1-1-2014

Why penetration testing is a limited use choice for sound cyber security practice

Craig Valli
Edith Cowan University, c.valli@ecu.edu.au

Andrew J. Woodward
Edith Cowan University, a.woodward@ecu.edu.au

Peter Hannay
Edith Cowan University, p.hannay@ecu.edu.au

Michael N. Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

WHY PENETRATION TESTING IS A LIMITED USE CHOICE FOR SOUND CYBER SECURITY PRACTICE

Craig Valli
c.valli@ecu.edu.au

Andrew Woodward
a.woodward@ecu.edu.au

Peter Hannay
p.hannay@ecu.edu.au

Mike Johnstone
m.johnstone@ecu.edu.au

Security Research Institute
Edith Cowan University

ABSTRACT

Penetration testing of networks is a process that is overused when demonstrating or evaluating the cyber security posture of an organisation. Most penetration testing is not aligned with the actual intent of the testing, but rather is driven by a management directive of wanting to be seen to be addressing the issue of cyber security. The use of penetration testing is commonly a reaction to an adverse audit outcome or as a result of being penetrated in the first place. Penetration testing used in this fashion delivers little or no value to the organisation being tested for a number of reasons. First, a test is only as good as the tools, the tester and the methodology being applied. Second, the results are largely temporal. That is, the test will likely only find known vulnerabilities that exist at one specific point in time and not larger longitudinal flaws with the cyber security of an organisation, one such flaw commonly being governance. Finally, in many cases, one has to question what the point is in breaking the already broken.

Penetration testing has its place when used judiciously and as part of an overall review and audit of cyber security. It can be an invaluable tool to assess the ability of a system to survive a sustained attack if properly scoped and deployed. However, it is our assessment and judgement that this rarely occurs.

Keywords: cyber security, penetration testing, vulnerability assessment

1. INTRODUCTION

It is important to define and delineate between two oft-confused terms: viz. penetration testing and vulnerability assessment because penetration testing is not vulnerability assessment, but vulnerability assessment may utilise penetration testing. Penetration testing is the act of probing a network to attempt to exploit vulnerabilities using a series of tools and techniques, to achieve penetration and compromise of the network asset. Vulnerability assessment is about the assessment of a network, assets, policies and procedures for vulnerability to attack or compromise through a variety of channels of which penetration testing is just one technique, and one which does not have to be exercised to achieve a vulnerability assessment.

This paper will explore issues around the overuse of penetration testing as a suitable paragon for assessing the cyber security posture of organisations. This paper is drawn from our collective

experiences within an Australian context over the past 5 years and is based on over 80 penetration and vulnerability assessment exercises of public (Valli, Woodward, & Hannay, 2011) and private organisations.

2. WHY THE LIMITED CHOICE USE?

The logic behind the use of penetration testing needs examination and exploration. We posit penetration testing with well-known tool sets such as NMAP, Nessus or OpenVAS is a relatively simple procedural task. This means that organisations that undertake IT security services with wide scope penetration testing solely via tool usage are arguably pursuing and receiving a low quality service. It should be noted that quality professional penetration testers rarely use this as an approach.

The commonly used penetration testing programs are typically verbose in their reporting of discovered issues. The tools by default will often report a false positive that requires further testing and verification by experienced IT security professionals. This use of false positives is in fact erring on the side of caution, i.e. test to be sure and it is a sound concept for the most part. But the amount of reports we have read when assessing jobs or as precursor to employing our services that list dangerous Linux or UNIX exploits on a Windows-only network for instance are an all too common occurrence.

These types of naïve penetration tests are often performed by relative novices in the IT security field, who are hired by large corporate firms as junior employees, who are simply trained to follow a procedure. While this may seem good business practice we would argue that there is little value-add to the client, and little long term value for the organisation conducting the test-in fact this type of naïve test methodology could be detrimental to the testing organisation. The reason for this being that the organisation has been made no more secure, and when this is discovered, there will be reputational damage to the organisation which conducted the sub-standard testing.

3. MYTHS TO MANAGEMENT

The following are what the authors call the seven myths to management justifying the need for penetration testing, and are based on observations and engagement.

3.1 The Penetration Testers Found All of Our Cyber Security Problems

This statement is about as optimistic as panning for gold in your morning shower. Most systems that have penetration tests done on them rarely fail to achieve entry or compromise, which points to a larger systemic problem in the security posture of the organisation. This behaviour represents a fairly typical immature stance which attempts to apply a systematic approach to a systemic problem, the result being a false sense of security. To paraphrase Dijkstra, "penetration testing can show the presence of vulnerabilities, but does not prove the absence of vulnerabilities", the latter being quite a different perspective.

Many of the tests have poor scoping and poor planning of the process in its entirety. In many cases when we asked for the business motivation for the testing we found that it was being used as some token to signal the management there was/or is an issue with cyber security. There is often little post-test follow-up or process around a penetration test as its seen as an atomic process or on time fix similar to a conventional inoculation.

3.2 Our Penetration Testers are Experienced

Experienced in what exactly? Just because you are competent computer administrator or computer scientist or network specialist it does not make you a capable penetration tester. The capable penetration tester is a person who tends to have an in-depth knowledge of networking, at least one operating system, and can understand how programs run and operate at a systems level. In addition to these highly advanced IT skills they also need investigative and analysis skills and most importantly a

full appreciation of the upstream and downstream consequences of their actions when attempting to attack systems.

Importantly there are currently no professional standards enforced at a national level in Australia to become a penetration tester. It is ironic that a system that may be responsible for the provision of electrical power to a whole city may also be at the mercy of a non-certified, non-registered penetration tester. And yet, the replacement of light bulb in the same room where that penetration tester has his/her laptop attached would require the attendance of a licensed and certified electrical contractor to replace it.

A stark example was that of a major Australia bank seeking new penetration testers to join their internal testing team. All applicants were subjected to practical standard assessment of their skill base; a prudent and necessary step. One of the contenders was already employed by another organisation as a security analyst and specifically listed their skills as a network penetration specialist and was paid in excess of $100,000 per annum for their services. The problem: the applicant scored 17% on the test, one of the lowest scores ever recorded. When further probed about his knowledge, the applicant was unable to articulate basic network protocol information, which would be assumed for the position.

3.3 They Tested All Our Systems

The team may well have done an excellent job of testing hardware and software, but did they test your wetware? People and processes are key points of failure in any system and we would postulate are normally the weakest link in any such system. It never ceases to amaze us how often people forget people in a system.

Some of the most effective systems penetration is achieved through social engineering techniques and not clamouring away at the keyboard for hours. This includes leaving USB sticks on the floor or in the car park that staff can subsequently pick up and put into their systems, sending e-mails with attachments that contain malicious code that staff subsequently open and again allow compromise of the systems.

It has been our observation that less than 2% of organisations we have tested actually have a cyber incident response policy. Furthermore, these actual policies rarely translate into plans and processes to respond, and when an incident occurs, the response ultimately fails if it starts at all.

3.4 You Do Not Understand My Industry

When negative audits do arise one of the key defences by managers or persons responsible is that "you do not understand my industry". Whilst that may be true, it is not defensible. A good penetration tester and vulnerability assessor typically does understand the TCP/IP protocol or how the IT systems in your industry work. If your systems are found to be vulnerable no amount of industry know-how is going to save you. A computer is binary: it either works or it does not. There is no middle ground.

3.5 No One Would Be Interested in Us-Why is Management Doing This?

Many organisations, and more importantly IT professionals, are still not aware of the major risk that insecure configuration and systems presents. In Australia and worldwide there are numerous press articles and reports that indicate that cyber espionage and cyber attack is an increasing problem (IBM, 2011; Symantec, 2013). These Australian press articles are typically derived from statements by major businesses and our lead security and intelligence agencies who work in this domain such as Australian Signals Directorate, Australian Security Intelligence Organisation and CERT Australia (Hilvert, 2012; Joye, 2013; Wiggins, 2013).

Cyber attack is also no longer a full-frontal contact event. That is, individuals or organisations who are seeking to attack a particular business will now no longer just attack the intended target in isolation.

These highly organised criminals are now attacking business associates and partners to glean valuable intelligence and information about their intended targets. In short, attackers are becoming more strategic. They do not directly attack executive management, but seek to gain intelligence from lower levels of management who would not normally consider themselves as being "on the radar" in terms of cyber warfare. So while you may not be a primary target you may be a secondary or tertiary target or collateral damage in the overall campaign against another party.

3.6 This Tool Knows it All

Why the tool may actually "know" something about security it as only good as the person using the console to operate it. All too often we see reviews conducted by individuals or companies that have limited value and demonstrate a lack of understanding of the key cyber security issues identified by tool.

In some standout cases we have seen simple, unedited and uncommented outputs from cyber security software that any individual with a simple procedure sheet and a basic understanding of computing could accomplish. What is even more galling is that some organisations charge premium rates for this level of ineptitude. One example was one in excess of $70,000 for running open source Nessus over a client's network, with nothing more than a covering letter from a senior partner attached. The cover letter had no significant analysis, it simply summarised vulnerabilities found as High, Medium and Low and an offer to extend further services to resolve them. Further, however, it is observed that this paucity of reporting coupled with large cost is often confused for quality by requesting management.

3.7 We Get Pen. Tested Once a Year. We are Fine!

Sound cyber security practices which include penetration testing, vulnerability assessment and auditing should be a process that is embedded within any IT system as an ongoing process. The threat against cyber enabled systems is advanced and persistent. Cyber attacks and incursions are a 24 hours 365 days a year reality for all entities connected to the Internet. So one has to wonder why the annual deployment of a pen testing team is going to increase your cyber resilience. See Myth 1.

Execution of an ongoing cyber security strategy through good policy backed up with sound processes evinced as result of bringing in the "testers" to demonstrate the management the risk that cyber security presents is never evident.

4. DISCUSSION AND CONCLUSION

Our position is that we unequivocally support the prudent and judicious use of penetration testing as part of the execution of an overall cyber security strategy. Testing and assessment with advanced methods and techniques can reveal vulnerabilities in systems on a number of levels and when remediated produce a more secure outcome for an enterprise. However, as we have outlined in presenting the seven myths, there is much effort needed to redress current issues around the fallacious use of penetration testing in organisations.

We also see an increasing need for more rigorous accreditation and certification of competence in cyber security and its sub-discipline, penetration testing. The answering of a 300 multi-choice question test hardly demonstrates advanced skills or competence with relevant tools and techniques. The use of practical tests as part of an interview process for penetration testers should be an automatic default for final shortlisted candidates. These tests do not have to be long and arduous but should enable an organisation to assess an individual's core competencies in penetration testing.

The skill sets needed of a professional penetration tester are highly advanced and are not just about having strong IT capabilities. There is a need to understand a variety of factors and possess skills including but not limited to identifying risks, and in the process demonstrating an understanding of second and third order consequences of actions undertaken in the execution of penetration tests.

Human management skills and of course effective communication are also key skill sets that are required of a professional penetration tester.

Organisations, and more importantly persons responsible for the management of the IT and cyber security function, such as Chief Information Officers and Chief Information Security Officers must seriously consider what purpose random or symbolic penetration testing of the organisational systems actually achieves. The penetration tests in of themselves must not be seen as an end, but often the first step on a journey of re-engineering an organisations cyber security posture through application of good practice.

Company directors in the case of large organisations need to have a better understanding of the risks that poor cyber security will present to the organisation. In addition, they should understand the often substantial further risks the inappropriate use of penetration testing can present to the organisation. These risks include but are not limited to reputational loss as a result catastrophic failure, possible partial loss of data or system integrity, all of which when realised have potentially catastrophic financial and organisational outcomes. This increased understanding will require ongoing education of company directors, and persons responsible for the management of the IT functions to effectively understand and address these risks.

Cyber security service providers have an obligation also to ensure that the business practices they employ allow their staff to generate quality outcomes for their customers. The delivery of a quality outcome for the customer is largely still the exception rather than the rule currently when it comes to penetration testing service provision. Service providers, however, are not the root cause of all malfeasant outcomes relating to penetration testing.

In conclusion, there is currently, and has been for a long time, a shortage of suitably trained and capable cyber security professionals (including penetration testers). But, this circumstance can only change when the market has attained a certain level of understanding and demands maturity in service delivery. The levels of professionalism and the expectation of competence in the whole cyber security supply chain must lift well above current levels. This needed elevation can only start to occur when the community of praxis expose and dispel, the myths that have bred to support unbridled exploitative opportunism that is all too often current penetration testing practise.

REFERENCES

Hilvert, Brian. (2012). More cyber attacks on Australian Government. Retrieved on 13th March, 2014 from http://www.itnews.com.au/News/320439,more-cyber-attacks-on-australian-government.aspx

IBM. (2011). X-Force 2011 Mid-Year Trend and Risk Report: IBM.

Joye, Christopher. (2013). Spy agency reveals big increase in cyber attacks, *Financial Review*, (25 Sep 2013).

Symantec. (2013). Internet Security Threat Report 2013, *18*, Symantec Corporation.

Valli, C., Woodward, A., & Hannay, P. (2011). Backtrack in the Outback-A preliminary report on cyber security evaluation of organisations in Western Australia. Paper presented at the Conference on Digital Forensics, Security, and Law, Richmond, Virginia, USA.

Wiggins, Jenny. (2013). CEOs step up cyber offensive. *Financial Review*, (5th Jan 2013).