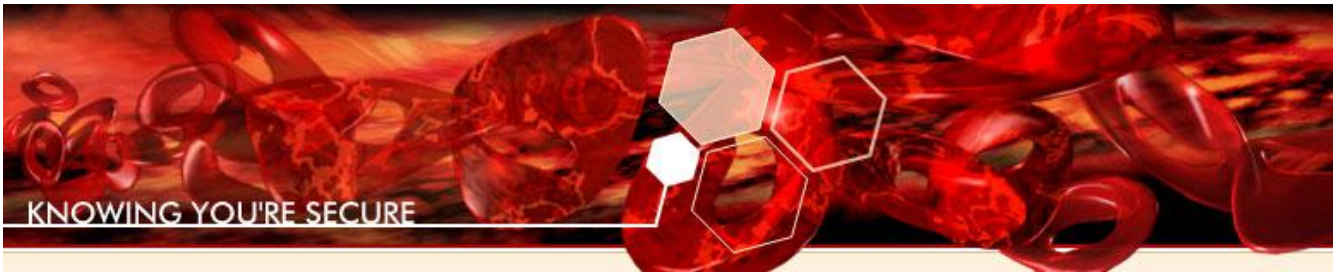

Understanding the Distinction between Vulnerability Assessment Tools and Penetration Testing Suites

January 21, 2010

By: Alex McGeorge, Immunity Inc.

Table of Contents

1 Introduction

This paper illustrates the differences and addresses some of the common misconceptions regarding vulnerability assessment products and penetration testing products. In so doing we must address the distinction between these two terms as they are understood within the larger security community. For an expanded look at how Immunity views security testing please see the white paper *CANVAS Exploit Categories Explained,* available on the Immunity website.

1.1 Target Audience

This paper is written for security professionals new to the industry, or managers of security teams who may not come from a security background. Computer security, like most technical disciplines, comes with its own terminology and definitions for that terminology that may conflict with how other industries may define these same terms. The distinction between vulnerability assessment and penetration test is one of the most common misunderstandings for security professionals new to the industry.

2 The Problem

Like most industries, computer security evolved out of a need which was identified by a problem. Modern networking and operating systems grew from designs and concepts first put into practice by academics sharing information between each other, without much concern for malevolent users of that technology. The user community was small, information was largely exchanged between people who knew each other personally, and therefore security was not a concern in the design process from the beginning.

Now that technology has matured and evolved past the imaginations of its inventors, it has been exposed to an incredibly larger group of users, whose motivations cannot be trusted. As a result the security industry was created to help mitigate some of the ramifications of these initial design decisions, as well as continuing poor software engineering practices. A practice which had been prevalent in the physical security world for decades was adopted by the computer security industry, namely to empirically test the security of a system to identify potential and existing security problems.

Industry consensus centers on two main technologies to aide in this testing, vulnerability assessment tools and penetration testing suites.

3 Vulnerability Assessment Tools

Vulnerability assessment tools operate on a “look but don't touch” basis. For a variety of reasons, the tests are designed to be non-intrusive.

3.1 Technical Details

A good deal of vulnerability assessment tool functionality can be compared to what's called 'banner grabbing.' Each host independently enumerated by the tool (or provided by the user) will be scanned to determine which services are listening. Those services typically present text or other data identifying their version at the beginning of the service transaction. This text is then referenced against a database containing software versions known to be vulnerable. If a match is found then the user is alerted to the vulnerability. Some tools can go deeper by interacting with the service to check for common insecure configurations or attempting to further pinpoint the version of the software beyond what it initially displayed. Another approach used by these tools is to log on to the computer and check the cryptographic hash of programs which run the service. Many tools can be configured not to do this because some users consider this overly invasive, but the idea of this practice is to gain additional certainty that a particular vulnerability may exist.

Though design and coding challenges certainly exist within vulnerability software development, banner grabbing and database references are not programmatically complex. As such these tools have grown in their ability to scale across large networks and assess many hosts simultaneously, which is, by contrast a programmatically complex process. Most tools which are competitive in today's VA software market are useful for very quickly gaining a high level understanding of a network's security.

3.2 Drawbacks

The primary criticism of vulnerability assessment tools is that they don't go far enough in determining if a computer is vulnerable. Keep in mind that all of the data examined by these tools is ultimately under control of the system administrator; therefore it is possible to alter the service enough such that the assessment tool will not flag a computer or service as vulnerable but underlying vulnerabilities may still exist. Further, mitigation may be in place which administrators believe will protect them against exploitation; these tools are incapable of testing this belief because of the limited depth in which they explore these issues.

In Immunity's experience answering the question of “are my systems really vulnerable?” is significantly more complex than looking a banner. It has become common practice that all enterprise systems have some type of anti-virus or other mitigating technology installed. These technologies are improving and may legitimately render vulnerability non-exploitable on systems they are installed on. The way to test this question is to attempt an exploit and further to be able to diagnose why an exploit failed. Solely relying on the output of any tool which does not do exploitation tends to produce a degree of false positives and/or false negatives.

4 Penetration Testing Tools

Penetration testing tools differ from vulnerability assessment tools, in that active exploitation of found vulnerabilities is attempted. This means that when a potential vulnerability is discovered the tool will attempt to take advantage of the vulnerability to affect a non intended action against the system being tested.

4.1 Technical Details

Previous to the early 2000s, penetration testers were forced to write their own software to exploit

vulnerabilities found in systems they were testing. Immunity and a number of other private companies and open source products have evolved to supply exploits to the larger security community for their testing needs. This software attempts to prove definitively that a system is vulnerable by demonstrating completion of the non intended action(s) the vulnerabilities allow. Typically this involves gaining a command shell or completing an action only allowed by a user of a higher privilege level.

Exploitation, especially of memory corruption vulnerabilities, has always been difficult. Now that more protections are in place to prevent successful exploitation of these vulnerabilities, the difficulty has increased even more. Companies and projects in this part of the security community focus on making highly reliable exploits that work across a large section of differently configured hosts.

4.2 Drawbacks

The two major criticisms of this type of security testing revolve around the invasiveness of the testing. Security professionals armed with pen-testing tools will ideally achieve administrative access to the system being tested and thus may require more trust than professionals armed with only vulnerability assessment tools. Secondly, exploiting vulnerabilities can lead to system or service instability on the system being tested, especially where inadequate attention has been paid during the exploit development process to cross-target compatibility issues. With the advent of professionally backed exploits the risks surrounding crashing services during an exploitation attempt have significantly decreased. Exploitation techniques have improved by a significant degree such that crashing services is now very uncommon.

Penetration testing also relies on the skill of the person conducting the penetration testing. A good rule of thumb is that pentesting is 60% human and 40% automation. The percentage for automation continues to increase every year by 5-10% however we believe that pentesting (as opposed to Vulnerability Assessment) will never be 100% automated for heterogeneous environments due to the changing vulnerabilities and the exploits required.

5 A Mixed Approach

Fortunately for the tester in charge of assessing the security of a system, there is no prohibition against running multiple tools. Many exploitation tools will accept output from vulnerability assessment tools to assist the user in focusing exploitation against hosts likely to be vulnerable.

5.1 Methodology

All penetration tests operate on a compressed schedule, the reconnaissance phase for attackers may last several months (some say years) where in a modern penetration test this phase may be a few days or perhaps only a few hours. In order to help overcome this disadvantage an operator can leverage the strengths of both tool sets to spend their time as productively as possible. Beginning the assessment with a vulnerability scan across the target assets which are in scope will allow for quick identification the next steps to take with a penetration testing tool. Once potential vulnerable hosts have been found a reduced list of hosts can be supplied to the tool doing exploitation such that operators can focus their efforts on those assets they may be able to access.

5.2 Advanced Methods

The upper tier of penetration tests require operators with the ability to find and write their own exploits. Enterprise patch management, from a technology perspective, is a solved problem with comprehensive offerings from many vendors and increased security awareness from systems administrators. Vulnerability assessment tools allow the penetration tester to prioritize exploit development efforts. Consider a penetration test of an entity's web facing assets; even if each provided service is current with each of the patches, the penetration tester obtains a list of the proportions of services running across these assets from the vulnerability assessment tool. This allows

the sophisticated penetration tester to focus their vulnerability research and exploit development efforts against software where compromise of those services will allow as much expanded access to the enterprise as possible.

5.3 Conclusion

Efficient penetration testing can draw from the strengths of both vulnerability assessment and exploitation tools. Users can leverage the scalability and reconnaissance capabilities of Vulnerability Assessment tools and the certainty provided by the results of pentesting tools. Ultimately using both techniques is in the best interests of an organization at it will provide the most accurate results possible in an effective timeframe.

Immunity, Inc:

www.immunityinc.com

sales@immunityinc.com

Phone: +1 212 534 0857

Fax: +1 917 591 1851

1247 Alton Road, Miami Beach, FL 33139