2010

Penetration Testing and Vulnerability Assessments: A Professional Approach

Konstantinos Xynos
University of Glamorgan

Iain Sutherland
University of Glamorgan

Huw Read
University of Glamorgan

Emlyn Everitt
University of Glamorgan

Andrew J C Blyth
University of Glamorgan

PENETRATION TESTING AND VULNERABILITY ASSESSMENTS: A PROFESSIONAL APPROACH

Konstantinos Xynos, Iain Sutherland, Huw Read, Emlyn Everitt and Andrew J.C. Blyth
Faculty of Advanced Technology
University of Glamorgan
Pontypridd, CF37 1DL
United Kingdom
kxynos@glam.ac.uk, isutherl@glam.ac.uk, holread@glam.ac.uk,
eeveritt@glam.ac.uk, ajcblyth@glam.ac.uk

Abstract

Attacks against computer systems and the data contained within these systems are becoming increasingly frequent and evermore sophisticated. So-called "zero-day" exploits can be purchased on black markets and Advanced Persistent Threats (APTs) can lead to exfiltration of data over extended periods. Organisations wishing to ensure security of their systems may look towards adopting appropriate measures to protect themselves against potential security breaches. One such measure is to hire the services of penetration testers (or "pen-tester") to find vulnerabilities present in the organisation's network, and provide recommendations as to how best to mitigate such risks. This paper discusses the definition and role of the modern pen-tester and summarises current standards and professional qualifications in the UK. The paper further identifies issues arising from pen-testers, highlighting differences from what is generally expected of their role in industry to what is demanded by professional qualifications.

Keywords: Penetration testing, pen test, cyber security, vulnerability assessments

INTRODUCTION

Internet connectivity continues to increase as millions of new devices are attached to this global network (IDC, 2009). An example of the continuing demand for connectivity is the shortage of IPs that are based on IPv4 (Moses A, 2010). This increase in connectivity has not gone unnoticed by criminals and organised-crime as security analysts have noticed a rise in the volume of attacks targeted against those connected to the Internet (ACPO, 2009). Although crimes relating to financial gain reached £52 billion in 2007 (Cabinet Office, 2009), cyber-espionage attacks have targeted systems that provide nation states' network access to the rest of the world (Markkoff, J., 2008) and we are even beginning to see APTs being reported (Higgins, K. J., 2010)

Commonly deployed security measures include firewalls, intrusion detection systems and anti-virus software, but security-conscious organisations go one step further by trying to understand the possible weaknesses of their deployed network, rather than just a paper-based analysis of the documented system. This can be achieved by employing a highly skilled security specialist to attempt to "break-in" to the network and related systems to determine what vulnerabilities are present. This service would typically include recommendations for mitigating the vulnerabilities and/or re-configuration to block these potential holes in the network. These security specialists are referred to as penetration testers or pen-testers.

A penetration test can therefore be defined as the process of systematically and actively testing a deployed network to determine what vulnerabilities may be present and to create a report with recommendations to mitigate or resolve these vulnerabilities.

Penetration Testers: A changing role

The focus of a penetration tester is similar to that of a hacker in that they are seeking to breach a network system, but their motivation is to improve security. Initially the methods and patterns employed by the penetration tester would be similar to those utilised by hackers. However, penetration testers differ to hackers in that they only probe a network, instead of continuing to exploit and cause malicious damage.

Furthermore, a penetration tester is limited to a specific set of systems they can analyse due to contractual obligations. These limitations may take into consideration the amount of time allocated for the test, which specific systems they may probe and the extent to which they may perform the analysis.

Corporate organisations generally desire the minimum amount of disruption to the functioning of the organisation's main and back office operations. This means that the process of testing a network and its systems needs to be almost non-intrusive and that the services the organisation provides should continue to work as normal during and after a test; ensuring high availability and minimising the disruption to business processes. This means that the systems may not have been fully penetrated in order to determine the degree of risk these vulnerabilities may pose. Hackers on the contrary, do not care if availability of a system goes down and will attack it to achieve their set goals by any available means.

Usually, large corporations look at hiring a penetration tester to minimise any future damage or information leakage from a potential hacking incident. There is also increasing pressure for corporate organisations to comply to external standards (e.g., Sarbanes-Oxley, HIPAA, PCI DSS, ISO 27001) which usually require or recommend some form of security review (Bentley, L., 2006). This does mean that these can occasionally lead to a simple security exercise with a 'tick in the box' approach and therefore limiting the penetration tester to conducting a simple vulnerability assessment.

Penetration Testing vs Vulnerability Assessment

A vulnerability assessment usually includes a mapping of the network and systems connected to it, an identification of the services and versions of services running and the creation of a catalogue of the vulnerable systems.

A vulnerability assessment normally forms the first part of a penetration test. The additional step in a penetration test is the exploitation of any detected vulnerabilities, to confirm their existence, and to determine the damage that might result due to the vulnerability being exploited and the resulting impact on the organisation.

In comparison to a penetration test a vulnerability assessment is not so intrusive and does not always require the same technical capabilities. Unfortunately it may be impossible to conduct such a thorough assessment that would guarantee that the most damaging vulnerabilities (i.e., high risk) have been identified.

The difference between a penetration test and a vulnerability assessment is becoming a significant issue in the penetration testing profession. There are many penetration testers that are only capable of performing vulnerability assessments and yet present themselves as penetration testers. If a company is unfamiliar with the process they may think a networked system has been fully assessed, when this is not the case.

RELATED WORK

There has been considerable effort dedicated to the technical aspects of penetration testing. Arkin, Stender and McGraw (Arkin, B. *et al* 2005) investigate the importance of the subject from the software pen-testers perspective, concentrating on where the role of the tester lies when assessing flaws during software development. Within the software development life cycle, Arkin *et al.* suggest without proper and timely assessment, organisations "...often find that their software suffers from systemic faults both at the design level and in the implementation" (Arkin, B. *et al,* 2005). The same can be said for the network security of an organisation; without proper and rigorous assessment, the network design of an organisation will lead to unknown flaws inherent in the network implementation.

There has been limited work on the skills and abilities required of the pen-tester, and less so on the legal, social, ethical and professional issues arising from such sensitive work. A notable exception to this assertion is the work by Pierce, Jones and Warren (Pierce, J. *et al,* 2007). In their paper they provide a conceptual model and taxonomy for penetration testing and professional ethics. They describe how integrity of the professional pen-tester may be achieved by "...avoiding conflicts of interest, the provision of false positives and false negatives, and finally legally binding testers to their ethical obligations in [their] contract" (Pierce, J. *et al,* 2007). This is certainly noteworthy and should be expected of an individual working with potentially sensitive information, however this appears more of a personal "ethical code of conduct" rather than something which can be enforced and assessed.

Pierce *et al.* (Pierce, J. *et al,* 2007) also discuss the *then* provision by universities "...toward offering security testing courses". Additionally, in 2006, McRue (McRue, A., 2006) commented on the "...first U.K. university to offer a dedicated degree course in hacking". This has certainly shown an emerging trend in the education sector for penetration testing courses, however these tend to be degree classifications and not necessarily an industry-recognised certification standard.

PENETRATION TESTING REQUIREMENTS

There are a number of organisational issues that need to be addressed before a network penetration test or security review. These requirements can include legal and contractual issues specifying liability etc. This may also include the technical requirements involved in the penetration test: The range of IP addresses over which the test is to be conducted, time constraints, the source IP address and the systems that are to be targeted (and also those that are not to be targeted) as part of the test. There may also be a requirement to inform specific individuals that the test is taking place, for example in relation to health and safety issues where the target is a safety critical system. These requirements can vary across the globe, depending on legal structures in the host country and this may pose a challenge for organisations who span international boundaries.

Theoretically there are a number of ethical and competency issues that penetration testers face in conducting an assessment, from testing systems or protocols not explicitly included or excluded from a test, to significant omissions that could possibly be disastrous to an organisation. The penetration tester is contractually and ethically bound to abide by the customers requirements, but should ensure the penetration tests is conducted correctly and does not lead to a false or misleading sense of security.

Although Code of Conduct and Best Practice is laid out by numerous professional bodies, in actual practice the individual is often required to take an informed decision given a particular situation. Therefore the individual should possess the necessary procedural, ethical and technical training.

Professional Standards and Ethical Competency

There are a number of professional and certification bodies that have some form of Code of Conduct, Code of Practice or Ethical Code by which the members need to abide. These include a number of internationally known professional memberships such as the IEEE (The Institute of Electrical and Electronics Engineers) (IEEE, 2010) and the BCS (British Computer Society) (BCS, "BCS - The Chartered Institute for IT", 2010), which try to encourage professionalism and the raising of standards in the industry. These bodies have societies or groups in specialist areas like the IEEE Computer Society (IEEE CS) (IEEE, 2010) and BCS Information Security Specialist Group (BCS-ISSG) (BCS, 2010). Some organisations are security focused such as the Institute of Information Security Professionals (The Institute of Information Security Professionals (iisp), (2010). It is not unusual to have a membership revoked on the grounds of breaching the Code of Conduct or unethical practice by the member. Previous work by (Pierce, J. *et a,l* 2007) highlights the ethical issues relating to penetration testing.

Professional Standards and Technical Competency

In addition to ethical and professional codes, professional bodies should set and progress the standards in practice and competency. In an industry where anyone can possibly run a few tools and create a report, professional bodies help distinguish their members from non-members and a Code of Conduct is put in place to guide the penetration tester. Examples of the codes of conduct include that of the EC-Council (EC-Council, 2010) and the ISC2 Code of Ethics (The ISC2 Code of Ethics) both of which are available online.

Due to the nature of the entire computing field and especially with penetration testing, systems change and are updated at a frequent rate. The professional tester is forced to keep up to date and constantly develop their skill set in terms of knowledge and understanding of new systems that are rolled out rather than rely on the output of automated tools.
There are a number of resources a penetration tester can use to maintain technical competency including the Open Source Security Testing Methodology Manual (OSSTMM). To address the issue of more and more applications becoming Internet based, and the need to test the security aspects of Web applications, resources such as the open-source methodology Open Web Application Security Project (OWASP) can be used.

MAINTAINING COMPETENCY AND PENETRATION TESTING CERTIFICATION

One method of attaining the necessary training is via an academic or professional training course which addresses the basic concepts of information security and network technology through to the ethics and standards required for professional practice. At the undergraduate level ethics is very important and must be taught, or at least explained at the beginning of every module that provides an insight into penetration testing or some sort of hacking technique, (Logan P.Y. & Clarkson A., 2005) provides an excellent review of the requirements of course content for teaching penetration testing.

Although a university degree provides in depth training in the subject area, there is a need to demonstrate continuing competency in the subject area. One way of achieving this is via a certification scheme which requires a regular re-certification to demonstrate a continuing competency in the subject area.

In the UK, there are three recognised certifications; CHECK, CREST and TIGER Scheme. There are two main commercial certification bodies that can certify penetration testers in the UK. These are TIGER Scheme (TigerScheme, 2010) and CREST (CREST, 2010). These systems require a high quality of service maintained under the Terms & Conditions of CHECK (CESG, 2010).

IT Health CHECK Service

The IT Health CHECK Service (CHECK) (CESG, 2010) provides an assessment of Her Majesty's Government (HMG) or Critical National Infrastructure (CNI) systems and networks in the UK. Before an organisation performs a penetration test of such systems, they need to first become a CHECK Service Provider (CSP). It is assumed that anyone performing a CHECK service holds UK security clearances (CESG, 2010). This may cause problems for non-British nationals who wish to pursue a career in the UK as a penetration tester. The most senior designation for a penetration tester under this scheme is that of 'CHECK Team Leader'.

Council of Registered Ethical Security Testers (CREST)

One system operating in the UK is CREST (CREST, 2010). This not-for-profit organisation is governed by a memorandum of association, with about 19 member organisations at the time of writing (CREST, 2010). Its main purpose is to provide assurance of competency for organisations, and for the individuals within those organisations.

CREST was created to fill a niche in the UK security testing industry, by providing assurance for Non-Government Organisations (NGOs), i.e. the private sector. This is because the existing CHECK standard is only applicable for Government organisations. Members are provided with guidance on standards, methodologies, further recommendations and a code of practice. However it should be noted that this information is not publicly available from the CREST website (CREST, 2010) at the time of writing.

The scheme provides assurances of professionalism to organisations, but not to individuals. "Individuals not employed by CREST Companies can take the CREST Certification Examination to become CREST Associates, but cannot undertake CREST approved testing without working under the auspices of a CREST member company" (CREST, 2010).

TIGER Scheme

The TIGER Scheme (TigerScheme, 2010) is focused on providing an independent method of determining the skill and ability of a penetration tester. The scheme has a number of levels from the Associate Membership to the Senior Tester qualification. The structure of the scheme involves separate management committee, operating authority and examination body. These form the strength of the TIGER Scheme; with the technical and professional standards enforced by the Examination Body being derived from the advice of a technical panel composed of independent experts. The technical panel acts on behalf of the Management Committee, to ensure the examination are relevant to the penetration test community. The University of Glamorgan in the UK currently acts as the Examining Body for the TIGER Scheme.

The TIGER Scheme Senior Tester is equivalent to CHECK Team Leader. Since it is a multi-tiered system candidates without UK security clearance can still be awarded TIGER Scheme Senior Tester status but not CHECK Team Leader status, as this is confirmed through a separate process with CESG (CESG, 2010).

An Issue with Definitions

Feedback from TIGER Scheme candidates has provided a variety of opinion on the content and execution of a penetration test examination. Currently the examination for the TIGER Scheme Senior Tester is operated as a penetration test where systems have to be compromised and utilised as a stepping-stone to launch other attacks and tools in an information gathering exercises. This is similar behaviour to that of a hacker entering a system and exploring the rest of the network.

A common failing point that candidates face is the lack of recent experience and practice in this area of penetration testing. The majority of the candidates would have no problem in conducting a vulnerability assessment but have problems making use of complicated hacking techniques.

As described in the literature when looking at the differences between a penetration test and vulnerability assessment there is probably a good argument to be made to the penetration testing community and profession; this is that they should look at creating a vulnerability assessment certification that would ensure that the individual is capable of conducting a detailed vulnerability assessment without having the capabilities of conducting a detailed penetration test.

INTERNATIONAL PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

The introduction of the TIGER Scheme and CREST have shown how a governmental initiative has resulted in defining a requirement that industry can follow. When setting up a certification there must be trusted and experienced professionals that will propose and contribute to the certification standards and these in turn need to be assessed accordingly. Examination bodies have to be impartial and avoid any potential conflict of interest in the accreditation process and ensure a certain quality is maintained. This can only be achieved by having an independent examining body with staff that has the relevant expertise. The authors believe that Universities are ideal examining bodies. They are experienced in operating the quality control required for a rigorous examination process, independent and impartial from industry when assessing candidates against a defined standard.

CONCLUSIONS

Although penetration testing is an industry recognised term, there is still ambiguity as to what a penetration tester actually does and how they provide assurance that the work they carried out is fit for purpose. This is particularly true of the penetration test versus vulnerability assessment debate.

This paper discusses the key issues relating to penetration testing, introducing the main issues from both the pen-tester and the client organisation sides. How does a pen-tester demonstrate professionalism? How can an organisation be assured that the team they hire can be trusted to fully complete the assigned task? These are the current challenges to the industry that can only be addressed by relevant, professional qualifications.

Ensuring that current best practice is known, these questions can be addressed by those in the industry. There are many different certifications available, and knowing what is available and recognised to be of a high standard will help only raise the bar in an industry that can require service providers and their clients to exchange potentially sensitive information.

ACKNOWLEDGEMENTS

The authors would like to thank the support provided by the members of the Information Security Research Group (ISRG) at the University of Glamorgan.

REFERENCES

IDC, (2009), “Number of Mobile Devices Accessing the Internet Expected to Surpass One Billion by 2013”, Reported on 9 Dec 2009, Available at: http://www.idc.com/getdoc.jsp?containerId=prUS22110509 [Accessed 25 July 2010]

Moses A., (2010), “Internet addresses running out”, Sydney Morning Herald, Available at: http://www.stuff.co.nz/dominion-post/national/technology/3958727/Internet-addresses-running-out [Accessed 25 July 2010]

ACPO, (2009), “ACPO e-Crime Strategy 2009 Report: A Strategic Approach to National e-Crime”

Markkoff, J. (2008). Before the Gunfire, Cyberattacks. New York Times . Available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1. 2 [Accessed 25 July 2010]

Higgins, K. J. (2010). "Anatomy Of A Targeted, Persistent Attack", DarkReading, 27 Jan. 2010, Available at: http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222600139 [Accessed 25 July 2010]

Dekker, M. (1997). “Security of the Internet”, CERT Coordination Center Reports, Available at: http://www.cert.org/encyc_article/tocencyc.html [Accessed 25 July 2010]

Stoll, C. (1989), “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.”, Doubleday, NY, USA.

EC-Council, (2010). Certified Ethical Hacking Training Course. URL: http://www.eccouncil.org/certification/certified_ethical_hacker.aspx [Accessed 25 July 2010]

Bentley, L., (2006), “Penetration Testing Key to HIPAA Compliance for Care New England”, IT Business Edge, Available at: http://www.itbusinessedge.com/cm/community/features/interviews/blog/penetration-testing-key-to-hipaa-compliance-for-care-new-england/?cs=22127 [Accessed 25 July 2010]

Cabinet Office, (2009), “Cyber Security Strategy of the United Kingdom”, June 2009, Available at: www.cabinetoffice.gov.uk/media/216620/css0906.pdf [Accessed 4 August, 2010]

Arkin, B., Stender, S., McGraw, G. (2005). “Software Penetration Testing”, IEEE Security and Privacy, Volume 3, Issue 1.

Pierce, J., Jones, A., and Warren, M. (2007). “Penetration Testing Professional Ethics: a conceptual model and taxonomy”, Australasian Journal Of Information Systems, 13(2). Available at: http://dl.acs.org.au/index.php/ajis/article/view/52 [Accessed 25 July 2010]

McRue, A. (2006). “University opens school for hackers”. URL: http://news.cnet.com/University-opens-school-for-hackers/2100-7355_3-6085375.html [Accessed 8 August 2010]

IEEE, (2010), “The Institute of Electrical and Electronics Engineers”, Available at: http://www.ieee.org/ [Accessed 25 July 2010]

BCS, “BCS - The Chartered Institute for IT”, (2010), Available at: http://www.bcs.org/ [Accessed 25 July 2010]

IEEE, (2010), “IEEE Computer Society”, Available at: http://www.computer.org/ [Accessed 25 July 2010]

BCS, (2010), “BCS Information Security Specialist Group (BCS-ISSG)” Available at: http://www.bcs-issg.org.uk/ [Accessed 25 July 2010]

The Institute of Information Security Professionals (iisp), (2010). URL: https://www.instisp.org/SSLPage.aspx?pid=183 [Accessed 25 July 2010]

The ISC2 Code of Ethics, available at: https://www.isc2.org/ethics/default.aspx. [Accessed 25 July 2010]

Council of Registered Ethical Security Testers (CREST), (2010). URL: http://www.crest-approved.org/Pages/RequiredMembership.html [Accessed 4 August, 2010]

Insititute for Security and Open meththologies, OSSTMM - Open Source Security Testing Methodology Manual, Available at; http://www.isecom.org/osstmm/ [Accessed 25 July 2010]

Open Web Application Security Project (OWASP) Available at: http://www.owasp.org/index.php/Main_Page [Accessed 25 July 2010]

Logan P.Y. & Clarkson A. (2005) "Teaching students to hack: curriculum issues in information security", Technical Symposium on Computer Science Education, Proceedings of the 36th SIGCSE technical symposium on Computer science education, p157-161

TigerScheme, (2010), "TigerScheme" Available at: http://www.tigerscheme.org/ [Accessed 25 July 2010]

CREST, (2010), "Council of Registered Ethical Security Testers" Available at: http://www.crest-approved.org/ [Accessed 25 July 2010]

CESG, (2010), "CHECK – What is CHECK" [online], Available at: http://www.cesg.gov.uk/products_services/iacs/check/index.shtml [Accessed 25 July 2010]

Council of Registered Ethical Security Testers (CREST), (2010). URL: http://www.crest-approved.org/Pages/MembersList.html [Accessed 4 August, 2010]