

Book Review: Professional Penetration Testing

EH-Net Exclusive - Free Download of Chapter 4: Setting Up Your Lab

Review by Andrew Waite, EH-Net Member, InfoSanity.co.uk

When I first heard about Thomas Wilhelm's new book in my Twitter feed, the title immediately caught my attention, 'Professional Penetration Testing: Creating and Operating a Formal Hacking Lab.' As I'm currently trying to build up my own training and testing environment, this tome promised to provide answers to all my questions. A quick Google search to learn more and a useful discussion right here in the EH-Net Forums left me surprised that the release of the book had managed to slip underneath my radar. So when offered a chance to get my hands on the material and provide a review for those that had similarly managed to miss the release, I jumped at the chance.

The unique selling point of this resource over potential alternatives is best highlighted by the author's own foreword, “This book is a divergence from most books as it discusses professional penetration testing from conception to completion. Rather than focusing solely on information system vulnerability identification and exploitation, by the end of this book we will have examined all aspects of a professional penetration test, including project management, organizational structures, team building, career development, metrics, reporting, test-data archival methods, risk management, and training...in addition to... information gathering, vulnerability identification, vulnerability exploitation, privilege escalation, maintaining access, and covering our tracks.”

OK... now I'm totally hooked. Let's see if Mr. Wilhelm can reel me in.

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

EH-Net Exclusive - Free Download of Chapter 4: Setting Up Your Lab

The printed material is split into three sections, Setting Up, Running a PenTest & Wrapping Everything Up. Alongside the book, the DVD is well stocked with the building blocks of a basic lab setup. Unsurprisingly given the book's author, the live CDs created by Heorot.Net (De-Ice targets, pWnOS and Hackerdemia) are included. Backtrack is used as the attackers platform. I'm assuming for reasons of space, the ISOs (BT2 & BT4) aren't included on the DVD, but it is probably a safe bet that anyone interested in the material will already have a couple of Backtrack discs on hand.

Also included on the DVD are the videos from Heorot's Courses, Pentesting Fundamentals Course (HPTF) and Intermediate Penetration Testing Course (HIPT). As the full courses this material was developed for and taken from currently cost \$295 and \$445 respectively, this alone would allow the book to provide a good return on investment.

Setting Up

The book's first section covers aspects of penetration testing required to be taken into account before you find yourself in a client's environment for the first time. As the book covers a broad array of subjects I would recommend taking note of the information in the first chapter, as different ways of approaching the printed and digital content is suggested depending both on the reader's prior knowledge and experience, and the reader's role either technical or managerial.

Chapter 2 covers the almost obligatory discussion of ethical and legal issues within the field of information security. The discussion of ethical requirements goes beyond the usual canned definitions of black, white and grey hats pointing out that in the real world things are rarely black or white (or grey). If you're new to the field and want a better idea of where you fit, this is one of several sections contained within this book that could provide the answers you seek. The legal aspects covered in this chapter seem to be in-depth, but only cover US laws (other nations laws are listed but not discussed in detail). As I'm neither a lawyer or based in the US, I can't provide too much extra information in this area.

Chapter 3 attempts to provide the answer to one of the most frequently asked question by those new to or wanting to break into the field of information security, 'How to get a job in penetration testing?' Although the subject is often glossed over in other books, this one provides some good advice, starting with potential career paths towards information security and penetration testing and providing some extensive discussions of potential certifications to work towards. The career advice contained is good. If you are already in the industry or have researched this area to any degree, it is unlikely this chapter will provide any earth shattering information. On the other hand, if you're fresh, this provides a good single point of reference that could save time on research and trial and error. And trust me, with the wealth of knowledge needed to be in this field, your time could be put to better use.

Chapters 4 and 5 mark the start of the technical content. After following the information the reader should be able to have a fully functional lab environment with a good variety of target systems to hack. The focus of the material is a virtual environment with VMware Player on a Windows host system, but the information is provided in a clear enough manner that the environment required for the examples and labs can be created using any virtual system or dedicated physical hardware that the reader has available with little modification required.

Alongside the lab environment detailed and used for examples within the book, other potential ways to practice skills and techniques are discussed including online hacker-games, capture the flag events and a surprisingly frank discussions of targeting live, real-world servers. This is definitely highlighted as (likely, depending on location) illegal, unethical and is strongly discouraged. However I think the fact that this 'option' is discussed at all highlights the amount of real-world knowledge contained in the volume.

Additional functions for a virtual lab are also discussed, including using the environment as a safe way to harvest and analyse malware. This is part of the contents that initially drew my attention to the book; whilst the information provided is valuable this is not the primary focus of the material, meaning that the technical depth of this section was not as thorough as I was hoping for, it was useful nonetheless.

The final chapter of the first section defines the requirements for proper project management for a successful penetration testing engagement with a client. Several methodologies are detailed and discussed including the Project Management Body of Knowledge (PMBOK), Information System Security Assessment Framework (ISSAF) and Open Source Security Testing Methodology Manual (OSSTMM). Although this is (potentially) one of the least interesting chapters included in the book, the information provided will allow an information security professional to thrive in the wider business environment. This is one of the key factors that makes this book stand out from similar resources.

This chapter also provides a good example of the benefit of having the material available in multiple formats. On first read I found the methodology chapter a bit dry and lost motivation to continue reading, however I watched the accompanying course videos on project management methodology. I found the format much more digestible. Once the topic was better understood I was able to return to the printed information and successfully work my way through the content, gaining the benefit of the information provided.

Running a PenTest

The book's second section contains the 'meat' of the technical instruction. The activity flow and chapters should be familiar to anyone with a limited knowledge of penetration testing or having read (or skimmed) similar available books, each chapter details a different phase of a typical pentest engagement.

Starting with Information gathering, the initial chapter in this section details both passive and active tools and techniques whilst largely following the ISSAF methodology. The techniques described are fairly fundamental such as basic Google searches and more specialist search sites for passive processes to DNS, Whois and Traceroute for active scans. Keeping in line with focus of the book, the chapter finishes with a discussion of how the results could impact the initial

project plan and provides real-world advice for a project manager needing to handle any unexpected findings during an engagement.

Again the digital content provides a good accompaniment to the printed material. Whilst Ping and Traceroute are basic utilities, the video content details several different tools for creating packets to replicate the functionality of the common tools. This helps the reader understand the purpose and underlying technology behind even basic tools rather than just firing off tools without understanding what is going on in the background.

The focus of Chapter 10 is 'Vulnerability Identification.' The material covers the basics of OS and service enumeration. A manual process is shown first using Netcat to connect to open ports. This provides an understanding of the underlying processes beyond the more automated and intelligent tools that can grant pentest engineers the ability to manually confirm the findings of other tools. Nmap is covered extensively with a comparative discussion of Nmap's different scanning options for eliciting additional information from services and bypassing firewalls and IDSs rather than merely relying on default functionality. Again the examples used in the chapter and exercises contained at the end allow the reader to safely replicate the techniques within their own lab environment.

Following on from the previous material, Chapter 11 focuses on the activities necessary to prove the potential vulnerabilities discovered during previous work. Keeping with the same concept of starting with a manual process, there is an example walkthrough of exploiting a vulnerable Webmin installation running on pWnOS setup in previous chapters using a publicly available exploit found on Milw0rm. Creating custom exploits for potential vulnerabilities highlighted during an engagement are touched on, but are placed outside the scope of the book. Project management advice continues to be provided by pointing out that custom exploits are expensive in terms of required time and resources from a business and project management perspective.

Next up is a detailed installation and first use guide for Nessus. As Nessus doesn't actually exploit any vulnerabilities, I can't help thinking this material would have been better suited to the previous chapter. Regardless the information is clearly presented and should provide a good foundation for anyone wanting to get a handle on a very useful tool for a penetration tester. Core Impact also receives a detailed walkthrough of it's capabilities, again exploiting a vulnerability on one of the target systems built within the lab environment. The Nessus and Core Impact sections highlight a niggle I have from the layout of the book; images and screenshots are often not near to text that references them causing the reader to have to flick a few pages forward or back to find the referenced material. Not a show stopping problem, but enough for me to notice and break concentration when trying to take in the material.

Covering the increasing trend towards web application security, the material covers web app testing using WebGoat as a target platform. The information is well written, but as the subject isn't the core focus of the book the examples don't get much beyond the usual OR 1=1 sql injection example. Finishing up the exploitation material of the chapter is again some real-world advice for managing this phase in real-world projects and engagements.

Chapter 12 focuses on activities to be undertaken once a system is compromised from collecting sensitive and restricted information available from the level of access achieved, to using the access as a toe-hold for privilege escalation on the compromised device. It can also be used as a staging area for further forays into the network. After the technical material is presented the chapter again ends with some good advice to handling the closing stages of a penetration test engagement.

It is within this chapter that the book touches on additional vectors for information gathering and compromising security systems. Layer 2 man-in-the-middle attacks are given a brief but in-depth review including an example walkthrough using Ettercap to transparently gather username and passwords for a web application. Social engineering is highlighted but is only given cursory coverage with little more than a few bullet points providing a brief overview of the possible techniques employed by social engineers. In contrast the book's first discussion of wireless testing and weaknesses, the subject is surprisingly more detailed here with a description of attacks against both WEP and WPA protection mechanisms and an example walkthrough showing how to bypass these protections using the Airodump-ng suite. Whilst short this material will provide a good foundation for anyone wanting to get started within the realm of wireless security.

The final two chapters in this section cover both maintaining access to a compromised system and covering your tracks to avoid the attentions of the legitimate system administrator. The material for maintaining access largely comes down to introducing and discussing shells, reverse shells and encrypted tunnels. This surprised me as I would have expected the issue of shells to be covered earlier in the material, as the creation of shell connection of any variety is often the way a penetration tester compromises a server in the first place. Leaving this material in post compromise activities feels unusual. Regardless of the placement, the material is well written and aptly explains when and why the different types of connectivity are useful and/or required.

Chapter 14 contains the discussion of hiding your presence on a system including removing evidence from log files and hiding malicious files within the filesystem. From reading similar books I was initially surprised by the absence of rootkits from discussion at this point. Considering the book's focus is providing professional testing methodologies in real-world scenarios this may be understandable, especially as the one mention of rootkits in the book states that, "The changes made to the system by a rootkit are not easy to undo once the testing is complete and may introduce additional weaknesses to the systems security." So in retrospect, this is not something you want to be doing to a client's systems if you want a repeat contract.

Wrapping Everything Up

The final section of the book covers what to do once the dust has settled and the technical activities have been completed. This is not something I have seen covered in similar books beyond a bullet list of tasks. This book's scope being beyond just the technical aspects is one of its main strengths and this section highlights this well.

Chapter 15 provides requirements and advice for presenting the findings of the penetration test in a professional manner. The printed material on this subject is strongly supported by the DVD contents with some good, in-depth advice included in some of the course videos and a report template for guidance. In keeping with the professional focus of the book, and with a 'practice what you preach' attitude, this chapter includes some very detailed instructions for generating a digitally signed PDF version of the final report to securely provide the project findings to a client.

Although short, Chapter 16 provides a good comparison of the two competing schools of thought over whether to archive or destroy the information collected during the course of the penetration test. As the author describes there are advantages and disadvantages to each approach and the 'correct' process is left for the reader to determine as neither approach is best for all possible circumstances. From reading the material provided by the chapter, I'm inclined to offer a potentially safer third option: Do that which is required, signed off, and paid for by the client.

Chapter 17 is also relatively short, covering how to clean up a lab environment following testing to ensure a clean

baseline can be used for each test, and that no malware remains live in the environment following the completion of testing. The information provided is well written but shouldn't be ground breaking for anyone with even limited experience operating a test environment.

The books final chapter tidies up any loose ends and highlights several 'extra curricular' activities that can and should be undertaken by the team following a penetration test engagement. These include creating/updating a risk management register and a knowledge database to allow current and future members of a pentest team to build on the findings and experience gained during the engagement, as well as conducting after-action interviews with project members to assess performance and promote knowledge sharing within the team. These processes can also be used to highlight areas requiring additional training or resources to increase the effectiveness of future engagements.

Summary

The summary has been the most difficult part of this review to write. When I initially got my hands on the book I was disappointed. As I stated at the beginning from my research, the book promised to be my guide to fully utilising my existing lab to help further my career in information security. In this regard I don't feel that it lived up to billing. The material does a good job of covering setting up and initial usage of a lab, but if you've had any experience working within a lab environment you may not learn anything that you didn't already know.

However I want to quickly state that after reading the book and working through the DVD content and end of chapter exercises, I do think that this book is an excellent resource. If you are looking to make a break into the security industry and want a solid first step, this is the book for you. Alternatively if you already have some technical skill but want to know how to be more effective with the business aspect of your career, again this may be the resource for you.

The business and project management side of the books material is really well written and it's a topic not covered extensively in any depth in information security or computing resources in general. As the maturity and professionalism of the industry is often questioned, having this material and advice available to both practising professionals and those entering the market can only be a good thing for the industry as a whole.

The only reason I would suggest purchasing an alternative resource is if you are only looking to improve technical skills. Then again, if you only want to improve technical performance, are you sure that is all that needs improving? Next time someone asks how to get started in a career in information security, this is the book I'm going to be suggesting.

Andrew Waite, EH-Net Member, InfoSanity.co.uk - Andrew is currently a hosting engineer with the Onyx Group in the UK. Through this work he's had the opportunity to experience a wide variety of technologies and environments, before choosing to follow his passion and pursue a career in information security and incident response. Despite graduating university in 2007, he has been unable to quench his thirst for knowledge. Alongside building a personal testing and training environment to aid professional development, he's worked on several personal projects, ranging from wireless security and honeypot systems to malware analysis and physical security, the results of which are released via InfoSanity, his personal website and blog.