Legal Issues in Penetration Testing

By: Mark Rasch
Cyber Law Editor
Security Current
November 26, 2013

When I was a kid growing up in the Bronx, a high school buddy got a job as a "security tester" at the Alexander's department store on Fordham Road. His job was to shoplift. This was to see whether the security personnel were doing their job, or were asleep at the switch. On his first day at work, he successfully shoplifted for several hours, until at the end of the day, he was caught. When detained, he showed the security guards his

(temporary paper) ID card, and he was promptly beaten up. He wasn't sure whether he was beaten because the guards didn't believe that he was working for management at the time, or because he was.

The story illustrates some of the dangers associated with penetration testing. While there are many practical issues, there are many legal issues that pen testers must address, preferably before they begin an engagement. What follows is a brief primer on things to consider.

1. **Legal Authority**

Let's face it, when you are engaged in pen testing, you are in a sense "breaking in" to a computer or computer network. Of course, ethical hackers would only attempt to penetrate a system at the behest of the owner or operator of the system, or otherwise test systems with the actual or implied consent of someone with authority.

There are many different types of pen tests. A software code review for vulnerabilities can be part of a pen test. A ping sweep can be part of a pen test. A probe or exploit. A configuration review.

Computer crime laws, like 18 USC 1030 make it a crime to access or attempt to access a computer or computer network without authorization or in excess of authorization. What constitutes "authorization" and who can authorize such access can quickly get muddy.

Thus, security professional Scott Moulten conducted a pen test on a Georgia city's security when they wanted to link their network to the network of the County for which Moulten was working to provide e911 services. Moulten performed a port scan and throughput test on that city's network to see if the computers were vulnerable to exploit. When Moulten's port scan revealed significant vulnerabilities, he reported them to his employer and its customer, the County. Embarrassed by the findings, the city called the Georgia Bureau of Investigation, which searched and seized his computer, and arrested him for violating the Georgia computer crime laws. The statute in question makes it a felony to use a computer with the intention of "obstructing, interrupting, or in any way interfering with the use of a computer program or data… regardless of how long the alteration, damage, or malfunction persists." Since the port scan

CISO Spotlight
Contributors
Executive Overviews
Executive Viewpoint
Expert Insights
Featured Articles
White Papers

infinitesimally slowed the computer, the government supposed, Moulten violated the statute.

Similarly, Stefan Puffer, a Houston computer security consultant conducted a “war driving” exercise, with the head of the Harris County’s Central Technology Department and a reporter for the Houston Chronicle. Puffer demonstrated that the Harris County clerk’s office’s 802.11b network was misconfigured to allow anyone to have access to the network. Puffer claims that he stopped the exercise when he saw the misconfiguration. Harris County discovered pornography on one of the computers, and after all the County employees denied any involvement, they arrested Puffer for hacking. Tens of thousands of dollars of legal bills later, a jury acquitted Puffer in all of 15 minutes.

When Bret McDanel discovered that his former employer was continuing to advertise as “secure” an email service that had a significant vulnerability, and a service that the former employer refused to fix, he decided to take action. He emailed users telling them about the vulnerability and directed them to his own website for information about the vulnerability. McDanel was not only prosecuted, but convicted and served 16 months in jail, after which the Department of Justice conceded that the conviction was wrongful.

So the lesson learned here is that penetration testing, even when authorized, can result in a host of legal trouble. Pen Testers must make sure that they have written, signed and clearly enunciated authorization to conduct their tests.

Get Out of Jail Free

Before beginning a pen test, the parties should enter into a contract indicating exactly what the pen testers will do (and will not do) and the range of IP addresses, subnets, computers, networks or devices that will be the subject of the pen test. If the test includes a software review or decompiling, make sure that the copyright to the software permits (or does not prohibit) the reverse engineering or code review. The pen tester should get a “get out of jail free” card from the customer, specifically indicating not only that the pen testing is authorized, but also indicating that the customer has the legal authority to authorize the pen test. If a cloud customer authorizes a pen tester to test their network in the cloud, this does not mean that the cloud provider has authorized the test. The cloud provider could go after the pen tester for unauthorized access.

Another practical problem for pen testers is getting the scope of the pen test wrong. If a customer provides an incorrect (or incorrectly transcribed) range of IP addresses to be tested, and the pen tester tests against these IP addresses, the pen tester may find himself or herself on the wrong end of an FBI investigation, or a hack-back. The situation is even worse if the customer provides a correct IP address range, and the pen tester attacks the wrong IP addresses. Ooops.

2. **Damage Control**

Another legal issue that comes up in pen testing, particularly when pen testing is conducted on a production or live system, is the potential impact a pen test may have on the users of the system. So when conducting a pen test, it is important to notify the customer in writing about the potential harm, damage or disruption that may occur even when a pen test is performed perfectly. This "harm" or "damage" may include harms or damages resulting from the responses of users to the pen test itself (including their attempts to remedy problems.) The customer needs to understand that a pen test can disrupt a brittle system, and that they assume the liability associated with conducting the test. This includes not only "ordinary" damages, but also "consequential" and "incidental" damages as well.

3. **Indemnification**

Okay, so you have a contract that specifically authorizes the pen test, and you have agreed that you will not be liable for damages you cause. But then there are those pesky third parties. Your pen test destroys the medical records of some patient, and voila! They sue *you*. In addition to specifying responsibility for damages, you want the customer to indemnify and hold you harmless for damages resulting from you doing what you say you are going to do.

You need to consider the scope of this indemnification. What if the customer provides you with the wrong IP address range, and you "hack" the wrong person? The indemnification can include the damages from the other system having to respond and/or secure themselves. But what if the FBI kicks in the door of one of your pen testers and injures (or worse) the pen tester, a colleague or a family member because someone reported the pen tester as a "hacker?" Who is liable for the damages then? Again, these are all points of negotiation, but you will not know if you do not ask.

4. **Hack-back**

Sometimes a customer will want you to hack back against an attacker. Sometimes the customer will treat you as the attacker, and hack back at you. The law treats hacking back the same as it treats hacking (for the most part.) It is unlawful.

The same is true for pen testing systems that are not in the control of the customer. Be careful here. It is not clear what gives a customer the right to authorize a pen test. Ownership? Intellectual property rights? Leasing of an IP range? Licensing of software? It is one thing to "own" a house, another to rent it. In addition, when doing a pen test, what are you testing? Physical security? Logical security? Software security? Software configuration? Hardware configuration? Settings? Does the fact that a company leases hardware, licenses software, and rents space affect their ability to give consent? Another issue for the lawyers.

5. **Scope of Work**

Also, a pen test agreement should specify exactly what will and will not be done, and the assumptions that underlie the agreement. For example, if the pen test is simply an "external" vulnerability assessment, we need to define the perimeter (what is "external") and the scope of the test. The same is true for an internal pen test ,what is being tested, how and for what purpose. Avoid terms like "state of the art" that have no real meaning, and simply elevate expectations. Nobody and I repeat *nobody* ever uses "state of the art" anything. By the time the agreement is signed, the state of the art has moved on.

Similarly, you need to define the assumptions that underlie the pen test. The pen tester will rely on the customer to define which systems need to be tested, and more importantly, which ones do not. When Cable and Wireless was hacked several years ago, it was as a result of a certification by a pen tester that they met a particular standard for security. They did not. The confusion arose when Cable and Wireless apparently told the pen tester that particular systems were not hooked to the Internet (or that they were going to be removed from outward facing domains) and therefore that they didn't need to be tested. What we have here is a failure to communicate.

You also have to define things such as when the pen test will be conducted (what does "off peak" mean?) the nature of the access required to do the pen test, the nature of the cooperation

necessary to make the test meaningful and the scope (and manner) of notice to be provided prior to initiating the test. You do not want surprises.

6. **Professionalism**

Another issue to be resolved is the "standard of care" or "professionalism" question. What kind of pen test are you conducting? Are you just doing a port scan? Turning on NESSUS and leaving? And what do you warrant and represent that you will find? A typical pen test should warrant that the pen tester will use the type of professionalism and skills commonly found in the industry, but not make promises that the test will find all, or even substantially all vulnerabilities or misconfigurations. Remember, it is as important to document the lack of findings as it is to document the findings themselves.

7. **Licensing and Certification**

GIAC offers certification in penetration testing (GPEN.) Similarly, IACRB offers certification in pen testing proficiency (CEPT.) The EC Council offers licensing of penetration testers (LPT.) But in some states a pen tester may be required to be a licensed private investigator. Think that is stupid? It is. But it may be the law depending on why you are conducting the pen test. If you are "collecting and evaluating electronic records for the purpose of presenting findings in court" you may be required to have a PI license. In one extreme Texas case, the company that monitors red light and speeding cameras was found to have violated the Texas PI licensing statute for exactly that reason. About a dozen states have laws that require people engaging in certain types of "investigations" to be licensed as a PI in that state. The issue typically arises in connection with computer forensics and incident response investigations or in connection with expert witness testimony. However, if the purpose of the pen test is to determine the manner in which property has been damaged or destroyed (e.g., because of a hack or attempted hack,) then these broadly defined statutes may impact the ability to conduct the test. Since many of these statutes carry civil and criminal penalties, it pays to do your homework.

8. **Venue and Jurisdiction**

Another key issue in pen test contracts is to determine where the pen test is being conducted. If a California Company hires a Maryland company to conduct a pen test on its computers in Nebraska, and the pen tester launches the test from

Pennsylvania, whose laws apply to the conduct of the test? The answer typically (but not universally) is whatever laws the parties have agreed to. But if the pen test goes bad and injures a user or customer in New York, you can bet that they will want to apply New York law if that law is favorable to them.

9. **Privacy Issues**

A successful pen test can result in the pen tester getting into a computer or computer network that they should not have had the ability to access. Also, it may include accessing data or databases which contain sensitive personal information, credit card information, personally identifiable information (PII) or Private Health Information (PHI). The pen test may expose the tester to sensitive information about citizens of the European Union, such as sexual orientation or political affiliation, data whose privacy is protected by law. Is the access to that information by the pen tester a "breach" of the database which must be reported? Must the pen tester sign a "Business Associate Agreement" agreeing to protect the data they just accessed? The pen tester must understand the scope and extent of their duty to protect all data they access.

10. **Data Ownership**

One issue that rears its head during pen tests is, who owns the information that results from the test? Clearly, the pen tester owns the methodology and the report template. Clearly, the customer "owns" the findings and recommendations. But what if the pen tester develops new methodologies for conducting pen tests or solving configuration problems on the customer's dime? Who owns these "works for hire?" Another matter for the lawyers to resolve.

11. **Duty To Warn**

Saying that the customer owns the report of the pen test creates another problem. Networks rarely stand alone. They are interconnected. What should a pen tester do if they discover major unplugged vulnerabilities that will impact customers, third parties, or the population as a whole? Is their duty only to tell the customer and keep quiet? What if they discover a zero-day vulnerability that may have system wide or industry wide impact? What should they do then? Even if the customer "owns" the data, does this mean that the customer can control the use of the knowledge the pen tester obtains? It's all a matter of what the contract says, and what the Courts will enforce.

Conclusion

A pen test agreement seems like a simple document. I will test, you will pay. But like any agreement, the devil is in the details. Competent and experienced counsel will be necessary to avoid pitfalls. And like everything else in life, let's be careful out there.