ETHICAL HACKING – an oxymoron or an accepted industry term?

> "A Hacker is any person who derives joy from discovering ways to circumvent limitations."
> Bob Bickford (computer and video guru) in *MicroTimes*, December 1986

BCS Position

Ethical hacking should **not** be considered to be an accepted professional industry term. If Penetration Testing is what is being taught, then that is how it should be labeled – rather than seeking to use marketing spin to gain traction and credibility within an industry that is seeking to improve its professional image. A teaching unit with the title "ethical hacking", whilst headline grabbing and engaging students, would not be a responsible way forward.

1. The original request

1.1 In January 2008 BCS received a request from Northumbria University: they were "looking at the subject of Ethical Hacking and arguing [internally] that it is an industry accepted term (for penetration testing / red teaming etc). The university Learning and Teaching Committee and the university's Academic Board asked that a perspective be sought from the professional body on the title / subject.

1.2 This paper details the response from the BCS Security Forum Strategic Panel (SFSP), following a considerable e-conversation amongst its membership. Given that the BCS is the leading professional body for those working in IT, it is important that a request for an opinion on such a contentious subject is met with measure and sense, rather than accepting the available wisdom, or in this case, often sensationalism.

1.3 Consultation has also been undertaken with the BCS Ethics Forum.

1.4 So this paper asks that the reader see *through* the Hollywood glamorisation of the roles individuals seek to take and to strike a professional furrow through the muddy fields.

2. Detection versus prevention?

2.1 There are lots of security glossaries around. Microsoft has one but it doesn't include the word testing. SANS has one that includes penetration testing but describes it as merely testing the external perimeter security. The IETF has a better definition for penetration testing, but falls down when it comes to "hacker" by describing it as "someone who figures things out and makes something cool happen". A selection of definitions is provided in Annex A at the end of this paper. Either way, there is significant controversy: http://en.wikipedia.org/wiki/Hacker_definition_controversy.

2.2 No matter how many explanations are given, in line with the contradictions in the definitions, it remains difficult to see the wood for the trees. In general, the term hacker/hacking is used and understood by many in two different ways: (i) expert (ii) someone who gains unauthorised access to a system. The first meaning is usual amongst programming/security professionals, the second is a general public (and student) understanding usually arising from press coverage.

2.3 Penetration Testing and IT Health Checks are carried out under prescribed schedules against known risks and threats. Testers look for ALL the weaknesses in a system which require fixing, given the risk appetite of the organisation. They are geared to provide system/product owners with information about vulnerabilities and weaknesses. They are carried out in a set timescale that is determined by the funds available to the Testing Authority. Testing shows what is not working 'properly' in some context; fixing is a process whereby what is deemed necessary to work is made to work, again in some context, risk appetite being just one such context. Pen testing can be carried out on all new network connected products that are deemed to have a certain risk level – i.e. they contain or may access sensitive information that could impact an organisation or its customers.

2.4 Penetration testing is not hacking. It aims to identify weaknesses, not set out to access or modify data. The objectives are different, but many companies selling penetration testing are actually selling in depth vulnerability assessments often just carried out from outside the external perimeter of the organisation and only probe the Internet side of a firewall, web and email services.[1]

2.5 The confusion between penetration testing and vulnerability assessment / scanning - by both the people marketing and paying for such services – obviously doesn't help the wood from trees problem. Some organisations provide comprehensive IT health checks, which include war dialling (testing the IT access via the phones), social engineering (testing IT access via manipulating people to give away information) and physical attacks, e.g. dumpster diving.

2.6 IT Health Checks include (or can include, clients choice based on costs) in depth vulnerability assessments carried out both sides of a security perimeter together with a review of firewall rule sets and a review of operations and associated documentation. A purist and limited view of penetration testing is to find a vulnerability that can be exploited such that a named file can be copied from a system and a file placed in a named location (i.e. to prove penetration was successful)[2]. Note that once an exploitable vulnerability has been found, that is the end of the exercise, you don't go on and look for other vulnerabilities or whether identified vulnerabilities can lead to dependent vulnerabilities.

2.7 Ethical Hacking is not the same as Penetration Testing or IT Health Checks – it is definitely a misnomer; there is a great divide between the two. As the name implies "hacking" can be in many forms, brute force attack, simple attack or prolonged attack. However, it is accepted that the 'ethical hacker' moniker, is a little less opaque than '{white/grey/ blackhat} hacker'; it has gained some traction - e.g. with CEH certification[3] and to differentiate from illegal activities.

2.8 It is also accepted that the aim of some 'hackers' is simply to identify weaknesses, (which was the original use of the term prior to the media using it in place of the term Cracker) - in systems or applications – but they may not use ethical (or lawful) methods in their quest and may also misuse access or data they obtain; or they may be borderline ethical or unethical and be called

[1] It is accepted that this a perimeter defence view of what vulnerability assessment is about; it must be set in a broad context of vulnerability assessment (people, process etc etc).
[2] This is not making any statement about what is or is not a file – i.e. whether code is 'a file'; or a hyperlink is a file etc.
[3] http://www.firebrandtraining.co.uk/courses/ec_council/ceh/hacking.asp

'vulnerability researchers' and publish their findings on full-disclosure sites / mailing lists. Obviously, within a regulatory or legal context, some 'types of data' are illegal under all circumstances unless allowed by a judge or because of a law enforcement role.

2.9 It may be better to refer to 'lawful hacker' to differentiate between legal and illegal hacking, as is done with 'lawful intercept', but then we get yet another term to add to the confusion. At the end of the day, it boils down to semantics and the lack of agreed definitions across the (ill-defined) security industry.

2.10 The ethical hacking industry has grown up specifically because it can be hard for businesses to assess the efficacy of IT security measures without what they perceive to be expert testing. By using widely available tools and sharing all relevant research, the industry keeps as up to date as the crooks.

2.11 By way of illustration, if you assume that 'Robin Hood' was setting himself up as an ethical robber, beyond the legend is a complex moral point whether robbery (an illegal act) can ever be justified on ethical grounds. If you accept that 'hacking' is 'using illegal means to circumvent the security of the system' (which is one of the many available definitions), can this ever be justified by your declaration that you wear a white hat and are attacking the systems only to expose their weaknesses? And if this is not what you are doing, then you are, arguably, not hacking, whether ethically or otherwise.

2.12 However, the wider point at issue within the context of the original request may actually be less about what term is being used and more about what the universities are teaching. Teaching someone how to carry out penetration tests, or how to be part of a red team, or how to find security holes in code reviews, is different in nature to teaching someone how to hack (whether or not there's an "ethical" wrapper attached to the material).

3. Expressions of intent

3.1 By way of expressing some of the finer points of the arguments, the following encapsulates areas of confusion:

⇒ A person is found inside a bank 'tinkering' with the bank vault combination. *Is he a bank robber?*

⇒ A person is found 'rattling' door knobs on people's homes and when a knob turns, he walks in. *Is he a burglar?*

⇒ A person rapidly approaches the driver of an automobile stopped at a traffic light, shows a knife, and tells the driver to get out. *Is he a carjacker?*

⇒ A person trained in software technology spends his livelihood trying to find vulnerabilities in code. *Is he a hacker?*

⇒ A person who exploits software coding errors posts those vulnerabilities on the Internet, rather than provide the vulnerability information to the software manufacturer. *Is he a criminal?*

3.2 Of course, the answer to all of these is, "Was the person engaging in legal activity?" That's always the issue.

⇒ If the bank was closed, and the individual was not hired by the bank to 'check the vault' then by *intent*, he may be perceived to be a *criminal* but in terms of legality, he may only be guilty of trespass or breaking and entering.

⇒ If the person 'rattling' door knobs walks into a home without the permission of the homeowner (person with authority to grant access), then as per the above, by *intent*, he may be perceived to be a *burglar* but in terms of legality, he may only be guilty of trespass or breaking and entering – particularly until he steals something.

⇒ If the person with the knife and driver are not actors for a movie / skit, he's a *carjacker*.

⇒ If the person spends his life finding vulnerabilities and does nothing with the information, he's a "security researcher", *not a criminal*.

⇒ If the person posts the vulnerabilities on the Internet, perhaps he should be considered to be a *CRIMINAL* – particularly if he as removed something, damaged something or shown intent to do so.

3.3 Ethical Hacker? It depends on the facts. However, there is no such animal as a *Security Researcher* who exposes vulnerabilities, and posts them to anyone other than the software manufacturer because in today's world a Reasonable Person would know that the exposure will be taken advantage of by miscreants.

3.4 Context is king - the actions and intent of an individual are the most critical aspect of whether they are a criminal, however they are titled. *Skills* such as hacking, safe-cracking, lock-picking, social-engineering, etc. can all have legitimate or criminal aspects to them.

3.5 Understanding the etymology of the word, it is undeniable that a 'hacker' will still have skills - an enquiring mind-set, with significant knowledge / capability and the ability to take a novel approach to an issue. It is how a 'hacker' uses their skills that determines whether they break the law.

3.6 With regards to vulnerability research and disclosure, if a vendor:

⇒ Fails to acknowledge vulnerability notifications in a timely fashion

⇒ Fails to review notification and confirm vulnerability in a timely fashion

⇒ Fails to accept that there is a vulnerability in their product

⇒ Claims that the vulnerability is 'only theoretical', so will not act

⇒ Claims that the vulnerability is actually a 'feature', which it then refuses to change

⇒ Fails to address / fix vulnerability in a timely fashion

⇒ Fails to disclose sufficient information for customers to verify issue or resolution

⇒ Fails to acknowledge the input of the security researcher in the vulnerability advisory

⇒ Fails to adequately design security into their products and test before release

⇒ Attempts to stifle legitimate research and public discussion of vulnerabilities

3.7 Then who is more responsible for the publication of the vulnerability - the vendor or the security researcher? At least disclosure puts the customer in a position to be aware of and respond to the issue that the vendor was unwilling to address.

3.8 It is important to acknowledge that legitimate security researchers are not the only ones looking for such vulnerabilities. Better that they are published publicly (after the vendor has had sufficient time to respond) than see the trade in zero-day vulnerabilities amongst the criminal fraternity and used against the vendor's customers.

3.9 We must promote responsible research, working closely with vendors. Disclosure by a 'security researcher' that has made insufficient attempts to communicate and work with the vendor in addressing what they have uncovered in their research is unacceptable and irresponsible.

3.10 All of the above postulation is likely to be tested when the Police and Justice Act goes through in April or May 2008 as it will, in all likelihood, include clauses criminalising the distribution of hacking tools.

3.11 The Crown Prosecution Service have produced Guidelines that establish that to successfully prosecute the author of a tool it needs to be shown that they intended it to be used to commit computer crime. The difficulty remains as to how they handle widespread use of open source tools. But ultimately we are back to the issue of intent as expressed previously.

4. Conclusions

4.1 In answering this question, the group of professionals consulted were in agreement on a number of issues:

⇒ If a university wants to use the 'hacking' label, we should question who they are targeting and what they are actually teaching?

⇒ Any reference to hacker(ing) gives the wrong impression in business – just because it is a media friendly term doesn't mean that we should allow a slang term to become the de facto words for something which ought to be professional – we need to remain concerned about lax terminology.

⇒ There is a need to move away from the "Hollywood" term and provide something with a more legal representation.

4.2 Experts who are contracted to test the security of systems are not hackers (in the media sense) because their access is authorised. Therefore 'ethical' hacking becomes a discussion of whether it is ever ethical to gain 'unauthorised' access to a system. It is accepted that some would claim that demonstrating weaknesses in a system can be for the greater public good (systems that hold medical records for example), or for exposing cover-ups of facts that are in the public interest (e.g. chaos computer club exposing details of chernobyl). However, neither stand up against the major two ethical theories used in undergraduate teaching - *Kant* (absolutist, it would be wrong no matter what reason) and *Consequentialism* (normally supporting wider public interest matters; fails because it depends on outcomes, which are unknown and unpredictable).

4.3 It is accepted that there is a need to teach penetration testing in an appropriate manner in order to combat hacking in all forms – i.e. it is acceptable that in order to ensure that a system is safe from attack, the techniques used by the attacker (the unethical hacker) should be understood and, where safe to do so, applied as a test that the system can withstand them. Where students are concerned, these two interpretations of the word must be explained and made very clear.

4.4 On balance, the professional's who were consulted agreed that ethical hacking is an oxymoron." Apart from the discussions surrounding intent, no one felt hacking was ethical or that a university should *use* the term or *teach* "ethical hacking".

4.5 In conclusion, **ethical hacking** should **not** be considered to be an accepted professional industry term. If Penetration Testing is what is being taught, then that is how it should be labeled – rather than seeking to use marketing spin to gain traction and credibility within an industry that is seeking to improve its professional image. A teaching unit with the title "ethical hacking", whilst headline grabbing and engaging students, would not be a responsible way forward. Any course run within this field should contain a mandatory component covering the ethical implications.

Andrea Simmons, MBCS CITP, CISSP, CISM, IISP, BA
Consultant Security Forum Manager
For and on behalf of
BCS Security Forum Strategic Panel, chaired by Louise Bennett
British Computer Society
Mobile: 07961 508775
Email: andrea.simmons@bcs.org.uk
Web: www.bcs.org/security

ANNEX A Available definitions

1 A trawl through Wikipedia and www.whatis.com etc. provide the following available definitions for a number of key terms which need to be borne in mind when providing a professional judgement on the acceptance of certain "vogue" terms. 2007.

2 This compilation of definitions should be read with sense and sanity in mind – i.e. it is quite possible to see the contradiction between those who seek to maintain a difference between things which are rendered virtually identical when put under a microscope such as this.

3 "**Hacker** is a term used by some to mean "a clever programmer" and by others, especially those in popular media, to mean "someone who tries to break into computer systems." The term hacker is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

4 "An **ethical hacker** is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as *penetration testing*, *intrusion testing*, and *red teaming*. An ethical hacker is sometimes called a white hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat.

5 "In a similar but distinct category, a hacktivist is more of a vigilante: detecting, sometimes reporting (and sometimes exploiting) security vulnerabilities as a form of social activism.

6 "A **white hat hacker**, also rendered as **ethical hacker**, is, in the realm of information technology, a person who is ethically opposed to the abuse of computer systems. Realisation that the Internet now represents human voices from around the world has made the defense of its integrity an important pastime for many. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them.

> "A hacker who is legally authorized to use otherwise illegal means to achieve objectives critical to the security of computer systems"[1]

7 "The term *white hat hacker* is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity for monetary gain or charity. Many such people are employed by computer security companies; these professionals are sometimes called **sneakers**. Groups of these people are often called tiger teams.

8 "In wargaming, the opposing force in a simulated military conflict is known as the **Red Team**, and is used to reveal weaknesses in current military readiness. More generally, Red Teaming can refer to an independent peer review of an existing practices, or future proposals. Normally this is accomplished internally amongst government agencies. However, some private investigation companies provide this service to corporations.

9 "The primary difference between white and black hat hackers is that a *white hat hacker* claims to observe ethical principles. Like black hats, white hats are often intimately familiar with the internal details of security systems, and can delve into obscure machine code when needed to find a solution to a tricky problem. Some use the term *grey hat* and fewer use *brown hat* to describe someone's activities that cross between black and white.

10 "In recent years the terms *white hat* and black hat have been applied to the Search Engine Optimization (SEO) industry. Black hat SEO tactics, also called spamdexing, attempt unfairly to redirect search results to particular target pages, whereas white hat methods are generally approved by the search engines.

11 "A **grey hat**, in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.

12 "One reason a *grey hat* might consider himself to be grey is to disambiguate from the other two extremes: black and white. It might be a little misleading to say that grey hat hackers do not hack for personal gain. While they do not necessarily hack for malicious purposes, grey hats do hack for a reason, a reason which more often than not remains undisclosed. A grey hat will not necessarily notify the system admin of a penetrated system of their penetration. Such a hacker will prefer anonymity at almost all cost, carrying out their penetration undetected and then exiting said system still undetected with minimal damages. Consequently, grey hat penetrations of systems tend to be for far more passive activities such as testing, monitoring, or less destructive forms of data transfer and retrieval.

13 "A **cracker** is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. The term "cracker" is not to be confused with "hacker". Hackers generally deplore cracking."

14 TigerScheme (http://www.tigerscheme.org/) adopted Security Tester for Penetration testing is fine, as is vulnerability testing and application testing.