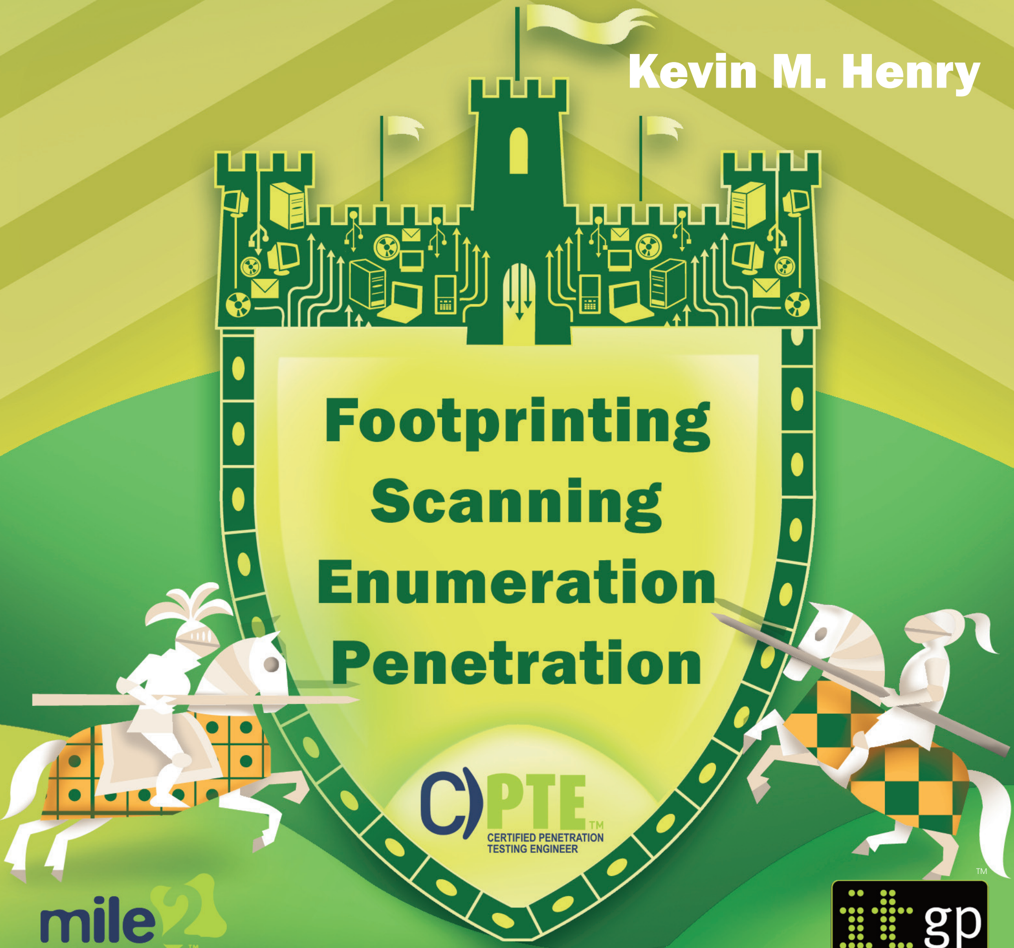
Penetration Testing

Protecting networks and systems

Kevin M. Henry



mile2™
IT Security Training

itgp™

Penetration Testing

Protecting networks and systems

Penetration Testing

Protecting networks and systems

KEVIN M. HENRY

IT Governance Publishing

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2012
by IT Governance Publishing.

ISBN 978-1-84928-372-4

PREFACE

This book is a combination of attacking and defending. It is an attempt to shed light on the thoughts, motivations and actions of an attacker against an organization or individual, so that each of us can better defend our systems, our intellectual property and our values. Part of a good defense is a strong offense – and knowing how to probe, test and strengthen our systems is also knowing how to test and evaluate the effectiveness of our security controls and the resilience of our systems.

To become a great penetration tester requires experience and skill. It involves creativity, persistence and patience. This book discusses the management and planning side of penetration testing. It is not focused on how to use the tools available – tools change and new ones come out continuously – but rather the timeless managerial and planning skills needed to plan, conduct and report on the security of a system, network, organization and its people. Mix this knowledge with hours learning the tools, and you will be well on your way to understanding how to make a difference to the security, reliability and resilience of your organization.

ABOUT THE AUTHOR

Kevin Henry has been working on computer systems for over 35 years. He began as an operator on the largest mini-computer installation in Canada in the mid 1970s and has since worked as a programmer, analyst, auditor and security expert. He currently provides security auditing, training and educational programs for major clients and governments around the world and is a frequent speaker at major security conferences.

Kevin lives with his wife and children in Blumenort, Manitoba, Canada, where winters are cold, and people are always friendly and helpful.

ACKNOWLEDGEMENTS

The author would like to thank Ray Friedman, Steve Mayes, Keyvan Ejtemai and Marc Thompson for their support and the opportunities they have provided over the years.

We would like to acknowledge the following reviewers of this book for their useful contributions: Jared Carstensen, Manager, Deloitte & Touche, Tiago Henriques and Antonio Velasco, CEO, Sinersys Technologies.

This book is dedicated to Rosalyn. I cannot thank her enough for her support and care – she is truly a Pearl beyond price.

CONTENTS

Introduction..10
Chapter 1: Introduction to Penetration Testing...........12
Case study..13
Security basics..16
Risk management...24
The threat environment...27
Overview of the steps to penetration testing..........................30
Penetration testing versus hacking..33
Benefits of penetration testing..34
Summary...35
Key learning points..35
Questions...36
Chapter 2: Preparing to Conduct a Penetration Test ..38
Approval and scope..38
Planning..42
Summary...47
Questions...48
Chapter 3: Reconnaissance...51
The start of the test..51
Physical information gathering...51
Other data sources...57
Avoiding footprinting...63
Key learning points..63
Questions...64
Chapter 4: Active Reconnaissance and Enumeration ..66
Port scanning..67
Countermeasures to active reconnaissance............................73
Key learning points..74

Questions..75
Chapter 5: Vulnerability Assessments...........................77
The attack vectors 78
References and sources of vulnerabilities........................81
Using vulnerability assessment tools 82
PCI DSS requirements 84
Malicious code 84
Reporting on the vulnerability assessment 91
Key learning points 91
Questions..91
Chapter 6: Hacking Windows® and UNIX.....................94
Having fun 94
Common hacking initiatives 95
Defeating data theft...98
Protecting against unauthorized access...........................99
Access controls 102
Actions of the attacker 103
Focus on UNIX/Linux 106
Advanced attacks 107
Source code review 117
Case study: Attack on a Chinese bank 121
Key learning points 123
Questions..124
Chapter 7: Launching the Attack.................................128
Steps to an exploit 128
Attacking wireless networks 129
Pen testing wireless...131
Network sniffing 133
Firewalls...138
Intrusion detection and prevention systems (IDS/IPS).142
Key learning points 142
Questions..143
Chapter 8: Attacking Web Applications......................145

The steps in attacking a web application 147
Questions...155
Chapter 9: Preparing the Report 158
Determining risk levels...162
Risk response 163
Report confidentiality 167
Delivering the report...168
Key learning points...168
Questions..169
Appendix 1: Linux 171
Appendix 2: Encryption 173
Concepts of cryptography 173
Appendix 3: Regulations and Legislation.....................188
Examples of regulations and legislation 189
Protection of intellectual property 194
Appendix 4: Incident Management...............................195
Concepts of incident management................................195
Additional Questions and Answers 199
Answers..217
References...218
ITG Resources..219

INTRODUCTION

Today's world runs on technology. Nearly every business benefits from – and relies on – technology in one form or another. The use of technology has brought tremendous advantages to society by making services, features and knowledge more readily available than ever before. We can communicate across the planet (and, in fact, across the universe) in seconds, and can effectively control millions of devices instantly – something we could never have done previously through simple human action.

The use of technology also, however, presents several risks to society. By using it, we develop a greater reliance on devices that lack the sense of judgment and discriminatory thought that a knowledgeable person would have. Such devices may provide us with erroneous data and cause us to make incorrect assumptions, errors in judgment or action, and possibly even seriously injure or harm society, finances and individuals.

To correctly deploy technology is a serious challenge – one that requires constant education, practice and testing. Moreover, the use of technology must always be seen in context. Technology is not an end in itself, it is not the magic answer to every problem, and it should never be implemented just for the sake of using a new tool or because it is available. Technology has one purpose, and that is to support the mission or objectives of the user/organization. As we will see through this book, the proper use of technology starts long before the technology itself is purchased. It starts with defining the business objectives and then designing the best solution for to meeting those objectives.

Despite the best intentions of designers, architects, developers and operations staff, technology is still subject to failure, breaches and compromise. Equipment, processes and people require careful monitoring and regular testing to ensure that the systems, networks, applications, security equipment and other technologies are working in a secure, reliable manner, and that they are not presenting new opportunities for attack against the organization.

Testing is the key to providing assurance of the correct implementation and operation of technology, and this book will examine the skills and techniques used by a professional penetration tester to provide the accurate, thorough and meaningful reports that their clients or management teams need on the secure operation of systems and equipment.

CHAPTER 1: INTRODUCTION TO PENETRATION TESTING

Penetration testing captures the imagination and sparks the interests of many people. It is part mystery, part challenge, part creativity and part risk. It has the glamour and mystique of doing something on the wild side of life by simulating a criminal act, but without the penalties. Therefore, it is no surprise that many people are drawn to penetration testing and want to know more about what it is, how to do it and, moreover, how they can use it to help protect their systems and defend their networks.

Protecting the systems and networks of today requires a broad understanding and in-depth knowledge of the tactics, tools and motivations of the adversary. The person given the responsibility to protect a system should know the nature and techniques of the enemy, and be able to prevent successful attacks by discovering and securing any vulnerabilities in their systems or networks before the adversary can find them.

Penetration testing is the simulation of an attack on a system, network, piece of equipment or other facility, with the objective of proving how vulnerable that system or "target" would be to a real attack.

Penetration testing is based on knowledge. The more knowledge the tester has, the more effective their attack will likely be. But what knowledge do they need? They need knowledge about the target, the operating environment, the users, the culture, the business itself, the physical security and, most of all, knowledge of how to use the tools (and their imagination) effectively.

Many people have a narrow and limited perception of penetration testing; they see it as an attack using a few common tools against a list of commonly known vulnerabilities. This type of testing provides some benefit to the organization, but is far too superficial and restrained to be really effective and meaningful. A pen test is innovative, probing, testing, evaluative, persistent and thorough.

In this booklet, we will examine various types of penetration tests, the tools commonly used, and the ways to leverage a pen test to provide the greatest possible benefit to the organization. The resulting penetration tests will deliver assurance and confidence to clients and business owners that their systems, networks and facilities are secure, that the level of risk to the organization of an attack is within acceptable levels, and that their information systems are being managed properly.

Case study

The General responsible for overseeing the security and operations of a military network requested a penetration test. The General was convinced that his network was secure, well-hidden and impenetrable. He had diligently instructed his staff to ensure that the network was well managed, unnecessary services were disabled, and that no extraneous information about the network was available anywhere outside of the network itself. He hired a top-quality pen testing team and challenged them to enter his network, but, at the same time, was convinced they would not even find it, let alone gain enough knowledge to launch a proper attack.

A couple of weeks into the test schedule, the pen testing team requested a meeting with the General. As he entered the meeting, the General asked if they had "given up already." The team then laid in front of the General the information they had managed to access, and stated that they were required to cease the test once they had obtained such information under the rules of the engagement. (Note: these rules must be set out at the beginning of the test, since there may be serious implications and potential damage to the organization once the testing team has gained access – especially when succeeding in penetrating a military network.)

Upon reviewing the documents obtained by the pen testing team, the General exploded in rage, demanding to know how they had managed to obtain so much sensitive, classified material. He threatened to demote his entire technical team and launch a legal investigation into his department. It was at this point that the pen testing team advised the General that the General's network was quite secure, and that the way they broke into the network was not through a sophisticated technical attack. They were able to access all of the information by simply sending a DVD that contained a Trojan horse to the General himself. When inserted into the General's machine, the Trojan promptly copied the entire contents of the hard drive on the General's machine to a secure server that the pen testing team had set up.

They delivered the DVD to the General using a journalist that had an interview with him to discuss a news article being written about technology in today's military. The DVD contained video clips and articles as a sample of the work that the journalist had already done to prepare the article.

Such an attack should not have been successful – no foreign media should have been installed onto a classified machine, and both policies and technical controls should have prevented this. But what happens in reality? Many people, including Generals, senior managers and even technical staff, could fall for such an easy trick.

As can be seen in this case, there are many challenges involved in carrying out a successful pen test. The first is to gain approval to conduct the test, the second is to determine the rules of engagement, the third is to know the reporting structure and who to deliver the results to, the fourth is to ensure the pen test is not limited to a strictly technical attack and, finally, the fifth is to ensure that the test provides meaningful results and recommendations for the organization.

We all know that most organizations would fall for such an attack. There is no technical control that is sufficient to totally prevent user mistakes! The 2011 attacks against RSA (the security division of the EMC) are an example of how easy it can be to penetrate even the most security-conscious organization. In the case of RSA, the exploit was enabled through a simple spear phishing e-mail sent to an employee. The employee opened the attachment that was linked to the e-mail (which promised them a list of open employment positions) and thereby launched the hacking tool that provided a backdoor into the company for the attacker to use[1].

[1] *http://www.f-secure.com/weblog/archives/00002226.html*.

The purpose of a pen test is to find any problems on the system and network, and in the user training, business procedures and operational controls related to the system being tested. A successful pen test is one that discovers the vulnerabilities and determines the level of risk they pose to the organization. An unsuccessful pen test is one where the team fails to find existing serious vulnerabilities and provides management with a false assurance of security, or one that provides the organization with a flood of meaningless data that is not sorted according to priorities or levels of risk.

The many breaches that Sony experienced in 2011 were mostly the result of simple attacks. The vulnerabilities that allowed the attacks to do the damage and compromise those systems affected should have been found by competent pen testers and thereby corrected. The Verizon-USSS data breach report of 2010 indicated that 96% of all data breaches were avoidable through simple or intermediate controls[2]. This is where many pen tests are failing. The pen tester bears the responsibility to perform their duties in a professional and competent manner, and thereby provide the information required by their clients to strengthen and secure their systems and networks.

Security basics

Penetration testing is a process of testing and validating the security posture and maturity of an organization. In order to test the security program, it is necessary for the pen tester to know what to look for and what the security priorities are.

[2] *http://securityblog.verizonbusiness.com*.

The first problem is that the term "security" is an abstract term and can mean many different things to different people.

Definition

One resource[3] defines security in the following ways:

1. Freedom from danger, risk, etc.; safety
2. Freedom from care, anxiety, or doubt; well-founded confidence
3. Something that secures or makes safe; protection; defense
4. Freedom from financial cares or from want
5. Precautions taken to guard against crime, attack, sabotage, espionage, etc.

We can see many positive aspects of security – freedom from worry and danger, for example – but we also see that security is very much an emotional term, conveying a sense of safety and protection. The last definition is most relevant for us: "precautions taken to guard."

A pen tester is not testing emotion or a feeling of safety; the tester is testing the precautions, the defenses and the levels of risk or danger.

The information security triad

For many years, the information security industry has defined the term "security" as comprising three core

[3] http://dictionary.reference.com.

elements: *confidentiality*, *integrity* and *availability*. There are good reasons for this. Using these three elements to define security gives a more complete picture, and provides a way to move the term away from an abstract, emotion-based meaning to one denoting something solid and measureable.

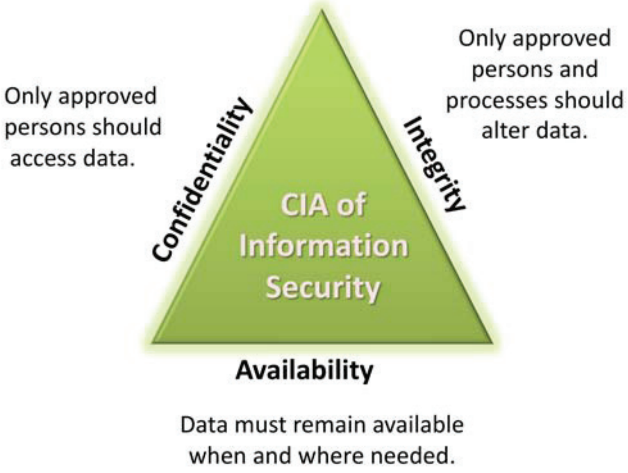

Only approved persons should access data.
Confidentiality
CIA of Information Security
Integrity
Only approved persons and processes should alter data.
Availability
Data must remain available when and where needed.

Figure 1: The CIA triad

Confidentiality

Confidentiality is based on confidence – trust and assurance that the organization is protecting sensitive information and systems from unauthorized access and disclosure. This requires the organization to *know* what information it has that requires protection. It starts with the classification of systems and data according to the level of damage that

]

would occur if the security of that system or data was compromised.

The objective of an attacker is not just to prove that they can get access. They want something. They want the organization's sensitive data, and they want continued access; they want to "own" the systems and networks of the organization for their own benefit. The pen tester must, therefore, see the objectives of the test as evaluating the ability of the organization to resist compromise, detecting an intrusion, and mitigating any damage that results from an intrusion.

The pen tester is testing the security of the system and ensuring that the core assets of the organization are protected from compromise.

Testing for confidentiality, therefore, is testing whether an unauthorized person can gain access to the organization's systems and data, and whether an authorized person may be able to commit unauthorized acts.

Integrity

"Integrity" refers to the accuracy and precision of data and systems processing. When an organization relies on the accuracy of data – or the reliability of a process – it must be confident of the integrity of that data and process and prevent improper modification or alteration of that data or process, whether through error, malicious activity or equipment malfunction.

A pen test is always a test conducted at a point in time, but the pen tester must still ensure that the data is not only accurate at the time of the test, but that the controls are adequate to protect it from improper modification in the future, as well. This would mean testing for the ability to make a change or alter a process in a way, or by a person, that should not have been permitted.

Availability

In today's world of rapid business operations, where decisions must be made both quickly and accurately, the availability of systems and data must also be assured. Where users and customers rely on systems providing data and service in a real-time mode, an outage may have catastrophic consequences. For many organizations, it is simply not good enough to tell customers that their systems are down or that the data they require is currently not available.

The main point is that not all systems and data have the same importance – some systems are critical, while others are simply "nice to have." Air traffic control systems are extremely critical (as long as the airport is operational), but an automated teller machine (ATM) or automated banking machine (ABM) is not nearly as important. The failure of an ATM is an inconvenience; the failure of air traffic control – for even a few moments – may result in extreme loss of life. Therefore, there is no security solution that is suitable for every need. Each business must tailor its security solution according to factors including the law, customer expectations, financial impact and reputation. When testing the security of an organization and its susceptibility to failure or compromise, the pen tester must relate the tests and the test results to the operational and security environment the organization works in.

The yardstick

By using confidentiality, integrity and availability as yardsticks, an organization can measure how well they are doing (their current level of security) against their desired position (where they need/want to be). Availability, for example, is an excellent yardstick. The organization will need to ask: what is the standard/level of availability the organization requires? How are they currently doing in comparison to that metric or standard? Are the systems and data of the organization meeting the required standard? Are they exceeding the desired standard? Or, are the current levels of availability substandard and inadequate? These questions are critically important, since they allow the organization to put a solid definition on what security means for them. A secure system is a system that provides the levels of confidentiality, availability and integrity required by the organization. Once the organization knows what those levels of security are, and whether or not it is meeting them, it can put in place the steps to address any security deficiencies and allocate the time, budget and resources required to implement its security program. This is why a pen test is so very important – it identifies the current security level of the organization, helps put together the plan to fix any vulnerabilities before an attacker finds those same vulnerabilities and makes the organization a victim of an attack.

The pen tester should not work strictly according to a template or checklist. A checklist is generic, and may be insensitive to the unique characteristics of the organization. Instead, the checklist should be used as a framework and then adjusted accordingly. The pen tester must understand the operational and security environment of the organization, and must measure the security against best practices, standards and the security position the organization is attempting to reach. Some organizations are more cautious than others; others have a larger risk appetite. The pen test must deliver an assessment that is sensitive to that operational environment.

Non-repudiation

Another area sometimes included in the CIA security triad is non-repudiation. Non-repudiation is a very important term in e-commerce and networked operations. Non-repudiation makes it possible to link an activity to its originator. It ensures that the person that initiated an activity would be unable to later deny that they were the person that committed that act. This would remove their option hide their identity and mask their activity. The pen tester will test the non-repudiation controls to determine whether an attacker would be able to erase log files, masquerade as another user, or set up false user accounts on the system to hide their activity.

Information classification

Not all information, and not all systems, require the same level of protection. Therefore, many organizations will set up a security classification scheme that will identify and label data according to the level of protection it needs. Information that requires higher levels of protection must be labeled and handled appropriately – according to how the data is stored, handled, transmitted, disposed of and displayed. The security controls must be adequate to protect sensitive information from unauthorized changes, disclosure and destruction, and the tests performed should ensure that the data protection controls are working correctly and cannot be easily circumvented by an attacker.

When is security enough?

The inevitable question is, “When is enough security enough?” There is no easy answer to this question. If an organization has had a breach, then there was not enough security – no matter how much they spent on it. If they have not had a breach, then there is always the suspicion that they are spending too much! Pen testers have a responsibility (and some may say a liability) to provide accurate and complete results to the client organization. They must ensure that they completed their work with due diligence and competence and have not provided false or misleading information to the client. There is no *one* answer to the “enough security” question, and all of the benchmarks and best practices represent only an attempt to define “adequate security.” The pen tester must be able to defend the testing program they have set up. This is why the pen tester may want to base their tests on standards, such as the Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27002 or COBIT,® or other such benchmarks.