Virtual Penetration Testing: a Joint Education Exercise across Geographic Borders

Helen Armstrong[a], Matt Bishop[b], Colin Armstrong[c]

[a,c]Information Systems, Curtin University, Australia
[b]Computer Science, University California, Davis

Abstract:
This paper describes an exercise that combines the business case for penetration testing with the application of the testing and subsequent management reporting. The exercise was designed for students enrolled in information systems and computer science courses to present a more holistic understanding of network and system security within an organization. This paper explains the objectives and structure of the exercise and its planned execution by two groups of students, the first group being information systems students in Australia and the second group comprising students enrolled in a computer security course in the United States.

Keywords: Penetration testing, vulnerability testing, security education

1 Introduction

Today's organization typically relies on a multitude of new and aging information technology and heterogeneous systems all stuck together with ethereal adhesive. Integration complexity rises as new systems and applications are added, together with the risks. A secure technology environment is an unspoken requirement for decision makers in today's globally competitive marketplace, and ensuring these systems are secure is an ongoing battle for an IT Department. Conducting assessable assignments in a simulated realistic business environment facilitates achieving better learning outcomes, and past research has shown that practical application of knowledge cements understanding, and builds skill levels, of the learner. Learning through experience and hands-on techniques are well tested and produce superior skills-based learning outcomes in IT security (Kercher & Rowe 2012, Papanikolaou et al. 2011).

Skill and knowledge in securing networks and systems are essential foundations for security practitioners. Most security curricula discuss these at length. Skills in network attack and defense come from this foundation. Those two particular skills enable the practitioner to test the security of an organization's networks and systems through the use of penetration testing, giving feedback to an organization on the security of its enterprise information technology as seen by attackers. However, security skills and knowledge are limited to the discipline within which the education is delivered. Security studies in computer science and computer engineering commonly in-

clude areas and a focus on the equipment, technology, infrastructure, protocols, cryptography and systems applications whilst those in information systems and information technology have a more business focus including security policy, disaster recovery, network security management and information security (ACM 2008, 2010). In many cases there is a chasm between security management and the technical gurus: computer scientists have a deep understanding of the inner workings of the network and operating system but little or no skill in presenting a business case to management. On the other hand the information systems people focus on solving business problems and creating opportunities using technology and thus understand the effect of risks and security breaches on the organization's ability to achieve its goals and bottom line. However courses in information systems are seldom designed to understand the capabilities or limitations of the inner workings of the technology.

This paper describes a joint exercise between two groups of students that traverses the chasm described above. A group of information systems students in a business school in Australia interact with a group of students in a computer science program in the US to build a business case for, and design and execute, penetration testing of an organization's network security. The paper presents a discussion of related work, the framework used and a description of the project which is still a work in progress.

2 Related Work

Over the past decade much has been written on practical exercises in educational environments involving hacking and penetration testing. These publications fall into several main groups. Cyber defense forms a distinct group presenting red and blue team exercises (for example see Conklin 2006, Kercher & Rowe 2012, Lathrop Conti and Ragsdale 2003, Mattson 2007), a second group discusses designing network security exercises and experiments (examples: Logan and Clarkson 2005, Papanikolaous et al. 2011, Peisert & Bishop 2007, Tjaden & Tjaden 2006, Vigna 2003), and a third group focuses on network security laboratory design (examples: Aboutabl 2006, Anantapadmanabhan et al. 2003). By now we should have the design and delivery of practical network protection education under control! However, the need for cross disciplinary knowledge and experience is finding its way into a list of needed skills for security professionals, and potential employers are increasingly seeking employees with broader skills than technical skills, such as problem solving, team facilitation, and good spoken and written communications. To the authors' knowledge, no prior publication covers an exercise similar to that described in this paper – one that links business and computer science students in the same exercise across international boundaries with significant time differences. This exercise reflects situations that are increasingly more common for IT professionals who work in teams from distributed locations, often experienced in large global organizations.

The need for penetration testing is well published, but the question is whether we are preaching to the choir. Swanson (2000) explains such testing not only ensures an organization has adequate protection in place, but confirms also that they are working as designed and that the employees are using them effectively. Chickowski (2013)

reports that one of the challenges faced by security professionals is performing vulnerability testing on the applications that businesses can least afford to have compromised. Organizations can't defend against vulnerabilities of which they are not aware. Outsiders continually seek vulnerabilities by scanning and mapping organizational assets, and organizations should know where their vulnerabilities lie to defend those assets. Kennedy et al. (2011) posit that penetration testing is one of the most effective ways to identify systemic weaknesses and deficiencies in systems. The penetration tester can identify ways an attacker can compromise a system by attempting to circumvent security measures. However, penetration testing is not the only answer – managers must realise that it does not try to identify all vulnerabilities. It simply illustrates how a system can be compromised. Penetration testing and vulnerability analyses can be excellent means to highlight the need for security, particularly where managers see sensitive data compromised and security policies not being adhered to.

3 The Penetration Testing Framework

The exercise uses the Penetration Testing Execution Standard as the foundation for the approach and the activities carried out (PTES, 2012). The PTES provides a standardized approach, a baseline to assist in client expectation management as well as risk management. This standard is currently in the beta stage of development and is being used widely across the globe. It is supported by a set of technical guidelines to provide direction when undertaking a penetration test. The PTES development team encourages its users to "think outside of the box" when following the guidelines, as all situations do not fit a common mold.

The main phases of the PTES are as follows:

1. Pre-engagement Interactions: This first phase encompasses agreement with the client on the objectives of the exercise, the scope of the penetration test, and an agreement on the terms of engagement. Clients must understand what is involved in a penetration test, and they have to specify the limits of penetration and exploitation activities, particularly where systems are operating live during the testing. Requirements for lines of communication and reporting must make clear who is to receive and act upon the information in the final report.

2. Intelligence Gathering: This phase involves gathering information about the organization from public sources such as databases, social media, web sources, media coverage, public company reports, and other external and internal footprinting activities. Some common activities in this phase are gathering information on what applications are running, which ports are open/blocked, what devices are connected, patch levels on system applications, storage infrastructure, VMs and any known vulnerabilities of web applications. This information identifies the list of potential targets. Some information regarding the security measures in place within the organization may be gleaned from these sources by identifying network and host-based protection mechanisms and security measures applied applications, VMs and storage. The 'attacker' needs to learn about a target, including how it behaves, how it operates, and from that determine how it can be attacked (Kennedy et al. 2011).

3. Threat Modeling: This phase is sometimes termed ‘enumeration’ and entails a more detailed investigation of threats by gathering more information about users, network connections and available services and then modeling the most effective approach to attacking through the vulnerabilities identified in the intelligence gathering phase. This phase analyses business assets (such as intellectual property, trade secrets, etc.) and business processes as well as identifying threat agents and their capabilities. Using this information the tester will identify those potential vulnerabilities that pose the greatest threat in the client’s environment as well as opportunities to maximize the success of the attack. By thinking like the attacker, the tester models an attack by analyzing the weaknesses discovered.

4. Vulnerability Analysis: This phase involves mapping the target environment, scanning ports, and running vulnerability scans on the target organization’s system to confirm the existence of the vulnerabilities to be used in the exploitation phase. The analyst may use both active and passive means to identify vulnerabilities. Existing tools such as nmap (Lyon 2008) and metasploit (Kennedy et al. 2011) will confirm some vulnerabilities; others may require developing special tests solely for this environment or organization. This phase may not necessarily identify a single vulnerability as the avenue for attack, as a combination of several vulnerabilities often gives the tester much greater success.

5. Exploitation: This phase commences once the vulnerabilities have been mapped in detail. The tester will seek to gain privileged access to the target system by exploiting the vulnerabilities discovered in the previous phase. Methods to bypass countermeasures using both manual and automated methods are employed and detection mechanisms circumvented. When the tester is sure that an exploit will result in success as defined by the ground rules of the test, the tester may execute an exploit. Note that in many cases, stealth and speed are important to a successful attack remaining undetected; this must be considered in light of the goals of the test.

6. Post Exploitation: Once the organization’s system has been successfully compromised the tester then moves into detailed exploitation of the target’s infrastructure, pillaging and capturing valuable information and resources such as source code, intellectual property, and funds from high profile systems. This phase focuses on attacks that have the greatest business impact and uses whatever sources it can access—including the often-overlooked backups. Commonly the tester inserts backdoors for future entry, and other Trojan horses as permitted by the terms of reference for the testing. After documenting and gathering evidence of all exploitations and their results, the tester cleans up, removing test data, activity logs, malware and rootkits, and returns the system to a clean environment. Hackers spend a significant amount of time in this phase to conceal the fact of compromise and the tester must do likewise in order to identify weaknesses in reporting and attention across the enterprise.

7. Reporting: This final phase reports the testing activities carried out, the results and the means for remediation. This report forms the foundation for decisions on allocating resources to security to protect the organization’s systems against future attacks. The report should include executive level content explaining the risks, including business impacts and the bottom line, quantifying the risks. As executive staff or board members with little IT knowledge will call for different language and detail

than the CIO and IT professionals so the technical details are not included in the executive-level sections. Technical content will then follow, detailing the penetration metrics and technical findings, together with the test cases and examples used. Details of the vulnerability analysis, exploitation and post-exploitation should be included. The contents of the report should be discussed with the client before issuing the report as a deliverable, so that potential protective measures can be discussed and investigated with the aim to fill the gaps. Recommendations and an action plan, also previously discussed with the client, are included before the written report is presented. An executive summary is useful to highlight not only the most important areas for attention, but also confirm the value of the penetration testing.

4 Overview of the Joint Exercise

The education exercise comprises a group of students enrolled in an information security management undergraduate course within the School of Information Systems in Western Australia (InfoSys group) and a group of students enrolled in a computer science course in University of California, Davis (ComSci group). The two groups of students will work together to design and complete a penetration test on a client's information technology, each group completing activities within their discipline area and contributing to the learning outcomes of their degrees as well as interacting across discipline boundaries.

The objectives of the exercise are to:

- Develop skills in presenting a business case for penetration testing to management,
- Develop skills in designing and executing penetration testing in a safe and ethical environment, and
- Develop skills in presenting penetration testing results to management.

The physical deliverables for the education exercise include:

- Business Case Report to the Organization's Executive Management detailing the need for and objectives of a penetration test, cost/benefit analysis and an overall project plan for the penetration test activity, including the methodology to be followed, the objectives of each phase, activities included in each phase, resources, time frame and constraints (InfoSys group). The scope and boundaries must also be detailed including the rules of engagement.
- Detailed Penetration Testing design, specifying the tasks to be undertaken and the tools to be used in each activity (ComSci group).
- Penetration Test results, including activities carried out, results including vulnerabilities detected, and strengths and weaknesses of the system tested (ComSci group).
- Final report to management detailing the activities carried out, strengths and weaknesses, impacts associated with weaknesses and vulnerabilities detected, and recommended security measures to minimize the organization's exposure and losses (InfoSys group).

5 Business Case Scenario

Both sets of students are advised that they will work together to plan, carry out and report on a penetration test for the organization General Airline and Grading Assignments, LLC (GAGA). This company is based in the Remote Access Virtual Environment (RAVE), and consists of several client workstations running different flavors of Windows and Linux. A central server provides the support for the company's sales, services, and records. The recent attacks on Spamhaus, and on the New York Times, have made GAGA aware that connecting to the Internet for their business may pose some risk. This risk might be amplified; they feel, by having their web server and assignment grading service accessible to the world. So they have asked whether a penetration test can help them be sure their systems are secure, and if so what is the business case for such a test. Both groups of students (located in Australia and California) are employed by Penetration Testing and Assessments (PTA) with the information systems students providing the business related expertise and the computer science students providing the technical expertise. The information systems students will produce the business case report at the beginning of the project and the final report to management at the end of the exercise (deliverables 1 and 4). The computer science students will carry out the testing, logging all activities and report their results to the information systems students (deliverables 2 and 3).

Table 1: Division of Project Duties

Deliverable	Task	InfoSys	ComSci
Business case	Objectives, cost/benefit analysis, methodology, overall project plan	✓	×
Terms of engagement	Scope and boundaries, terms of engagement	✓	×
Penetration testing design	Document high level testing requirements	✓	×
Penetration testing design	Detailed design of testing process and tools	×	✓
Penetration testing	Conduct testing process	×	✓
Penetration testing	Maintain testing records	×	✓
Penetration test results	Prepare technical test report	×	✓
Final report	Prepare final management test report	✓	×

The exercise will follow activity stages related to the deliverables as illustrated in Table 1. The InfoSys students will raise the business case for penetration testing and provide the scope and terms of agreement for the exercise. These students will write a document explaining to management the objectives of the activity, the associated benefits and costs, the testing process to be carried out based upon the PTES methodology and an overall project plan detailing timelines and resource allocation. Agreement must also be reached with the client regarding the rules of engagement once

penetration has been achieved, including boundaries for the exploitation activities, and this will depend upon the objectives of the test and whether the system is live at the time of penetration and exploitation.

The ComSci group will carry out activities relating to the identification and exploitation of vulnerabilities. Their first task will be to gather information about the target, using tools like nmap to determine which ports are open, and look at network traffic to see what systems it talks to. This information will enable the students to hypothesize flaws which will need to be documented for use in developing the detailed testing plan. Testing the hypotheses comes after the ComSci group has discussed these with the InfoSys group to identify which ones pose the greatest threat to the client's environment and which have the most likelihood of success. Once priorities related to the objectives and an ordered list are established, the detailed testing stage can begin. The ComSci group will then carry out the Vulnerability Analysis and Exploitation phases. They will try to confirm whether the vulnerability is present without exploiting it; which is a challenging task, because they have to think of a way to demonstrate its existence. They also must develop exploits for the vulnerabilities they find. The ComSci group will record all activities and their results. Descriptions need to be sufficiently detailed to reproduce the results and will include: date and time, event name, event synopsis (*very* brief) e.g. Brute Force, etc., event description, intended result, actual result (vulnerability identified or no vulnerability), tools and scripts used, and attachments or associated documentation.

In the post exploitation stage the ComSci group must interact closely with the InfoSys group to ensure they adhere to the rules of engagement and achievement of the objectives. This stage would commonly involve copying files, inserting new files, deleting existing ones, or inserting Trojan horses (usually back doors) to allow an attacker to enter the system with minimal fuss. When carrying this out the goal is avoid detection. Cleaning up before they exit is a crucial stage for post exploitation. The students will not know whether, or how, the teaching staff will be monitoring the systems and the students' activities. Again the students must record all their activities and results. This is also for their protection, because if GAGA claims they have damaged their systems in a way that is not allowed, the session recording will show them they did not.

The reporting phase involves developing a technical report describing the vulnerabilities the ComSci group found and assessing the security posture of the systems, evaluating the technical problems GAGA has, and providing technical recommendations to address the vulnerabilities you have discovered. This report needs to be supported by references to what they have found in their testing. This technical report forms part of the final report to be presented to GAGA management.

The InfoSys group develops the final report that not only includes the technical details of the testing provided by the ComSci group, but also suggests means of minimizing the risks arising from the vulnerabilities detected at both the technical and management levels. The information systems students will thus need knowledge of information security management, including considerations of standards, methodologies and frameworks for undertaking specialized information security operations, secondary considerations include physical security; control of access, both logical and

remote; security considerations in the design, testing, implementation of computer systems including the role of standards; administrative controls and their impact on reducing risk; controls in networks; recognition and measurement of potential loss; Information Systems audit concepts and techniques; and scenarios and case studies.

The students themselves will be required to manage the communications between the InfoSys and ComSci groups. The two sets of students will collect into small groups, forming internationally linked groups of 5-6 students. These students will need to communicate regularly over the course of the exercise to ensure effective information transfer and decision making. There is a 15 hour time zone difference between the two sets of participants. Perth in Western Australia is located slightly west of 120^0 East of Greenwich in Britain and therefore at plus eight hours Coordinated Universal Time (UTC). The UC Davis campus in California is approximately 120^0 West of Greenwich and therefore at minus seven hours Coordinated Universal Time. While students in both project groups may find the resulting time difference inconvenient, this additional dimension provides a real world working environment that they may commonly encountered during their careers. Effective communications between the project participants may therefore become a determinant of project success. As Table 1 illustrates, it is imperative that the InfoSys group effectively explain the business case and terms of engagement to the ComSci group. Both groups then need to negotiate the penetration testing design phase, and the ComSci group must communicate operational aspects of the penetration testing, agree on the level of exploitation as the testing progresses, and provide the test results to the InfoSys group. Finally the InfoSys group must ensure the final report accurately reflects all tasks undertaken before submitting it to the management of GAGA, LLC.

6 Work in Progress

This project is currently underway and thus a work in progress. Many aspects are proving challenging as the exercise progresses. Not only is the time difference posing a challenge, but the timing of semester classes and due dates for submission of assignments differs between the universities involved. Understanding of the tasks required appears to be clear and the students are experienced in working in teams to achieve specific goals. What is a learning experience is the cross discipline communication and building an understanding of the science versus business needs.

There are many advantages this type of exercise delivers. Not only do the students have the opportunity to work on an exercise involving highly industry relevant skills development, but also working as a team across global and specialty expertise domains. This exercise is anticipated to develop time management skills, project management skills, problem solving skills and social, technical, and communication skills. In addition it presents opportunities to extend personal networks in an industry specific set of security practitioner roles and an associated appreciation for different stakeholder perspectives.

7 References

1. Kercher K, Rowe D (2012) Risks, Rewards and Raising Awareness: Training a Cyber Workforce Using Student Red Teams. Proceedings of SIGITE'12 October 11–13 2012 Calgary Alberta Canada
2. Papanikolaous A, Karakoidas V, Vlachos V, Venieris A, Ilioudis C, Zouganelis G (2011) A hacker's perspective on educating future security experts. 2011 IEEE Panhellenic Conference on Informatics
3. ACM (2008) CS2008 Curriculum Update. http://www.acm.org/education/curricula-recommendations. Accessed 3 May 2013
4. ACM (2010) IS2010 Curriculum Update. http://www.acm.org/education/curricula-recommendations. Accessed 3 May 2013
5. Conklin A (2006) Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course. Proceedings of the 39th Hawaii International Conference on System Sciences, Hawaii
6. Lathrop S, Conti G, Ragsdale D (2003) Information warfare in the trenches. In: Irvine C & Armstrong H (eds) Security Education and Critical Infrastructures. Kluwer Academic Publishers
7. Mattson J (2007) Cyber Defense Exercise: A Service Provider Model. Futcher L, Dodge R (eds) Fifth World Conference on Information Security Education, Springer
8. Logan P, Clarkson A (2005) Teaching students to hack: curriculum issues in information security. ACM SIGCSE'05 February Louis Missouri
9. Peisert S, Bishop M (2007) How to Design Computer Security Experiments. Futcher L, Dodge R (eds) Fifth World Conference on Information Security Education, Springer
10. Tjaden B, Tjaden B (2006) Training Students to Administer and Defend Computer Networks and Systems. Proceedings of ITiCSE'06 June 26–28 2006 Bologna Italy
11. Vigna G (2003) Teaching network security through live exercises. In: Irvine C & Armstrong H (eds) Security Education and Critical Infrastructures. Kluwer Academic Publishers
12. Aboutabl M (2006) The *CyberDefense Laboratory*: A Framework for Information Security Education. IEEE IAW West Point Military Academy, New York
13. Anantapadmanabhan V, Frankl P, Memon N, Naumovich G (2003) Design of a laboratory for information security education. In: Irvine C & Armstrong H (eds) Security Education and Critical Infrastructures. Kluwer Academic Publishers
14. Swanson, Dan, 2000. Secure Strategies. October. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/october00/features3.shtml (Accessed 3 April 2013)
15. Chickowski E (2013) Too Scared To Scan. 27th March - 09:46 PM. Dark Reading, TechWeb, United Business Media (UBM), Manhasset, NY. http://www.darkreading.com/security/application-security/240151869/too-scared-to-scan.html. Accessed 3 April 2013
16. Kennedy D, O'Gorman J, Kearns D, Aharoni M (2011) Metasploit, The Penetration Tester's Guide. No Starch Press Inc CA USA
17. PTES (2012) Penetration Test Execution Standard. http://www.pentest-standard.org/. Accessed 30 March 2013
18. Lyon G (2008) Nmap Network Scanning. Insecure.Com LLC Sunnyvale CA,USA