In Search of Low-Hanging Fruit: Improving Security and Privacy with Penetration Testing

by Bryan Miller

As a professional penetration tester and a business owner, I am often asked, "Why should I pay you to break into my network?" There are many reasons for doing so, and they have been discussed in many different places over the years. In fact, there are probably as many reasons for performing a penetration test as there are for *not* performing a penetration test.

In this article, I will explain what penetration testing is[1] and give some reasons for and against performing such testing. I will also describe some of the issues involved in deciding whether to perform penetration testing by using internal staff or by outsourcing the testing to a security vendor.[2] Penetration testing will also be discussed from an IT security and privacy perspective. I then describe the concept of "low-hanging fruit" and discuss the benefits of performing penetration tests to discover it.

WHAT IS PENETRATION TESTING?

As a security professional, I feel I have an obligation to my clients to try to persuade them to perform periodic testing from both internal and external perspectives. I use the term "persuade" because oftentimes it comes down to a passionate discussion about the risks and rewards of performing such tests.

Before going too much further, I should define what I mean by "internal" and "external" testing. An internal penetration test is typically performed by plugging into the client network as would any normal employee. One of the goals of penetration testing is to test for vulnerabilities that could be exploited by employees, contractors, guests, and automated attack software such as worms, viruses, and trojans. The current use of malware by attackers is increasing, is often combined with other attacks (such as phishing), and can lead to identity theft. There are many security and privacy concerns related to keeping such malware out of an organization.

An external penetration test is performed by attacking the client from outside the security perimeter, typically focusing on wireless, dial-in, and VPN access plus all Internet-facing computing resources. Such testing models the attacks that could be carried out by anyone around the world with the time, tools, and motivation. This is typically the area that the majority of IT security personnel spend the most time, energy, and money controlling. Management understands the concepts of "perimeter security," and such purchases require less justification than other security initiatives.

Penetration testing can also include social engineering components. Some of the common social engineering tests include dumpster diving (i.e., going through an organization's trash to look for sensitive information), sending phishing e-mails to employees, trying to gain physical access to facilities dressed as repair personnel, and testing physical controls, including doors, locks, cameras, and fencing. There are many regulations regarding the proper disposal of paper documents, and thus the dumpster diving test is important to ensure that privacy concerns are being properly satisfied. Phishing e-mails test employees' willingness to accept or send sensitive information via e-mail and are used to determine whether the organization's privacy procedures are being followed.

For years security professionals have debated the definition and merits of penetration testing. Many security practitioners and vendors still debate the meaning of terms. To differentiate themselves, vendors use such terms as "vulnerability assessments," "tiger teams,"[3] "white hat hacking," "black hat hacking," and so on. While there are technical distinctions between the terms "vulnerability assessment" and "penetration test," for the purposes of this article I will stick to "penetration test." Regardless of what term you use, the goal is to protect the electronic assets of an organization and help it comply with all required privacy regulations. There is a fair amount of overlap between IT security and privacy, and by performing penetration tests, we can satisfy a fair number of requirements for each area.

WHY SHOULD WE TEST?

Some of the reasons to perform a penetration test include:

- Satisfying legal and/or governmental requirements such as HIPAA, SOX, or the Gramm-Leach-Bliley Act (GLBA)
- Complying with industry standards such as the Payment Card Industry Data Security Standard (PCI DSS)[4]
- Complying with internal audit requirements
- Developing a baseline of the overall security posture for new management
- Assessing the security posture of an organization in an acquisition or merger opportunity

I have seen many cases in which security or privacy personnel were able to implement sweeping changes in current policies after a security audit showed sensitive data at risk.

One of the real benefits of performing penetration tests is what I call "putting together the pieces." Management needs to understand that this is where the real value lies in performing penetration tests. Most people can clearly understand the danger in having a weak password on a server, but a penetration tester can use that password to gain access to another server. This access will often provide information needed to take control over an organization's network infrastructure. The tester must follow the trail and use the clues provided by one device after another to eventually gain access to the really important and sensitive data. Examples of sensitive data often discovered during penetration tests include payroll data, employee information, client data, and financial data. The fact that the penetration tester can access this information during testing demonstrates that the organization has privacy issues it needs to address.

Compliance and security employees often ask for penetration tests to be performed because they need to know the organization's current security posture, whether it is to satisfy a legal or privacy requirement such as HIPAA or SOX or because of a previous data breach. The audit department can use the results of a penetration test to help define security and privacy policies or to give upper management the ammunition they sometimes need in order to enforce such policies. The legal department should welcome penetration tests since they prove due diligence on the part of the organization. Performing a penetration test does not guarantee an organization will not have a security breach resulting in a privacy violation, but if such a breach occurs, at least the management team can point to the testing as proof of their due diligence.

Of course, to prove they are sincere in their desire to limit privacy violations that could result from lax IT security, management needs to insist that the required remediation take place after penetration tests are complete. Privacy and security concerns are often disjointed in many organizations because the responsibility for each lies in separate departments. Information security is typically a component of IT, while privacy is generally the concern of compliance or legal departments. While security and privacy can greatly impact each other, historically they have been kept separate. Today, however, the new trend is to recognize the impact they have on each other and to begin to blend the functions of security, compliance, and privacy. This blending offers a tight synergy and can allow for economies of scale unavailable in current management structures.

Penetration testing is also appropriate for measuring the effectiveness of existing IT security and privacy controls, policies, and procedures. The tests can focus on specific applications, operating systems, departments, or physical locations. Security and privacy controls — including access controls (e.g., wireless and dial-in authentication), application controls (e.g., passwords and authentication tokens), and physical security controls (e.g., badges and biometric controls) — should be thoroughly tested. If an organization has a dedicated information security department, the results of a penetration test can help garner support for existing security policies that may not be stringently enforced.

The results of penetration testing can also prompt new security and privacy policies. Many of the controls mentioned previously are crucial in meeting privacy requirements. With the growing number of identity theft cases comes a higher level of responsibility on the part of organizations holding sensitive data. Proper implementation and monitoring of privacy controls are essential to ensuring that organizations can safely store and manage sensitive information. I have seen many cases in which security or privacy personnel were able to implement sweeping changes in current policies after a security audit showed sensitive data at risk.

WHY DON'T WE TEST?

Over the years, I have heard many reasons for not performing penetration tests. These include:

- "We already know where everything is broken."
- "If you tell us what's wrong, we'll have to fix it."
- "We don't have anything that hackers want."
- "We're too small to matter."
- "We haven't fixed the things you found broken last time."
- "Our employees don't know how to do bad things."

While there aren't right and wrong responses to each of these objections, I certainly feel there are more and less appropriate responses. One appropriate response is to remind clients of their obligation to protect the sensitive information they possess on their employees, clients, and customers. There are many privacy concerns relating to employee information that need to be addressed. Simply hoping that your employees and contractors are honest and wouldn't try to access unauthorized information is not enough. Each organization has some responsibility to implement appropriate security and privacy controls and to periodically test those controls.

Where appropriate, an appropriate and effective response is to help the client understand that security and privacy compliance is often mandated by state or national law. It is unfortunate but true that some organizations would not provide a sufficient level of information security unless legally required to do so. Given the many different statutes that are in effect today, it is hard to imagine having to explain to a company why these privacy regulations are needed. Yet it is important to convince them that complying with privacy regulations makes sense for reasons other than simply avoiding regulatory violations.

Compliance is good because in the long run it saves the company time, money, and reputation. Employee lawsuits due to privacy violations cost companies millions of dollars each year and often result in employees and customers losing faith in the integrity of the company. The effects of privacy and security violations are seen in the news each week, with companies receiving fines and bad publicity for each violation. Some companies never fully recover from large security or privacy breaches. Others will recover but carry that stigma for a long time and spend large amounts of money in advertising campaigns designed to bolster their corporate reputation.

DO IT YOURSELF OR OUTSOURCE?

If you're still reading, I hope you agree that penetration testing is a necessary undertaking. Debate continues on whether internal or external testing is more important, as well as on the frequency of testing. But most security and privacy advocates agree that periodic security audits need to be performed. Some clients alternate internal and external testing on a yearly basis. Others perform external tests on a more frequent basis, such as quarterly or semiannually. Some clients train their internal IT staff to perform the tests, while others only use external resources to keep the separation of duties clear.

At one time, firewalls and other security devices had arcane syntax and were often hard to configure and manage. Today, modern firewalls have rich GUI command interfaces and software wizards that greatly reduce the amount of knowledge that security technicians need to properly configure such devices. Between the advances in firewall technology, the increasing use of antivirus and anti-malware software at the perimeter, and an increasing awareness of internal threats, the overall security posture for many organizations has greatly improved. However, much still needs to be done to ensure that all organizations, both regulated and nonregulated, put forth the due diligence to ensure privacy and security concerns are being met.

It is unfortunate but true that some organizations would not provide a sufficient level of information security unless legally required to do so.

Once you've decided that penetration testing is a good thing, how do you go about doing it? One option is to outsource the whole process to a reputable security vendor. This option is appealing because it makes the whole process nice and neat and keeps the internal auditors very happy. Auditing best practices generally recommend that outside consultants perform such tests since there is a clear separation of duties and the chance for conflicts of interest are eliminated. However, it is perfectly acceptable for internal IT staff to perform tests throughout the year and then have an external consultant perform the tests for official compliance reporting. This way the cost of the external consultant is reduced, since most of the issues would already have been found and resolved. If you do choose to outsource, it never hurts to

understand some of the process and terminology just to make sure the vendor you choose is using an acceptable methodology and that the results are sufficiently documented to allow you to remediate the issues.

If you choose to do the work using your own IT staff, the first step is to select an acceptable methodology. There are many different methodology documents in use today, [5, 6] and they all basically attempt to ensure that all areas of network infrastructure devices are properly tested. Some of the more popular ones are OSSIM, COBIT, and those developed by the Center for Internet Security (CIS), the US National Institute of Standards and Technology (NIST), and the US Central Intelligence Agency (CIA). Some methodologies are more structured and rigid than others, and you will have to examine them for yourself to find the one with which you are most comfortable. There is no right or wrong answer in choosing a methodology. The main decision factor should be your comfort level and a solid understanding of the techniques employed in the document.

As a business owner, would you rather spend $5,000 to find a Web server vulnerability that could only be exploited by two hackers on the planet or to know that your administrator password is easily guessed and could be exploited by 30 million people?

The next consideration is tools and training.[7, 8] There are two schools of thought concerning tools and training. The first school advises going to training first and then starting to learn the tools taught in class. The second school recommends spending time learning the tools and then going to training. The goal of the second school of thought is to allow you to fine-tune your skills, since you will already be familiar with the tools discussed in class. Again, this decision is a personal one and will differ from person to person.

The choice of tools is a very crucial component of any good penetration tester's arsenal. When comparing tools, look for those that provide security and privacy reporting options. Many tools have report templates for common regulatory requirements such as HIPAA, SOX, and PCI DSS. Most professionals performing penetration tests will have well over 100 tools designed to test a wide variety of operating systems, applications, and infrastructure devices. When running tools during a penetration test, always test any given device with several tools and never trust one tool too much. Another consideration is which devices will be tested and how often. Generally, it is best to test all devices connected to your network on at least an annual basis.

LOW-HANGING FRUIT

When performing penetration tests, the low-hanging fruit is the most obvious target. Why is this? Simply put, testing time = dollars. Clients are always looking for the most benefit from each dollar spent. As a business owner, would you rather spend $5,000 to find a Web server vulnerability that could only be exploited by two hackers on the planet or to know that your administrator password is easily guessed and could be exploited by 30 million people? Some specific examples of low-hanging fruit I have found include the following:

- Blank, default, or easily guessed database passwords[9-11]
- Common passwords across different platforms and/or architectures
- Default or easily guessed passwords on infrastructure devices
- Lack of proper physical security for servers and other network infrastructure devices
- Laptops without full-disk encryption
- Obvious SQL injection issues in Web applications[12]
- Missing patches on servers and desktops
- Remote control/access programs that don't require passwords
- Sensitive configuration data stored or sent via e-mail without encryption
- Insecure wireless access points

For the majority of clients in most vertical markets, testing for low-hanging fruit provides the best bang for the buck. Given an unlimited budget, any penetration tester would be happy to spend months testing for every possible vulnerability in all network devices. Unfortunately, this option rarely presents itself in today's world. Budgets are tight and timetables are short. Given the frequency of new vulnerabilities and the easy availability of the tools necessary to exploit them, even testing everything would only be a viable approach for a short amount of time. Security auditing needs to be thought of as a wheel that never stops turn-

ing or a goal that is never quite achieved. There are no 100% guarantees in the field of IT security, so testing of security and privacy controls must be ongoing.

So what does low-hanging fruit look like in the real world? It seems to cluster around three common areas:

1. Passwords
2. Patch management
3. Policies and procedures

It doesn't matter if the client is a local grocery store, a *Fortune* 500 retailer, a government agency, or a pharmaceutical plant. It is these three areas — which I like to call the "3 Ps of Penetration Testing" — that consistently show up during internal penetration tests. (Please note that I said *internal* testing. In external testing, the major issues revolve around insecure wireless access, improperly configured firewall devices, and application security.)

Passwords

The category of passwords includes all forms of passwords and similar authentication schemes. Here the low-hanging fruit takes the form of default application passwords; missing, blank, and easily guessed passwords on operation system accounts; and other password uses, such as SNMP community strings. Another common area of password weakness is cases in which administrators use similar passwords across different platforms; for example, network administrators using the same password for the Microsoft Windows account, the Oracle "system" account, and the Cisco administrative account.

Patch Management

Patch management for desktop PCs and servers always seems to be an issue even in organizations that have robust patch management applications and policies already in place. It is not uncommon to find missing patches from vulnerabilities that were announced three or four years ago! The implications of missing patches on security and privacy cannot be overstated. Missing patches account for a very large percentage of successful network attacks.

Policies and Procedures

IT policies and procedures are often the bane of a network administrator. Next to documenting network topologies and device configurations, policies and procedures generally receive the least amount of effort. Nobody likes to write them, and few people read them. Yet they are critical to the overall success of any information security and privacy plan and should drive the configuration of all security devices.

There are many reasons why organizations don't have current IT policy and procedure documents. The first reason is that it takes a lot of time to create them, and managers don't often get evaluated on such projects. Metrics are developed to measure and reward successful network implementations, short response times for help-desk users, and great call qualities for new VoIP implementations. Few corporate leaders are going to reward IT managers for well-written policy documents. Another reason for not having accurate policy documents is that often the person writing them has no authority to enforce them.

The question of enforceability is usually illustrated by an organization's password policy. The security officer might write a policy indicating a minimum password length of eight characters. However, the employees might complain that the password is too long and hard to remember. Ultimately, the password policy is changed to allow shorter passwords, say five characters. This effectively reduces the overall security and privacy benefits of having strong password policies.

Despite these obstacles, IT managers need to work together with human resources, legal, and compliance personnel to convince top management of the need for current, accurate policies and procedures. Well-written documentation is the key to an effective management strategy and in the long run will help save the company money by ensuring a consistent process for each management task. Consistent procedure documents also reduce the time spent training new employees, which in turn helps to save money. Finally, accurate documentation is a key component of most security and privacy regulations.

CONCLUSION

It is my hope that this article has successfully made the case for performing regularly scheduled penetration tests. When combined with enforceable policies and procedures, such tests can be an invaluable aid to any organization.

One caution regarding penetration testing is to remember that penetration testing is not a silver bullet. It will not detect all problems in your networks and applications, especially when custom code is involved. By searching for and finding the low-hanging fruit in your organization, though, you are taking a major step in

securing the information that gives value to your company. From a privacy perspective, removing the low-hanging fruit is one component of a program to ensure that sensitive data is not available to unauthorized users. Increasing the overall security posture by eliminating low-hanging fruit will give management confidence that their privacy concerns are being addressed and will help reinforce the notion that security and privacy are inextricably intertwined.

Regardless of how and when penetration testing is performed, none of the tests will be beneficial if the proper remediation steps are not completed. Remember, the goal is not just to fix what is broken, but also to incorporate the findings into long-term policies and procedures that will help prevent the problems found from recurring at some point in the future. Business owners do not want to pay for annual tests and continue to find the same issues year after year. Take the results of the tests and use them to refine your IT practices so that each year the list of vulnerabilities continues to decrease. You may never see that list reduced to zero, but the real business value comes from the pursuit.

ENDNOTES

[1]"Penetration Test." Wikipedia (http://en.wikipedia.org/wiki/Penetration_testing).

[2]Beaver, Kevin. "Outsourcing Security Testing: What's Right for You?" SearchCIO-Mindmarket.com, 22 October 2004 (http://searchcio-midmarket.techtarget.com/news/column/0,294698,sid183_gci1018599,00.html#).

[3]"Tiger Team." Wikipedia (http://en.wikipedia.org/wiki/Tiger_team).

[4]PCI Data Security Standard (www.pcisecuritystandards.org).

[5]McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed*. 5th edition. McGraw-Hill, 2005.

[6]ISECOM (www.isecom.org/).

[7]SANS Institute (www.sans.org).

[8]"Education Overview." Foundstone (www.foundstone.com/us/education-overview.asp).

[9]"Securing the Initial MySQL Accounts." MySQL (http://dev.mysql.com/doc/refman/5.0/en/default-privileges.html).

[10]"An Unsecured SQL Server That Has a Blank (NULL) System Administrator Password Allows Vulnerability to a Worm." Microsoft Help and Support (http://support.microsoft.com/kb/313418).

[11]Oracle9*i* Default Accounts and Passwords." Oracle Corporation (http://download.oracle.com/docs/cd/B10501_01/win.920/a95490/username.htm).

[12]"SQL Injection Walkthrough." SecuriTeam (www.securiteam.com/securityreviews/5DP0N1P76E.html).

Bryan Miller has over 25 years of information technology experience. He has a BS in information systems and an MS in computer science from Virginia Commonwealth University (VCU) in Richmond, Virginia, USA, and was a former Cisco CCNA instructor at John Tyler and J. Sargeant Reynolds Community Colleges in Richmond. Mr. Miller has also been a guest lecturer at the VCU Fast Track Executive Master of Science (FTEMS) program. Beginning in fall 2009, he will serve as an adjunct faculty member at VCU. His industry certifications include the Cisco CCIE in Routing/Switching and the (ISC)^2 CISSP. In August 2007, Mr. Miller founded Syrinx Technologies. He is a member of the Greater Richmond Technology Council, the Retail Merchants Association, and the local chapter of the Information Systems Security Association (ISSA). Mr. Miller can be reached at bryan@syrinxtech.com.