

THE MAGAZINE OF THE BCS SECURITY COMMUNITY

iSNOW

SPRING 2011

www.bcs.org/security

PENETRATION TESTING

The ethics of accessing networks
and systems

bcs

The
Chartered
Institute
for IT

06 WHAT'S IN A NAME?

The differences between a penetration tester and a criminal cracker.

08 EXPOSING VULNERABILITIES

There are a lot of security lessons that can be learned from the WikiLeaks issue.



Information Security MSc

Flexible learning for everyone

We have extended the way in which Royal Holloway's internationally recognised MSc is offered.

- **CPD/CPE Modules:** Most MSc modules are now available as stand-alone courses of one week's duration (Block Mode). These modules may be taken with or without an examination.

As a result the MSc now has the following traditional delivery modes:

Full-time, one year, on campus; **Part-time**, two years, on campus; **Block Mode**, two years, on or off campus; **Distance Learning**, up to four years via the Virtual Learning Environment.

The introduction of CPD modules has enabled us to introduce even more flexibility into our methods of delivery.

- **Latest innovation** – 'Mix and Match' degree programmes. It is now possible to obtain the MSc by accumulating modules by any delivery method listed above (maximum period seven years).
- **Postgraduate Diploma** – each module is also available in condensed mode and taught as a one, two or three-day training course offered by QCC Training Ltd. Students may follow a structured programme of these courses and then undertake an MSc level project to obtain the Postgraduate Diploma in Information Security.

Royal Holloway
University of London



Information Security Group
www.isg.rhul.ac.uk
p.stoner@rhul.ac.uk
z.ciechanowicz@rhul.ac.uk
T: 01784 443101

PENETRATION TESTING

EDITORIAL

Henry Tucker Editor
Brian Runciman Managing Editor

PRODUCTION

Florence Leroy Production Manager

Advertising

E catherine@atalink.co.uk
T +44 (0) 20 7074 7921

Keep in touch

Contributions are welcome for consideration.
Please email: editorialteam@hq.bcs.org.uk

ISNOW is the quarterly magazine of BCS Security Community, incorporating the Information Security Specialist Group. It can also be viewed online at: www.bcs.org/isnow

The opinions expressed herein are not necessarily those of BISL or the organisations employing the authors.
© 2011 British Informatics Society Limited (BISL).
Registered charity no. 292786.

Copying: Permission to copy for educational purposes only without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage; BISL copyright notice and the title of the publication and its date appear; and notice is given that copying is by permission of BISL. To copy otherwise, or to republish, requires specific permission from the publications manager at the address below and may require a fee.

Printed in the UK by Interprint,
Swindon, Wiltshire.
ISSN 1752-2455. Volume 5, Part 3.

British Informatics Society Limited
First Floor, Block D, North Star House,
North Star Avenue, Swindon, SN2 1FA, UK.
T +44 (0)1793 417 424
F +44 (0)1793 417 444
www.bcs.org/contactus
Incorporated by Royal Charter 1984.

05 ISSG PERSPECTIVE

Gareth Niblett, Chair of the BCS ISSG, gives his view on future threats.

06 WHAT'S IN A NAME?

The difference between a penetration tester and a criminal cracker.

08 EXPOSING VULNERABILITIES

There are a lot of security lessons to be learned from WikiLeaks.

10 DISCLOSURE AND PS3

The ethics of finding flaws in software and then publishing them.

12 MULTIPLE DEFENCES

When it comes to staying safe, you need more than just penetration tests.

14 JUMPING FENCES

A personal insight into going from hacking to penetration testing.

16 LEGAL

A look at ePrivacy and some fines from the ICO.

18 OPINION

In the fast moving world of security you need more than just annual check-ups.



What is the cost of being locked out of your PC?

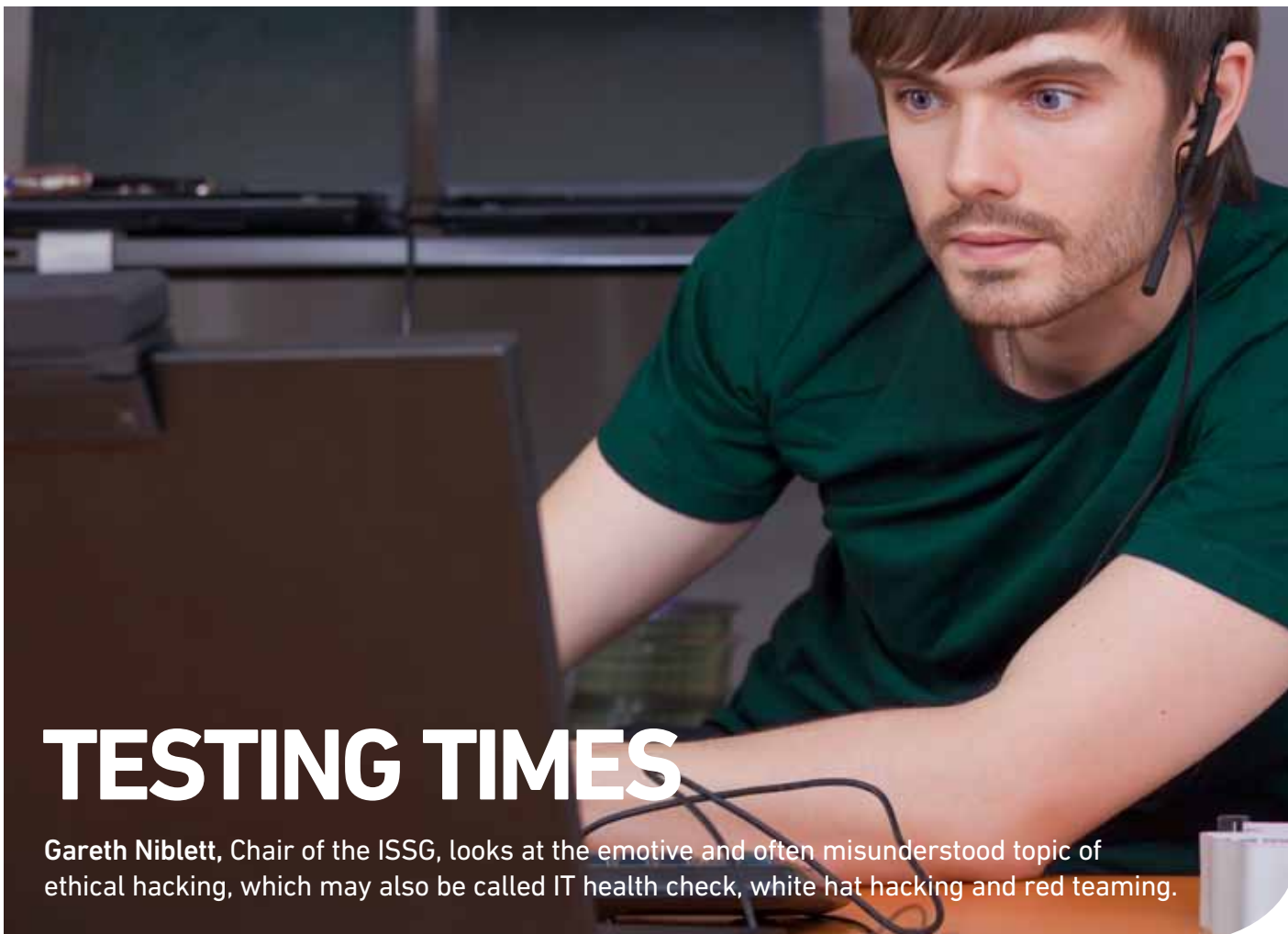
Now multiply this by the number of PC users in your business.

Specops Password Reset allows all users to reset their own passwords in seconds, maximising uptime, minimising downtime and reducing calls to the Help Desk by typically 90%. It works 24 hours a day and enables even remote users to reset...

That's innovation. That's simplicity. That's Specops.

SPECOPS

www.specopssoft.com
/cost-reduction-and-increased-efficiency



TESTING TIMES

Gareth Niblett, Chair of the ISSG, looks at the emotive and often misunderstood topic of ethical hacking, which may also be called IT health check, white hat hacking and red teaming.



There has been debate and disagreement as to whether the term ethical hacking is correct and appropriate. Adding ethical as a prefix to a word that has the baggage of hacking does not placate those that subscribe to a belief that hacking is solely unlawful (forgetting the history and alternate uses of the word). For myself, I have more of an issue with ethical, as

criminals may have a stronger ethical position than some professionals, demonstrated in some recent leaks. Ultimately it's down to authorisation and scope, not terminology.

As seen from numerous recent large-scale intrusions, seemingly backed by state-sponsors, spammers and fraudsters, failure to test adequately can be a factor. Only once you start with a known secure system or service can you look to keep it that way.

It's mine, I can do what I want

Restrictive laws can give those that wish to tinker and open up closed and proprietary systems a significant legal headache, even when only trying to restore a feature removed by the manufacturer. Copyright (monopoly rights) was originally conceived as a protection against duplication. Once you've bought, say, a games console why should rights of fair use to modify or adapt be so limited?

There is a lot of discussion around what responsible disclosure entails, and not everyone agrees (even on the name), but on the whole it is reporting the finding in a responsible way, usually to the site or vendor, and providing sufficient time to develop, test and deploy a fix before announcing it to the world.

Gareth Niblett is Chairman of the Information Security Specialist Group (ISSG).

www.bcs-issg.org.uk

FURTHER INFORMATION

Information Risk Management and Assurance Specialist Group:
www.bcs.org/groups/irma

BCS security portal:
www.bcs.org/security

ISNOW online:
www.bcs.org/forum/isnow



WHAT'S IN A NAME?

Michele Daryanani MBCS explains the difference between a penetration tester and a criminal cracker.

Not too long ago, I was down the pub trying to explain what a penetration tester does to make a living. After a brief explanation, I was confronted by a charming young lady who said something on the lines of 'Shouldn't you be more secretive about being a criminal? After all, a bank robber would not tell me that they rob banks when I asked what they do...'

This left me a little lost for words. No matter how hard I tried to explain that we had permission to do what we did, she wasn't happy. To her, a hacker, a cracker, a penetration tester were all the same thing – a criminal. I hasten to add she used the words criminal mastermind, which made me feel a little better, but still a criminal. Regardless of whether one has permission,

in her eyes, 'hacking' is immoral and should not be done.

Crack or breach?

The day after one of my clients proudly presented a vulnerability scan report as audit proof that they do penetration tests. While frustrating, this got me thinking what is the difference between a vulnerability scan, a penetration test and a criminal cracker (to use the right term) or a breach?

The easiest way to explain it is to stratify them. At the lowest level, there is a vulnerability scan, which is an information gathering exercise. These can be intrusive or non-intrusive, but in all cases are mostly automated. Without delving into too much detail, the traditional vulnerability scan

can be defined as a port-scan on steroids. Increasingly often, vulnerability scans nowadays are starting to include web-application scanners, network scanners and database scanners (amongst others).

In the most basic form, a vulnerability scanner will perform a black-box port-scan on a host, and then compare the responses with a list of known vulnerabilities to identify any known vulnerabilities. As scanners get more advanced, there has been more of a push in automating a penetration tester's functions, and some scanners have started two further lines of data-gathering. Nominally, these come in the form of white-box scanning (i.e. where the scanner has some prior knowledge



moment and back into history, to Austria in 1998 to be precise. The Sissi Star was a 10-pointed jewelled star, protected by an alarmed case, armed guards, a weight-sensitive pedal and bulletproof

system. A very charismatic client once told me that if he ever got a blank report from a penetration test (i.e. one where there were no vulnerabilities found), he would expect the tester in question to be fired.

A very charismatic client once told me that if he ever got a blank report from a penetration test (i.e. one where there were no vulnerabilities found), he would expect the tester in question to be fired.

glass. It was deemed to be 'un-stealable' until it was stolen, by someone who gained access to the room by parachuting onto the roof. The ironic part is, no-one noticed the theft until two weeks later, and Blanchard (the thief) didn't get identified with the theft for years (and many thefts) later. To cut a long story short, most of the Blanchard's victims did not know how vulnerable their security was until he demonstrated it; and in some cases, until he was captured and explained how he masterminded the crime.

To put it simply, the banks, shops and other institutions in question had spent sizeable amounts of money on security, but had no real way of testing said security until someone attempted a heist. Similarly, organisations spent sizeable amounts of money on securing their digital estate, but until someone tries to break the system, there is no way to validate its security.

Penetration tests don't come without risks though. If the test is done on live systems, as it often is, there is always the possibility of damage to the system. I would argue that the risk is justifiable as the worst a penetration tester can do in a controlled scenario is never as bad as a criminal could do; as a criminal breach would then lead to a loss of reputation, financial loss and potentially worse. This risk can be mitigated by choosing a penetration tester carefully, with experience being one of the key factors. I would strongly advise against hiring the latest cracker who broke into the system, as technically minded as they may be.

Cracker

This brings us to my last point – criminal breaches. I was once told that the difference between a criminal cracker and

I was once told that the difference between a criminal cracker and a penetration tester is in the title of the pieces of paper they carry. That is to say, a penetration tester has authorisation to break in.

of the system) and invasive scans. While these can provide some added benefit, the downside is that an automated tool can be very destructive, especially when performing invasive scans - i.e. those where, to identify vulnerabilities, the scanner needs to attempt an exploit.

This starts bringing us into the world of penetration testing. In the loosest sense, a penetration tester will start with a data-gathering exercise, nominally a vulnerability scan, and then take this one step further, by exploiting the vulnerabilities and quite literally testing the system.

Un-stealable

Stepping out of the technical realm for a

That is where a penetration tester comes into play. In a similar way to a software beta tester, a pen-tester will try to find a point where the system breaks. Exploiting the flaw, the tester will then attempt to find the worst case scenario. The exploit is then documented, usually along with a mitigation strategy and recommendations, and the report is returned to the customer.

While not a final and decisive proof of security, a penetration test can add an extra layer of checking. In the same way that it is highly unlikely that a beta tester cannot identify and fix all the problems in a short/limited amount of time, a penetration tester will most likely not find all the issues – but a good tester should be able to offer advice on any strengthening just about any

a penetration tester is in the title of the pieces of paper they carry. That is to say, a penetration tester has authorisation to break in, while the criminal should expect an arrest warrant. While an oversimplification, I can't say I totally disagree with it. Arguably, the addition I would have is that a true penetration tester has an undeniable sense of ethics and morality. I say arguably simply because a penetration tester can do a perfect job without either ethics or morality, but would you really want to let a 'criminal mastermind' loose?

For more articles go online to:
www.bcs.org/articles



EXPOSING VULNERABILITIES

WikiLeaks has caused a lot of controversy, but there are security issues to be learned from it says Dr Christopher Laing CISSP CHFI NUWARP Project Director and Digital Security Programme Leader at Northumbria University, Newcastle upon Tyne.

Back in 2007, very few people, well apart from the readers of *The Guardian*, had heard of WikiLeaks, or indeed Julian Assange. Just for those that still don't know, Julian Assange is the main spokesperson and Editor-in-Chief for WikiLeaks, and WikiLeaks publishes anonymous submissions from private, secret and classified sources, in essence WikiLeaks is a digital 'whistleblower'.

In its time WikiLeaks, has been awarded numerous accolades, starting with The *Economist's* New Media Award in 2008, and

the Amnesty International UK Media Award in 2009. In 2010, WikiLeaks was listed as one of those '5 pioneering websites that could totally change the news' by the *New York City Daily News*, while in the same year readers of *TIME* magazine voted Julian Assange their choice for *TIME's* Person of the Year.

Spread of information

At the beginning of that very same year, the US Secretary of State, Hillary Clinton speaking on internet freedom, at the The

Newseum, Washington, DC, pointed out that 'the spread of information networks is forming a new nervous system for our planet.' She went on to outline a vision in which digital whistleblowers would champion transparency; 'helping the people discover new facts, and making governments more accountable.'

However, by the end of 2010, less than 12 months later, things had changed.

Speaking at a State Department press conference Hillary Clinton this time condemned those same digital

whistleblowers, claiming that digital transparency was an 'attack on the international community', while at the same time Sarah Palin, a former vice-presidential candidate, called for Julian Assange to be hunted down by American special forces and assassinated, demanding that he should be 'pursued with the same urgency we pursue al-Qaeda and Taliban leaders.'

However, irrespective of the fate that awaits Julian Assange, WikiLeaks was a phenomenon. Only the internet and its associated technologies could have provided the necessary environment for its conception and birth. Whether it will see its teenage years is another matter.

Children

But as a phenomenon, WikiLeaks has spawned some interesting 'children':

- OpenLeaks (www.openleaks.org), a WikiLeaks clone created by Assange's former deputy, Daniel Domscheit-Berg.
- Brussels Leaks (www.brusselsleaks.com), an interesting title, but I understand it is directed at the European Union, in an attempt to shine the light of the public domain into the shady and shadowy inner workings of the EU – William Hague must be jumping up and down with delighted anticipation.
- TradeLeaks (www.tradeleaks.com), founded by another Australian, Ruslan Kogan, with the aim of having a 'WikiLeaks effect on trade and commerce'.
- Balkan Leaks (www.balkanleaks.eu), founded by a Bulgarian, Atanas Chobanov, with an obvious aim of fighting fraud, deception and corruption within the Balkans.
- Indoleaks (www.indoleaks.org), an Indonesian site, focusing on publishing secret or classified documents anonymously obtained from the Indonesian government.
- RuLeaks (<http://ruleaks.net>), originally providing Russian translations of the WikiLeaks released documents and cables, but according to the *Moscow Times*, RuLeaks has found some Russian whistleblowers of its own – although I haven't been able to access the site.

I'm proposing that in the spirit of internet freedom, the world needs a computing and software application equivalent of

WikiLeaks, let's call it DigiLeaks. DigiLeaks, would champion the transparency of digital and software vulnerabilities. It would allow for the public dissemination of software security vulnerabilities that often go unreported, or even worse unresolved. In essence DigiLeaks would act as an

Hillary Clinton pointed out that 'the spread of information networks is forming a new nervous system for our planet.'

intermediary, protecting the whistleblower from identification.

The whistleblower having 'discovered' a software vulnerability, could anonymously post the information to DigiLeaks, and DigiLeaks in a manner similar to WikiLeaks, could then subsequently leak that information to the computing media. No doubt some of the readers who are computing journalists are looking forward to day when they can announce with a 'world exclusive' banner, another and previously unknown security vulnerability with Internet Explorer, Safari or Mozilla Firefox. Just as, I am sure, some of you are asking for my internet to be cut off for daring to suggest such a heinous act.

Accountable software

But wouldn't such an approach 'help make software corporations more accountable for the testing and quality of their products'?

Wouldn't such an approach help make software corporations more accountable for the testing and quality of their products?

It may even generate greater interest in the use of formalised methods in the software development and testing life cycle; possibly even 'assist' in the development of the much talked about ISO/IEC 29119 Software Testing, the new international software testing standard.

Obviously such an approach is not without potential criminal prosecutions, and we would have to ensure that DigiLeaks was beyond any technological or legal attack – but that shouldn't be too difficult, after all, we are computing specialists. 'Comrades, are you with me?'

upSploit

I didn't think so, in that case let us investigate a third way, and make use of an often overlooked resource; our students. In particular, my students, and in this case,

one specific student: Thomas Mackenzie. Thomas Mackenzie is the spokesperson and Editor-in-Chief of upSploit (www.upsplit.com), which is a vulnerability advisory platform. Some of you may have used upSploit, and some of you may have been on the receiving end

of an upSploit advisory notice. In essence upSploit is the nearest 'real-life' working equivalent of DigiLeaks, but with one major difference. upSploit works by acting as an intermediary between the individual who discovered the vulnerability and the vendor. It provides an automated advisory management system, that takes the information provided and alerts the vendor to the identified security vulnerability. upSploit also makes use of responsible disclosure, that is vendors have 180 days to respond to the advisory that has been sent to them.

The vendors are reminded of this every month via email. In the final month, an email is sent every week, and in the final week, an email is sent every day.

Each email alerts the vendor to the vulnerability, highlights the number of emails that have already been sent, the date on which they were sent, and how

many days they have left to respond. If the vulnerability has not been addressed by the end of the 180 day period, the advisory is published to the advisory management database.

Each advisory has two states; confirmed and unconfirmed. A confirmed advisory indicates that the vendor has responded and the vulnerability has been addressed. An unconfirmed advisory, which acts as a 'rumour', indicates that the vendor has not responded to the advisory, and allows the computing public to confirm the existence of the vulnerability themselves. A rather neat solution to a difficult problem; what are your thoughts?

For more security articles go online to:
www.bcs.org/articles



DISCLOSURE AND PLAYSTATIONS

When flaws are found in software systems, to disclose or not to disclose is the question that needs to be answered says Ken Munro from Partner at Pen Test Partners.

Ethical disclosure is an issue that security researchers have been struggling with for years. You find a new vulnerability in a certain vendors software. What do you do next? Do you:

- post it to a forum for verification?
- report it to the vendor yourself?
- sell it in a vulnerability market; an outlet amusingly referred to as an '0-bay'?
- or sit on it, write a zero day, and go hack other companies with the same software?

Most software vendors have improved their response to researchers reporting vulnerabilities, but it's still a long way from perfect. Consider the following:

You report the vulnerability, the vendor acknowledges your finding, verifies it, then explains that it's going to take 12 months to issue a fix. They ask you to keep quiet about it in the meantime. So what if someone else finds the same bug in the meantime? What if someone has known about it for years, and has been quietly exploiting businesses?

Not very ethical, is it? What's the alternative? Well, how about posting it publicly at the same time as posting to the vendor, or maybe giving them a couple of weeks to get a patch out. The vendor goes nuts, companies complain that there's no patch available, the exploit is quickly picked up by Metasploit and every script kiddie under the sun now knows about it.

However, the usual reaction from

the vendor in this scenario is to get a workaround published quickly, and a patch out much faster than otherwise.

I had a similar problem myself a few years back – I found a set of really significant vulnerabilities in a building management controller. One could unlock doors, set off fire alarms, turn the heating off, pretty much anything. I rang the company, emailed them, wrote to them, called support, you name it. However, their business was about physical security, not IT security. They didn't have anyone that dealt with securing the systems they sold to clients. I drew a blank, all I could do was brief a government agency and a couple of relevant security associations. Putting my research out in to the public domain would have been irresponsible, as I had no faith in

the vendors ability to do something about it.

PS3 hacking

Which leads me on to some of the high profile 'hacks' of games consoles and other systems. Probably the most significant case is the recent publication of the master keys to Sony's crypto protecting their PlayStation 3. The firmware allowed anyone to install other operating systems on the PS3. This option made installing homebrew operating systems easier, and no doubt also facilitated the use of cracked content.

Hence, Sony updated the firmware to prevent this. However, this move really annoyed many users, and set parts of the community on a path to target the console. A team known as fail0verflow presented a method to compromise the device master key, effectively opening the console up.

This research took considerable effort, and its open publication helped numerous legitimate researchers understand new routes to compromise systems. To their credit, the group did not publish either the key, or the exact details of the attack. Their intention seemed to be more about the concepts that their research opened up, rather than punishing Sony.

You might see this as ethical disclosure. Unfortunately, a second researcher then replicated the attack, and published the master key; unethical disclosure.

Very similar efforts went in to the crack of the TPM chip preventing the use of third party controllers with the PS3. A researcher (Chris Tarnovsky) appeared a little annoyed that non-OEM controllers couldn't be used, so started working on the protection mechanisms. After several months of work, he not only worked out how you would use other controllers, he also broke the protection that TPM offers to secret encryption keys on numerous other laptops, devices and systems.

Infineon, the vendor of TPM chips, was rather red faced, and implemented upgrades to its system. Doesn't do much to help the enormous existing population of TPM equipped devices though.

Phillips Mifare, the technology behind the Oyster card, was compromised some years ago also. Again, a fascinating physical attack against the chip itself revealed issues with the cryptography that permitted cloning in some circumstances.

Does this research benefit us? I believe it does, as if there are more ethical

Implement security controls to distract the casual hacker and accept that a portion of the customer base is going to pirate games and content, whatever you do about it.



researchers out there are doing this, then those with criminal intent will be at it too. Further, particularly in the case of cryptography protecting state secrets, there are bound to be foreign powers at work in this space also. Would we be better off with Pandora's Box kept firmly shut, so that only those 'in the know' can attack critical infrastructures and businesses? I don't think so.

DRM circumvention

Then we have the Digital Millennium Copyright Act and EU Copyright Directive, which were supposed to keep a lid on DRM circumvention. Wonderful in theory, but my personal view is that the criminal underground will carry on as before, and all you really achieve is restricting the activity of the semi-ethical researcher. The result is that research is driven underground and we all lose out.

Yes, disclosure causes problems for us all, but I believe that we would be suffering far worse problems if we didn't have disclosure. It's time for vendors and manufacturers to step up, and deal with the challenge of disclosure, rather than trying to keep a lid on it by threatening

legal action.

Why not pay a significant sum to a researcher that finds a bug in a system, on condition that they keep quiet for an agreed period of time? It'll be a whole lot cheaper than the legal fees they would incur trying to gag them otherwise.

So, my conclusion is that the most sensible route for any console vendor is probably to let the hacking community do their 'homebrew' things if they want to. Implement security controls to distract the casual hacker and accept that a portion of the customer base is going to pirate games and content, whatever you do about it.

If you up the stakes, as in Sony's case by removing the ability to install homebrew operating systems on the PS3, then the hacking community will make that device a target for their considerable research efforts. What was the result of their efforts to lock down the device? Sony's master keys were published. Who lost out, in my opinion? Sony.

For more articles go online to:
www.bcs.org/articles



MULTIPLE DEFENCES

When it comes to keeping your business secure, although penetration tests are essential you can't rely on them alone, says Ben Ward MBCS.

Many businesses spend large amounts of money on cutting edge security devices to protect their systems from compromise. Once these devices are in place, they then invest in penetration tests to find any chinks in their armour. Many businesses also recognise that their data is vulnerable to attacks from employees, so complex monitoring and auditing systems are implemented. There are, however, some types of attack that can't be prevented by throwing money at technology.

It could happen to you

It's Monday morning, you've had a stressful weekend and you're running late for work. As you push through your workplace's front doors, another flustered individual stands behind you holding a large box

while fumbling in his pocket for his security pass. Being the helpful person you are, and understanding that Monday feeling, you hold the door open for him as you disappear off to your desk without a second thought.

In the IT department, the IT manager carries on with his daily tasks secure in the knowledge that the business has passed its annual penetration test with flying colours. The IT systems are impenetrable.

Meanwhile, the individual with the box approaches the reception desk and asks for the CFO. He says he has a package for him and has been told that there is a package in the post room for him to collect. The receptionist disappears into the post room to check for the package. When she comes out empty handed, the individual

reads out the address he is after, realises he has made a mistake, and exits the building. The working day carries on.

A week later, it comes to light that a massive amount of sensitive company data has been stolen. The source of this information leak is tracked down to the receptionist's PC. On closer inspection, a hardware key logger device is discovered in the back of the PC. This device has recorded all key strokes and transmitted the data to an IP address on the internet. The IP address is untraceable. The company's credibility is destroyed, and soon after it ceases trading.

Keep your friends close

It is a scary fact that the majority of IT system attacks are perpetrated from within

the business. Disgruntled employees, ex-employees and unscrupulous competitors can be a huge risk for any business. While the business spends massive amounts on complex technology such as firewalls, virus scanners and internet proxies, the real threat can be from something as simple as staff sharing information with friends and acquaintances outside of the business.

Then there is the threat from social engineering attacks, as illustrated above. No amount of technology spending can decrease the risk from these crafty and dangerous tactics. The reason that these attacks work is that it preys on human nature. It is natural for someone to assist a person in distress, to trust someone who looks like they belong at your place of work.

In 2009, Colin Greenlees from Siemens staged a social engineering attack at the request of a FTSE listed company and obtained some worrying results. He reported: 'It is all about confidence. I walked into the building [of the FTSE-listed firm] having an imaginary conversation on my mobile and the swipe-card operated lift was held open for me by what turned out to be the managing director, I remained there for five days working from a third floor meeting room.'

In light of these incredibly devious and cunning tactics, what can be done to protect your business's valuable data assets from compromise?

And your enemies closer

To protect your systems from internal threats, there are five important steps to take:

First, we need to recognise that proper training of staff and simple security processes can be far more effective than any technology that could be utilised. Even the most sophisticated technology will fall down when faced with intelligent and determined adversaries, who may be well funded by competitors or criminals. An internet proxy will not stop theft of paper documents. An event log analyser will not prevent a wily hacker pretending to be from the IT service desk and asking for a password from a user. Train your staff to not give out passwords over the phone, to never write down passwords, and to never share their logon details with a third party.

Second, the culture of the business may need to change. Staff will need to have a

In light of these incredibly devious and cunning tactics, what can be done to protect your business's valuable data assets from compromise?



This device has recorded all key strokes and transmitted the data to an IP address on the internet, which is untraceable. The company's credibility is destroyed, and soon after it ceases trading.

level of paranoia about every unrecognised face they see and must actively challenge people who do not appear to have proper identification. They must also be encouraged to report members of staff who they notice are not conforming to the business's security policy.

Third, carry out regular internal penetration testing in the form of security audits. The business will need to grant specific permission for this, as it could be viewed as hacking, even though the staff carrying it out may belong to the internal IT team. Assume the identity of a very low level user and then attempt to access confidential data. If you do manage to access this data, attempt to either copy it or send it out of the business.

Fourth, create a strongly worded acceptable use policy spelling out penalties for policy contraventions. Ensure that

this policy is refreshed and resent to the business at regular intervals. Ensure the business knows about the focus on information security by regularly emailing security related newsletters or mail shots to staff.

Fifth, use your technology! Implement measures to block known file uploading sites, block certain email attachments, monitor every activity on the network and alert on unusual activity. Discover what business as usual activity looks like and then jump on any unusual activity you find.

By following the above pointers, and continuing to invest in external penetration tests, you can be sure that your valuable systems are safe... for now.

For more articles go online to:
www.bcs.org/articles



JUMPING FENCES

Having been on both sides of ethical hacking/ penetration testing debate, Lannon Rowan, Security Consultant from Orange Business Services, provides a personal insight into the roles.

When I started working in this area it was a result of learning about hacking during my spare time. As a result having to do this for my day job was extremely appealing. The term ethical hacking always made me smile as I was now being paid to deliver testing for customers. Is this the answer to the question perhaps?

The transition to a security consultant delivering ethical penetration testing was interesting and challenging. New rules had to be learnt, and quickly, and they ranged from developing a clear understanding of business or the reasons why a test would be asked for. Taking time to learn about the customer and how they did security was good in order to understand their

requirements in more detail.

Who the stakeholders are in the test purchase is very important as this will help the understanding client requirements and the expected format or what level is expected after the test is completed. It is also surprising how often the messenger is shot as a result of delivering bad news to customers.

Making the scope for the test is clear and stops any disagreements at the end of the test. It is also a safety net to ensure that any testing results will meet customer requirements.

Make sure the client provides the testing company with a letter stating the parameters of the test and that is was

authorised. This is often described as the 'get out of jail' letter. Surprisingly this is not always provided.

The client being contactable during the testing times is essential in the case of any incidents relating to the test. These incidents can involve service impacting production systems that are part of the testing scope. Often testing is scheduled for after hours to limit this.

Scanning tools

The other thing to consider is that all firms or people conducting penetration testing are not created equal. By this I mean there are firms that offer ethical hacking and simply run a commercial



Types of test

There are many options that can form part of a penetration test. For example a basic test involves testing a company's external IP address range and producing a report of the results. This report usually rates the issues or vulnerabilities found by high,

to achieve system penetration.

Other areas that can also be used are Wi-Fi, social engineering and physical testing of buildings. There are also different levels of testing that can be conducted and it is easy to get bamboozled if you are not totally clear about the test

Making the scope for the test is clear and stops any disagreements at the end of the test. It is also a safety net to ensure that any testing results will meet customer requirements.

medium and low. This type of test is usually done at a low cost and often as a loss leader by companies in the hope of getting further tests. These follow-on tests have larger scopes or they are specialist or niche that take longer to deliver.

Other areas that can be tested are remote access devices or modems. Modems are often not secured and can be exploited to gain access onto a network. Internal tests are conducted where the tester is given local access to the network and part or the entire internal network is scanned. Scanning would look for systems that have security vulnerabilities. Passwords are able to be scanned to see if user passwords are easy to guess or to see if the account lockout and other controls

and deliverables you require.

Before any testing is started legally binding paperwork must be completed in order to protect both parties. The majority of testing providers should have this documentation as standard.

Questioning the ethical part of hiring a firm to do the test is important and the firm being hired must be evidenced by a track record and reference clients if possible. Due to the nature of the work being conducted many of the testing reports remain client confidential after a test and so a sanitised version might have to suffice. Example reports are also very important as this will provide clear evidence of the tester's ability to articulate their findings. There will always be a

It is important that the company being requested to do a penetration test has clearly defined test criteria methodology. This will make it easier to define a testing scope, type of test and what the deliverable is

scanning tool. The report from the tool is then given to customers as the deliverable for the test. The problem with this is there is no consistency checking of the tool results. What is also important to consider is how the results impact the organisation? Using this knowledge the results should then be reported to the appropriate level.

The other side of the scale are firms that have exceptionally skilled staff doing testing. These often have staff that are reformed hackers and understand how to initiate and conduct a successful test. It is important that the company being requested to do a penetration test has clearly defined test criteria methodology. This will make it easier to define a testing scope, type of test and what the expected deliverable is.

are functioning correctly. Most testers in my opinion should be able to deliver testing in these areas to a reasonable level.

Objectives

Consider the testing to have one of two objectives to either scan and report discovered vulnerabilities or to scan and attempt penetration of the systems. The reporting of these test is more detailed and the terms of penetration is agreed beforehand. Testing can be in the form of copies of files on the vulnerable system or placing a file on the system.

Often customers would want to know how the penetration is achieved in order to retest after the affected system is patched. This is where providers of vulnerability tests are divided between those that scan and those that are able to use the results

problem if a tester conducts a test but is not able to clearly report it.

The term ethical hacking, while not perfect, is the most appropriate for this type of service. Ethical hackers are hired to do the work and they provide a service to their clients. While all testers might not be created equal these tests provide valuable insight and assurance of the current security during the test. The day after the test conclusion new exploits may be discovered and the network could be at risk. Testing that will fully meet requirements can be achieved if the initial requirements for the test are clear from the start.

For more articles go online to:
www.bcs.org/articles



E-PRIVACY, FINES AND THE ICO

Charlotte Walker-Osborn and Laura Friend Technology Group, Eversheds LLP, discuss the implementation of the amendments to the E-Privacy Directive and ICO regulation.

EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector was introduced in July 2002 (E-Privacy Directive). Article 5(3) permits member states to store cookies, spyware or other tracking devices on the equipment of internet users and access stored information only if certain requirements have been met. The internet user must be provided with clear, comprehensive information about the processing including its purpose, and must have the opportunity to refuse such processing (informed opt-out). The UK implemented this directive through the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Article 5(3) was amended in 2009, changing the requirements from 'informed opt-out' to the highly criticised 'prior informed opt-in'. Following this revision, cookies, spyware or other tracking devices will only be permitted if the internet user affected gives consent after having received clear, comprehensive information about the purpose of the processing.

These amendments must be implemented in the member states by 25

May 2011. In the UK, the Department for Culture, Media and Sport is leading implementation and the Information Commissioner's Office (ICO) will be responsible for regulation.

In an ICO press release the Information Commissioner, Christopher Graham, urged UK businesses and organisations running websites to be prepared for the new law. However, he commented that 'the internet as we know it today depends on the widespread use of cookies and there are of course legitimate business reasons for using them'. This appears to have influenced the ICO working with the government to ensure changes benefit consumers without causing unnecessary burdens on businesses.

This concern was evident in September 2010, when the Department for Business, Innovation and Skills published a consultation that detailed the government's approach to the implementation of the directive. The consultation advocates flexibility of the ICO to adjust to changes in usage and technology and rejects a strict 'opt-in' system. Although prior consent of the internet user is required, Recital 66 of the

directive provides that this requirement can be satisfied if the internet user accepts cookies through the appropriate settings in their web browser.

The ICO notes that the government acknowledges that 'it will take time for meaningful solutions to be developed, evaluated and rolled out' and that businesses are unlikely to be ready by the implementation deadline causing uncertainty about the extent of their legal obligations. Businesses may be reassured that the ICO is not expected to take enforcement action in the short term whilst businesses and organisations work out how to address their use of cookies.

However, the European Commission's reaction to the suggestion of a transitional period without enforcement of the new law despite its implementation is as yet unknown.

Businesses should look out for the draft regulations and consider what changes may be needed to their websites in order to ensure compliance.

ICO fines

In February the ICO once again used its power to impose fines of £80,000 and £70,000 respectively on Ealing and Hounslow Councils.

Ealing Council ran an out of hours service for both councils, conducted by staff working from home on laptops. Two unencrypted laptops were stolen from an employee's home that contained details of around 1,700 individuals. Despite there being no evidence that the data was accessed and no complaints were received, there had been a significant risk to the clients' privacy.

Ealing Council breached the DPA by issuing unencrypted laptops to employees despite this breaching its own data protection policies. Hounslow Council breached the DPA for failing to monitor the procedures used by Ealing Council to operate the service. Both councils employed inadequate monitoring and failed to conduct sufficient checks to ensure compliance with policies.

Please note that the information provided above is for general information purposes only and should not be relied upon as a detailed legal source.

www.bcs.org/legal

information security

foresight in a complex environment

Master complexity and gain the foresight you need to safeguard your business at Infosecurity Europe 2011

- Demonstrate clear thought leadership to ensure security is high on the corporate agenda
- Achieve visibility of your mobile workers, cloud providers and web of third party suppliers
- Clearly navigate and understand increasingly complex legislation
- Deliver security to drive and enable clear business growth

Register FREE* to visit at www.infosec.co.uk



Follow us on Twitter
@infosecurity



Join the Infosecurity
Professionals Group



Join the Infosecurity
Europe Facebook Group

Europe's NO.1
Information
Security Event

19-21 April 2011

Earls Court

London UK

Organised by:

Scan this QR code for quick registration



*Visitor registration is free online before Friday 15th April. Onsite visitor registration £20

REGULAR CHECK UPS

When it comes to testing, in the world of information security **John Mitchell** believes that you should test more often than once a year.

In order to keep IT systems secure most organisations force frequent password changes on the basis of minimising exposure to a compromised account and yet they are willing to leave their entire network exposed for up to a year. I recommend regular penetration tests to my clients.

Regarding the actual testing, we once conducted an experiment where we had one group who looked at the potential exposures from a theoretical viewpoint and another group that conducted the actual ethical hacking. The theory group spent some three weeks examining the infrastructure, the firewall configuration and the tools available to hackers. They suggested a few tweaks, which were then applied.

We then let the hackers loose and they were into the network within 20 minutes. This gulf between theory and practice brings me nicely to the gulf between auditing controls and actually examining the results of control failures.

For my non-audit colleagues, a quick

briefing on the system based audit approach: The underlying process comprises four stages: gain an understanding of the system; identify where the controls should be to minimise risk; ascertain whether there is a control actually in place; test the control for its effectiveness in managing the risk.

It takes a bit of time, but is pretty surgical in its approach. I tend to short-circuit this process by going straight to the last bit, which is testing control effectiveness. I do this by hacking the data.

All systems rely on good quality data. Indeed the only rationale for any system is to process the data to produce reliable information for decision making.

Therefore, for all systems we should know the data quality rules. I use this information to peer into the databases using a variety of analytical tools to ascertain whether the data complies with the rules. If it does, things are likely to be OK from a control viewpoint. If they don't, then I know that there is a control failure somewhere along the line.

The full system-based approach is akin to my earlier description of the theoretical approach to perimeter security, whereas my looking at the data is akin to the actual penetration test. The challenge with any theoretical approach is that you are limited by your own imagination, whereas a practical attack by someone else will not have the same constraints.

The system-based audit approach tends to review a process in isolation and may miss key risks from outside the immediate area. My approach may well detect data irregularities as a result of unauthorised manipulation by (say) IT staff or hackers.

Discrepancies

I have found some really weird control deficiencies simply by examining the data: the £80 billion asset as a result of poor input validation (should have been £8,000); the insurance fraud because the perpetrator knew that claims under \$1,000 were paid without investigation (never rely on secrecy as a control mechanism); the corrupted links in the pensions database that meant that contributions were not going to the correct fund; the incorrect depreciation that overstated the balance sheet; the incorrect debt ageing that had an adverse impact on the uncollectable debt provision.

However, the best one was the Unix compiler that thought that one divided by one was 0.99999666663333. Not too much of a concern for a financial calculation, but what if it was on a missile guidance system? Target Baghdad, hello Tel Aviv.

It's also quicker and cheaper, which is something my clients like. The use of 'ethical' hackers will almost certainly be less than the cost of a penetration by a 'black hat'. Not least is the embarrassment caused when an amateur hacker breaks into your systems. This brings me back to my point that you should never rely on secrecy of the process as a control mechanism. Much better to assume that the enemy knows your processes at least as well as you do. The trick is to make it so difficult that the cost of the attack is greater than what could be gained.

Prevention has to be the name of this game as detection may be too little and too late.

For additional articles please visit:
www.bcs.org/articles



The Open University

“ Develop your IT workforce without disrupting the working day ”

Our professional development programmes can give your organisation a competitive edge and your employees the relevant practical, technical and managerial expertise they need to work in today's constantly changing global IT & Telecoms environment.

Solutions range from IT professional practice, enterprise software development, information security management, systems integration, computer forensics and project management, to awards in IT business and management including our triple accredited MBA.

Your employees can study outside of working hours using the latest learning technologies alongside ongoing support from us and what they learn one day can be applied the next.

Did you know?

- Our specialist programmes are developed by experts in association with professional bodies, sector skills councils, IT vendors and IT & Telecoms employers
- We're the largest and fastest growing Cisco Academy in the UK and among the top 5 universities for computer science
- Our triple accredited business school is in the world's top 1%.



CYBER SECURITY CHALLENGE.ORG.UK 



vmware IT ACADEMY



intellect member



Microsoft IT Academy Program



bcs Educational Affiliate



Accredited by Association of MBAs

e-skills uk

CompTIA

Develop your workforce

- ▶ www.openuniversity.co.uk/it
- ▶ corporate-enquiries@open.ac.uk
- ▶ 0845 758 5097 Quote: ZAMAAC

INSPIRING LEARNING



UNIVERSITY OF
OXFORD

part-time study in:
network security
trusted computing
security design
forensics
people and security

msc in software and systems security
www.softeng.ox.ac.uk/security