

Penetration Testing: Not Just a Hack Job

By **Matthew J. Decker, CISSP, CISA, CBCP**
mjdecker@agilerm.net

Introduction

Penetration testing (pen testing) requires the use of special network assessment tools and attacker techniques. Application of these tools and techniques in a production business environment must be employed in a professional manner such that careful consideration is given to providing a methodical and orderly delivery of service. People, process and technology must be balanced to ensure that the tested party receives meaningful and valuable results.

People - Key people need to be identified for pen testing activities. This includes managers to preside over the exercise, assessors to perform the test, and those responsible for day-to-day enterprise security and network operations. Bear in mind that the latter group, though identified, is not necessarily made aware of the timing and nature of the test. The right people with the right skills must be put to the task to obtain satisfactory results, thus the assessors must possess knowledge and experience with both the process and technology in order to be effective.

Process - Webster's Dictionary defines process as "a series of actions, changes, or functions that achieve an end or result." In short, process is the means to a goal. This article introduces a workflow for penetration testing activities and introduces a penetration and vulnerability testing methodology (P and V methodology) to facilitate the process.

Technology - The primary technology under consideration includes the tools to complete the test and the systems to be tested. There are no silver bullet technologies that replace the skills required to successfully find and exploit vulnerabilities.

Many books and articles have devoted considerable attention to the technical component of pen testing. If you're seeking to learn technical secrets to hacking an application server, this article will not provide any useful scripts. Nor is it the intent of this article to discount the value of the technical skills of a good pen tester. On the contrary, the right people with the right tools must be put to the task to obtain comprehensive and meaningful results. The intent of this article is to focus on the penetration testing process and pay it the attention it deserves, yet rarely receives.

Why Process is Paramount

Does everyone who contracts to have a pen test performed really want to have their systems cracked open and to have the details written up in a report for senior management to review? Give this a little thought and you should realize that some of the targeted entity's personnel might perceive the proposed testing to be a threat. It may be in their best interests that the pen test be conducted in a professional manner by individuals who

don't have the skills to succeed in finding and exploiting all but the most obvious vulnerabilities. Barring their control over this aspect of the test, it is likely that they will diligently protect the assets under their control, at least for the period of the test. On the other hand, many pen testers can't be satisfied at the end of an engagement if they haven't broken into anything. If the goals of the testing aren't clear, and if the rules of engagement aren't well documented and communicated, then human nature will manage the test. The critical "process" component of the engagement will break down and value to the business will not be maximized, if obtained at all.

Value from Penetration Testing

The difference between pen testing and vulnerability assessments is straightforward. A vulnerability assessment identifies and categorizes all declared vulnerabilities but doesn't permit exploits. Pen testing doesn't imply that all vulnerabilities have been identified, but exploitation of vulnerabilities found by assessors is expected. Attempts to reach critical back-end systems will be made by the assessors, usually to highlight that existing vulnerabilities represent a serious threat to the organization. An activity that includes identifying and categorizing all vulnerabilities yet also permits exploitation of those vulnerabilities is both a penetration test and vulnerability assessment (P and V).

Value is derived via meeting the business needs of the organization under test. If the targeted entity desires to learn where they are vulnerable, such that they can remediate their security issues, then a vulnerability assessment is a sound approach. Penetration testing provides minimal value in this case because the vulnerability is going to go away. If the targeted entity sponsor desires to drive home the point to senior management that the business is at risk because of inadequate budget or other issues beyond their immediate control, then a pen test may provide the high impact, eye-opening report to serve as the catalyst to fulfill the project sponsor's requests.

Red Teaming

The methodology presented in this paper utilizes the concept of red teaming. Red teaming stipulates that three teams—red, white and blue—will preside over testing activities. The process begins with baseline reconnaissance activities by the assessors to establish engagement scope, including domain searches, identifying IP ranges and researching corporate facts. The target entity may choose to provide this information, but the assessment team should always perform some of this as a matter of due diligence.

Following the above preparation, it is time to meet with appropriate personnel to establish the engagement goals. Example goal statement:

"The goal of this exercise is to identify and exploit vulnerabilities in the company's Information Technology (IT) assets, to reveal how an external attacker with no advance knowledge of the target network might gain unauthorized access to IT resources, and to test the capabilities and responsiveness of network security systems and personnel. Actual exploits may or may not occur depending upon the severity of the impact to operations."

This example indicates a "black box" test, since the assessors will have no advance knowledge of the systems to be tested. A "white box" test would indicate that the assessors would be given detailed knowledge of targeted networks and systems, thus emulating attackers with insider knowledge. Note, too, that the responsiveness of network security systems and personnel is being tested in this example. This will have a dramatic impact upon the test plan that the assessors will use, as they will apply stealth where appropriate to meet the engagement goals of finding all vulnerabilities and exploiting selected ones within the allotted time period for the testing.

The next step is to agree upon the tasking to be performed, such as social engineering, war dialing, denials of service, wireless testing, and tests of physical security. This process further clarifies the consequences that may be associated with testing activities. For instance, the targeted firm may permit social engineering and testing of physical security. If so, are they comfortable with the assessors gaining facility access at closing time, waiting quietly in a vacant conference room until all personnel have left for the evening, and proceeding with testing activities throughout the night? Are they aware that the likelihood for system disruptions can be minimized, but not guaranteed? Such issues should be discussed and documented.

Rules of Engagement

The result of this collaboration is a documented rules of engagement (ROE). All key members of the three engagement teams are documented in the ROE. The ROE is a living document that can be modified during the course of an engagement, but all teams involved must approve amendments to the ROE. The ROE facilitates communication of the controls to be placed around testing activities, and when signed by the engagement sponsor, becomes a "get out of jail free card" that assessors will carry throughout the testing period.

The structure and function of each team is outlined as follows:

Red team - The red team is the assessment team that will perform the testing. These should be trustworthy individuals with whom the tested party is prepared, either directly or indirectly, to share their corporate secrets.

Blue team - The blue team is typically LAN administration and/or the network security personnel responsible for day-to-day operations of the targets to be tested. The blue team always exists, but may not be informed if or when a test is to take place. The engagement goals drive this decision. If a goal of the exercise is to measure effectiveness of blue team incident response capabilities, then the blue team should not be notified of the test.

White team - The white team represents managerial control presiding over the exercise. If the red team has questions about whether or not to pursue a course of action in a given attack, the white team will be consulted for authorization. It is important to ensure that a white team member is identified from within the reporting chain of all blue teams affected by red team activities, especially if blue team members are not to be notified of the testing. This greatly increases the likelihood that a manager knowledgeable of testing activities can intervene prior to blue team members turning red team activities over to the local FBI office.

Contact information for each team member becomes a part of the ROE, such that communication can be maintained during the course of the engagement. The white team may need to contact a red team member at 3 A.M. to confirm that a critical system outage was not a result of red team activities. The red team may need to contact a white team member to keep from going to jail after being caught in a corporate conference room at 3 A.M. Communication is a fundamental aspect of the ROE.

Penetration and Vulnerability Testing (P and V) Methodology

Figure 1 shows the P and V methodology at a high level, and you will notice that we have thus far covered activities associated with the first two steps of the process. At this point, a sound foundation for the test has been established using the fundamental red teaming concept.

Note, too, that no activities have been conducted to attempt to gain unauthorized access to any facilities or systems. No ethical or "white hat" hacking has taken place because it isn't ethical until the signed permission to conduct these activities is granted. Now that we have a signed ROE, we can begin the testing activities. The next three steps are intended to complete the discovery process and permit the assessors to detail their test plan.

Detailed Reconnaissance

"Detailed reconnaissance" is conducted to complete, in depth, what was performed at a cursory and non-intrusive level in step one. This is conducted in concert with baseline testing to obtain access to employee directories, e-mail addresses and other information that lends to social engineering efforts. Armed with this information, the assessors can make highly effective, yet relatively anonymous attempts to get user IDs and passwords, VPN configuration files, valid modem dial-up numbers, and other information that will grant authenticated entry to the target enterprise. Many tried and true social engineering attacks continue to be effective, but techniques lending to social engineering are continually being nurtured and harvested in the wild. The recent "Internet Explorer URL Spoofing Vulnerability" is a good example. Unpatched systems can be exploited to give the appearance that a user is viewing a known and trusted site. Exploiting this vulnerability, attackers can send the user to any site and spoof the location shown in the browser address line. Another common technique that accomplishes the same result is "cross-site scripting." The next obvious step is to configure the site to trick the user into entering sensitive information like Name, SSN, UserID, Password, etc. Of course, the ethical assessor will only be asking for UserID and Password to facilitate the testing process. If collecting names and SSNs is relevant to the test, then the requisite call is made to the white team to obtain permission. It's all part of the process.

Baseline testing is conducted to target known services in the environment without necessarily using automated tools that can fill log files, set off intrusion detection systems, and attract a lot of attention. This involves light use of tools to gain an accurate picture of the targeted environment and may include wireless network analysis, Telnet, FTP, password guessing, e-mail spoofing tests, SQL injection, etc. The objective is to obtain enough information to penetrate the enterprise perimeter without making a lot of noise.

Remember the Goal

Now that the assessors have collected a wealth of information, it is time to organize and assess the data. It is not time to dig as deeply into

the enterprise as possible, as the information collected may give clues that permit a highly targeted approach to specific systems, and may also steer the assessors away from honey pots or other defense mechanisms. This is a time to reflect on the engagement goals and make a determination as to whether or not the information collected is sufficient to meet the goals. If not, then determining whether or not the goals are realistic is in order. Perhaps social engineering wasn't permitted and sufficient information can't be collected? Whatever the reason, this would call for revisiting the goals and ROE to consider refinements to the engagement.

If the goals of the test are likely to be met with the data now at hand, then detailed testing of specific targets and avenues of attack can commence. Testing continues until goals have been met, or testing avenues have been exhausted. If testing avenues are exhausted and the red team has come up with no issues, then the targeted entity is reasonably secure from attackers operating under the same constraints as stipulated in the ROE. If the ROE was restrictive to the point that the targeted entity obtains a false sense of security from the test, then the assessors might consider working this analysis into the final report. More likely than not, though, the assessors will have found vulnerabilities that require attention. In any case, the tested party receives meaningful and valuable results.

Summary

My red teams have conducted many penetration tests and vulnerability assessments using this approach and have been very successful. Bear in mind that success is measured not only in terms of finding and exploiting target vulnerabilities, but also in terms of providing business value to the targeted entity. Whatever your project role or level of involvement in the testing, don't allow assessors to move forward with a "hack job" mentality. Make certain that testing activities are wrapped within a well-defined process and that the goals of the organization are going to be met when the final report is delivered. 🛠️

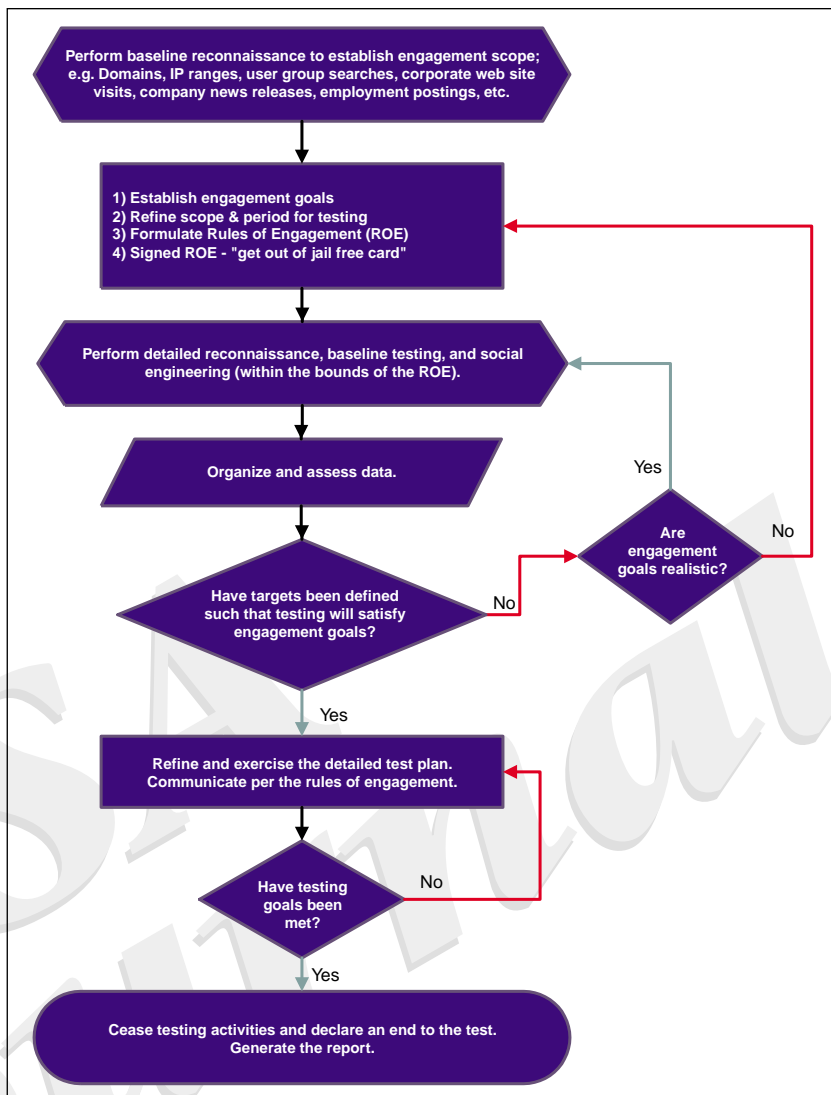


Figure 1: Penetration and Vulnerability Testing Flow Chart

Matthew Decker, CISSP, CISA, CBCP, is a Principal with Agile Risk Management, which specializes in security consulting and computer forensics services. Matthew served as president to the ISSA Tampa Bay chapter (1999-2003) and is a frequent lecturer on security topics, including security program development, security assessments and penetration testing.