowledge of IT security best practice but an ethical hacker should not work for you or any organisation that supplies your hardware or software, for example, because he or she will have prior knowledge of your setup and hardware versions. The non-independent ethical hacker could also be biased in their test results especially if vulnerability is discovered in something that their company has supplied.

Revision: 1.0.5
Revision Date: 01 July 2007

IPF

encription
ethical hacking services

It should be a serious consideration that the company you choose only supply ethical hacking services and nothing else. Companies that have chosen to enter the field of ethical hacking but have previously provided other IT services universally use their ethical hacking accredited technicians for other projects, diluting their expertise and experience in this demanding and specialised field. If an ethical hacker does not solely perform ethical hacks, how much value will their opinion have?

What types of test are there?

Just as there are many different areas of IT security there are just as many different types of test style and it is important to know what these are so you can choose that which you consider most appropriate to your aims.

A '**black box**' test will provide no information to the ethical hacker at all, just a pointer in the right direction to what should be tested. This could be the company name, address, an IP Address or website URL. A black box test will provide the most realistic ethical hack in that the ethical hacker starts with the same level of knowledge as the malicious hacker.

A '**white box**' test will on the other hand pre-arm the ethical hacker with knowledge of your network, servers or security policy for example depending on what is to be tested. Although not as realistic as a black box hack you will get more for your money as the ethical hacker will be able to pre plan and focus activity within the allotted time scale for the test.

Other definitions of tests exist and are vendor specific. I have heard of 'crystal box', 'rainbow box', 'oblique box' and all other manner of variations. The terms black and white box are sufficient for us.

External penetration test

This is the most common type of test and is aimed at IT systems from 'outside the building' testing systems that are 'internet connected', such as the DMZ of your network, VPN and your websites. The external ethical hack is typically done black box method as this will replicate the risk to your organisation that a malicious hacker poses. However as you will learn later on the greatest threat is not from outside, but this is where the majority of malicious hackers will approach your systems from.

Internal security (including partner links)

An internal security test focuses on what staff can see and do within their own IT network. People are the weakest link in IT security. They already have access to the IT network; what the malicious hacker aims to achieve is readily provided for colleagues. Without proper access control colleagues may deliberately or unwittingly jeopardize confidentiality and integrity of data. An internal security test will determine these factors and provide a route map to information assurance.

IPF

encription
ethical hacking services

Of course you may have the most secure of IT setups but this could in turn be disrupted by your suppliers and clients. More and more digital information is shared with partners and if this third party security is found to be lacking this can impact on the integrity of an organisations IT security. A thorough audit must include your partner chain.

Social Engineering

As already mentioned people are the weakest point in IT security. The term social engineering is very appropriate as in this type of test the ethical hacker will manipulate staff to achieve their aims. This may be to reveal sensitive information in person, over the phone, via email or fax. It may also include efforts to trick people into installing malicious software onto the IT network providing the hacker with the access they require. A social engineering test will establish the level of IT security awareness of an authorities' colleagues and typically the results are shocking.

Techniques used are diverse and can be very creative. Distributing free USB drives in an organisation still in their blister packs and looking as though they have come straight off the shop shelf is an easy way of getting software onto user's machines. Just because the USB drive is shrink wrapped doesn't mean it's new, or blank! Likewise CD's and DVD's can be mocked up to look like the real thing with little effort and at very little cost gaining the users trust in the media.

Perimeter Testing

At first glance you may wonder what an organisations physical security may have to do with their IT security other than gaining access to the computer equipment. By perimeter testing we are referring to what information leaks out of a location unbeknown to the people inside. The use of wireless technology is just an example of what may be sought in a perimeter test but just as important is searching for sensitive information in refuse generated by an organisation and also simply listening to staff conversations as they enter and leave a building for example.

An ethical hack may be scoped to just one of these areas or it may cover all. Depending on your requirements and desired outputs you may wish to test certain aspects of each of these security domains.

IPF

encription
ethical hacking services

So what is typically found during an ethical hack?

Websites are the second most vulnerable aspect of your IT an ethical hacker can test. The reasons for this are many. If you were to put out to tender that you wanted a new website built you are likely to have dozens of agencies beating down your door to tell you why you should use them. It is a cut throat [read 'buyers'] market and the web development agencies compete on price, search engine optimisation, marketing strategies, deadlines and budget. What they do not consider is security and this is for two reasons. Firstly to build security into web applications would push the price up and secondly no one is asking for security in web applications hence the development agencies remain blissfully ignorant to the threats they create.

Websites are now a common extension to the business management process, taking orders, handling customer requests, providing customer liaison and delivering new products requires that the web application itself has a high level of privilege on the web server. No matter how secure the server is, if the web application is vulnerable and has a high level of operator rights on the server then the server may in turn be compromised.

<Case Study 1>
In a recent test we discovered multiple cross site scripting (XSS) issues on the website of a large organisation. XSS is a vulnerability where inputting script commands via web forms and URL's can modify the behaviour of a page; either it's content or redirecting a visitor to another website altogether. Although in this instance the XSS did not threaten the security of the application itself it would have a direct impact on visitors to the website if they were to click a link with the XSS code embedded. This point was not driven home to the management team until we utilised this vulnerability in a social engineering attack on their staff. By utilising these XSS vulnerabilities we were able to send links to staff members which were to their own domain name, but by encoding JavaScript into the URL we were in turn able to use the councils own website to redirect these staff to our own website.
</ Case Study 1>

Wireless devices are also a ripe vulnerability area. A year ago the use of the WEP encryption protocol was adequate for most peoples security needs and at the time considered industry best practice. However cryptography has moved on rapidly since then and WEP security can now be defeated in around 14 minutes. WPA offers a higher level of protection providing it is implemented correctly and is now recommended by central government. That said we still encounter WEP encrypted access points and sometimes altogether unsecured access points. With the increased proliferation of mobile computing devices rogue WAP's (Wireless Access Points) are springing up more and more frequently.

What is an underlying theme in almost all vulnerabilities that we detect is a **lack of understanding** of IT security issues; certainly from web developers and users of mobile devices and it is the lack of knowledge that is the greatest threat to an authority. The department who enabled WEP security probably aren't aware of how quickly it can be defeated or how their website may compromise the integrity and confidentiality of their data.

IPF

encription
ethical hacking services

The number one vulnerability in any organisation regardless of industry or government sector is the **staff**. Trusting colleagues can be easily tricked into providing the hacker with the information they need or they can be persuaded to carry out actions that will jeopardise security.

<Case Study 2>
In a recent ethical hack we were given a selection of names and email addresses to perform social engineering techniques on. We split this into two groups of five and determined to attempt a different style of social hack on each group although both groups were to be tested via email first, falling back to telephone and fax if necessary. Needless to say these fall backs were not required.

The first group we sent an email impersonating another member of staff from the other group of given names. This was in part to test anti spam filters as this spoofed email should have been blocked. However it wasn't and it got through to all five contacts. This email contained a deliberate mistake. The content was requesting that members of staff download some software from the link provided. The purpose of the software was for IT performance monitoring and that this would be an anonymous process. However the link was broken. Half an hour later we sent another email apologising for the earlier mistake and providing the correct link. All five users downloaded and installed the software. What was most worrying about this attack is that we made no effort to disguise the URL in the link; it was clearly to www.encription.co.uk and not in relevance to the organisations internal or other website systems.

This hack falls into a social engineering group which we call **request testing** but would normally be called **spear phishing,** and it worked by gaining trust. It is a psychological principal that people are more likely to believe something if it sounds like something they have already heard. This certainly proved true in this case.

In the second group of staff to be tested we determined that we would gain their network and other logon details with the minimum of effort. This was achieved by emailing the test group a message with a link to an external website. The message explained that we were working in partnership with the organisation and had created a system for staff to log into via a web URL and update their contact details. The URL posted in this phishing email linked to a clone of the organisations website which we had made.

Of the five staff tested three gave us their usernames and passwords within 7 minutes of the email being released. We deliberately created our clone website so that on harvesting this information the visitor was returned to a login failure page. In doing so staff re-entered their details again and again. After a few minutes they then tried other combinations of usernames and passwords which they had for other systems. One member of staff helpfully emailed us to inform us that there was a problem with the system; he was a head of department and we later discovered his login details gave us administrative rights over his network node!

What about the other two people from the test group who didn't respond though? One was on holiday at the time and the other had recently left the organisation and no-one was checking his mail! If this had been different we may have got a full 10 / 10!

IPF

encription
ethical hacking services

What is truly interesting about these results is that we later performed a security awareness test for the organisation on several members of staff including those we had socially engineered. Of the test group the highest marks were obtained by those who had willingly compromised their own security.

The conclusion we draw from this is that understanding of policy does not reflect understanding of security.

All of the staff vulnerability we have mentioned here is down to a **lack of threat awareness**. The only remedy to this is to **train staff** in threat awareness and make them aware of the impact their actions may have, regardless of how well intentioned they may be.
</ Case Study 2>

What else should you expect?
The output of an ethical hacking exercise will be the report delivered after completion of all testing. This is what you are paying for and it is crucial that the ethical hacker gets this right. The report will have a different purpose depending on your job role. For IT Managers it is often necessary to justify spending on IT to increase your security, for HR it may be to outline the need for security awareness training. Whatever your focus the report should always follow these well worn principals.

First and foremost the report **should be clear and easy to understand**. A two thousand page technical manual may be thorough but it is of little value to an organisations staff that may not have the time to read and comprehend it all.

It should contain a **section for non IT / board / senior management (vulnerability overview)** Not everybody who will read the report will be technical and key concepts need to be expressed in a non technical manner. Particularly if the report is to aid in justifying further expenditure. The report should be technical where appropriate but use plain English throughout. The use of simple network diagrams is helpful for managers and an intelligent use of colour coding for rating the severity of vulnerability is highly desirable and you can see examples of this in Appendix A which has been taken from a real ethical hack performed by encription limited and anonymous.

Of course the report will be technical but technical aspects of the results should be described in two formats, firstly a **section for technical managers (technical overview)** introducing key concepts but in a language appropriate to the managers level of technical knowledge and providing them with the necessary information to project manage their response to the results and of course there will be a section for **systems administrators (full technical details including fix).** This will be no holds barred technical data. But it is still important to consider how this information is formatted. Stuffing the technical aspects of the report into an appendices will not enamour your IT staff to the ethical hacker and it is important that they can work together should there be any need for communication during debrief and fixing phase.

IPF

encription
ethical hacking services

Likewise it is a measure of an ethical hackers experience if they put into reports what they found that was worthy of praise. This is important for two reasons, firstly that your IT staff still need to know that the ethical hacker is not there simply to criticise it is just as important to measure and identify that which works so that these aspects of your IT defences remain unchanged and lessons may be learnt from them.

Conclusions

- **Testers should be 3rd party and not supply any IT services**
  This is very important. An existing supplier of IT services will have knowledge of your existing IT environment and you will not be assured of a fully unbiased appraisal of your security.

- **Security Testing should be the main business of the security company and not a second offering.** Penetration testing is highly specialised. To avoid the risk of your testers skills being diluted your supplier should concentrate solely in this area.

- **Will they do a test tailored to your needs?**
  This is an indication of how experienced the testers are and that they are not running the same test for every job they do. An ethical hack may take the shape of testing several areas of vulnerability from external to perimeter. An out of the box package simply cannot provide you with this level of tailoring to suit your budget and requirements.

- **Are the testers experienced security professionals holding recognised certifications?** And very importantly appropriate insurance to carry out penetration testing. There is always the risk when probing IT systems that damage or loss of service could occur. A professional and trained tester will mitigate these risks. An inexperienced or untrained individual may not.

- **Make sure it is not solely an automated test!**
  Out of the box software which can execute security audits is fine for interim testing but cannot be relied upon. An ethical hacker will use these tools but will always manually verify a result. In this emerging industry you stand a good chance of encountering vendors who will do just this and sell it as an ethical hack. An out of the box automated test stands a high probability of missing important aspects of your security posture and will never produce a tailored report for your needs.

IPF

encription
ethical hacking services

Finally

An ethical hack, when carried out and reported properly, will give you knowledge of all your IT security weaknesses and provide you with the information you require to fix those vulnerabilities. This will reduce your ICT costs over the long term, reducing vulnerability and support calls. An initial assessment can also provide you with the business case to justify further expenditure. However IT is a dynamic entity and a penetration test is only a snapshot in time. **Regular testing** is required to remain on top of security threats and regular training is needed to help colleagues protect your data and themselves.

IPF

encription
ethical hacking services

Appendix A

Anonymous extracts from penetration test reports.

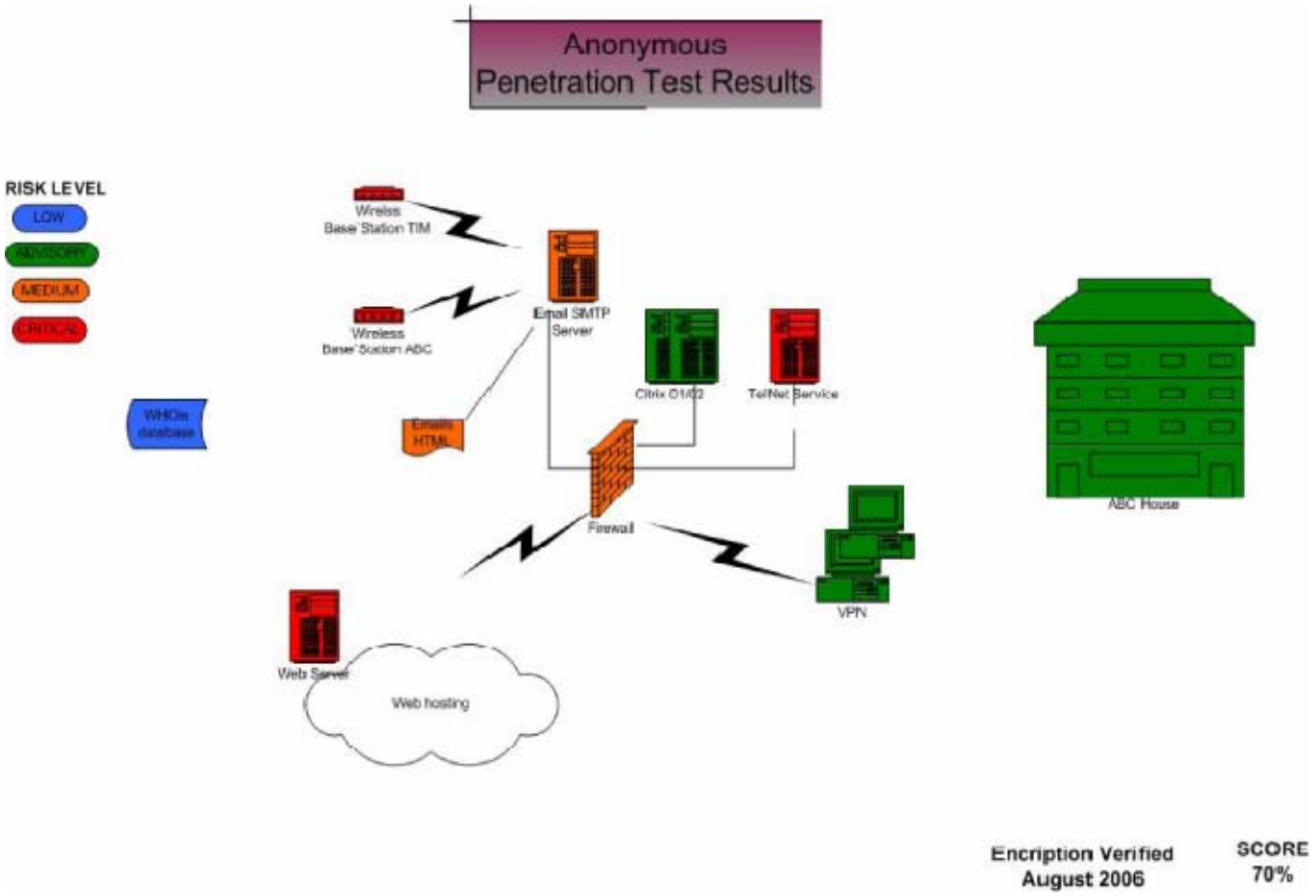
Contents

IPF

encription
ethical hacking services

Appendix A.1

Vulnerability Overview



IPF

encription
ethical hacking services

Appendix A.2

Executive Summary

ANONYMOUS

APPLICATION PENETRATION TEST REPORT

Executive Summary

With authorisation from Anonymous, encription limited undertook a series of confidential penetration tests over a four-day period. The objective was to identify potential security vulnerabilities in either the physical or IT environment at the ABC Office. No verbal contact was made with any member of staff.

Attempts to gain access to the IT infrastructure, the web site and other services reveals that a password of at least 6 characters is in use (recommendations are always for 8 characters).

Although vulnerabilities have been identified in services, such as wireless access points, there is still a level of security in place that will defeat many attackers. Third party suppliers, such as the web site and web hosting, cause the greatest security risks to the company.

The physical environment appears to be less secure and has some points where access into the building could be obtained relatively easily.

Using encription's verification scale, the security at Anonymous is good and is rated at 70%, **(100% being totally secure).**

Encription, in liaison with the web hosters would be able to resolve all of the identified IT vulnerabilities

IPF

encription
ethical hacking services

Appendix A.3
Example scope

1 INTRODUCTION
Application and network security experts from **encription** limited performed the following perimeter and penetration test for Anonymous.

2 SCOPE & LIMITATIONS
2.1 SCOPE
The test was aimed at Anonymous (ABC Office) from a holistic approach. All facets of the company's security were taken into account.

2.2 LIMITATIONS
There were no limitations during the test.

2.3 PRIOR KNOWLEDGE
The test team had no prior knowledge of the Anonymous security posture or IT infrastructure. No information was provided for them other than the company name and location.

2.4 METHOD
The testing was done in a 'Black-Box' method, in which the testers had no information or prior knowledge regarding the client's application's architecture or the technology used to implement it. Neither was there any knowledge of the client's level of security. This type of test gives an accurate simulation of an actual hacker attacking the system.

Tools used during the penetration test are a mixture of publicly available tools and special purpose home-grown tools. In the case of a truly black box test, as this is, extensive manual testing is implemented. A number of specific tests were created during the project in order to attempt exploitation of identified vulnerabilities.

DOCUMENT DETAILS
Document Type: Application Penetration Test
Project Name: ANONYMOUS / BB / unknown
Lead Tester: Campbell Murray
Secondary Tester: Jack Crane
Document Version: 1.00
Created by: Campbell Murray
Creation Date: 07 August 2006

IPF

encription
ethical hacking services

ABOUT ENCRIPTION LIMITED

encription limited is a UK based IT security company operating from Worcestershire. From this central location we are able to deliver our services nationwide.

With highly experienced consultants at our disposal, encription limited is able to meet your IT security needs, no matter how simple or complex, including consultancy, ethical hacking and staff training. All our consultants have extensive experience in IT security, forensic investigation and ethical hacking. We work to BS7799 (ISO27001) security standards and we are ISO 9001:2000 certified.

Our mission
Is to make IT systems and information, whether complex or not, more secure.

In doing so, we keep abreast of the latest IT security threats and work with appropriate organisations, professional bodies and the public sector to develop and maintain IT security standards, defences and techniques that will reduce the risk of an attack on your IT systems. Our solutions are tailored to your specific needs, risk profile, risk appetite and budget.

Our Partners
We are partnered with CIPFA and the IPF Performance Improvement Network [PIN] and the Better Governance Forum [BGF]
We are commercial partners of the SMART governance network.
We are members of the National e-Crime prevention initiative steering committee.
We work closely with WARP groups nationwide.
We work with the new public sector TIGER testing standards initiative.
We work with Police Crime Prevention Units providing training for crime reduction officers in IT security threats so that they can provide meaningful advice for business and the public alike.
We also collaborate with Police HTCU's (High Tech Crime Units).

Our Clients include
Public Sector, Local Authorities, corporate, building societies, accountants, solicitors and SME's.

About the author: Campbell Murray is the Technical Director of encription limited [www.encription.co.uk] and has many years experience in the building and penetration testing of web and network applications across a range of languages, server and database technologies. Campbell is an expert social engineer and has demonstrated repeated success in this field of testing.

Campbell is a founder associate and member of the management committee of the TIGER Scheme.

LEGAL NOTICE

ISO 9001:2000 REGISTERED FIRM