CAN PENETRATION TESTS PREVENT HACKER ATTACKS?

As seen in the Summer 2009 Issue of Ohio Record

BY JEREMY BURRIS, CISA, MCP, LPT, CPTS, CEH, ECSA

When it comes to doing an IT network penetration test, there is one important difference between a penetration test and a hacker attack: Hacker's don't have to follow the law.

What does that mean in terms of your internet security? Let's look at a few examples. A penetration tester will go to your Web site to gather information about your domain name. With this information, the tester can use tools that may show who owns that domain name and what Internet Protocol address is associated with that domain name. With your IP addresses, an attacker now has a "target" machine on your network that can be attacked from anywhere on the Internet.

A penetration tester may suggest that you hide your company's identity either by putting false information in your Domain Name Service registry (if your local Internet Service Provider will allow this) or by simply not providing any information at all. Anyone looking up this IP address will only learn which ISP has provided the IP address. At this point, a penetration tester would likely conclude that he can't determine which specific IP addresses are those of your company.

However, a hacker does not follow the law. The hacker can simply "hack" into the ISP's network and search its customer database. At this point, your bank is at the mercy of your ISP's network security (which may not be as strong as your own).

As another example, consider the timing of a penetration test versus an attempt to hack. A penetration tester may be given anywhere from a week to a month to find weaknesses in a company's network. Usually, there are limitations on the period during which these tests are permitted and even certain hours of the day (or night) when they can be carried out.

A hacker, of course, has no time limits. They are more likely to attack your network when they know that no one is working, to minimize risk of detection. In order to determine which ports are open on a given IP address (which tells an attacker what services and versions of software are running on your systems), a knowledgeable hacker might scan as few as one port per month. Doing so offers anonymity because that one port discovery "ping" will get lost in the hundreds of pages per month that a typical firewall produces and will never be investigated. By testing just the common ports that they know they can exploit, within a year or two, they can have quite a bit of information about the host IP address they are attacking. Hackers will work patiently to get into a network, especially if going really, really slowly means not getting caught and going to jail.

Or take the example of "social engineering," or tricking employees into performing actions or divulging confidential information. This is probably the top way hackers get information about your company. While a good penetration tester will travel to your remote branch locations and will try a few tactics to gather information from your own employees, there are legal limits to what

is acceptable. A penetration tester cannot try to trick employees of your vendors into giving out sensitive information, unless the vendor has given explicit permission. A hacker can and will.

Does this mean penetration testing is at a disadvantage? On the contrary. A penetration tester can use tools that do a better (and quicker) job at finding vulnerabilities on your network. For example, a vulnerability scanner run against your network would never be used by a hacker because these tools are very "noisy" from a network traffic standpoint. By generating so much traffic on your network, these tests scream to your network administrator, "We are being attacked!" Hackers must use slower methods and go through a painstaking process to find information and you can set up countermeasures against these methods.

With a properly implemented and conducted penetration test performed by a certified ethical hacker, the penetration test has the potential to provide far more information than anything a hacker may find (thus the reasoning for the penetration test) but it cannot show *every vulnerability* on your network because it must operate within the law. Some penetration testing scopes are better than others, but even the best penetration tester is not going to break the law to show you where you are vulnerable. While these tests are extremely helpful in tightening both your internal and external network security, keep in mind there are limits to their effectiveness.

About the Author

Jeremy Burris, CISA, MCP, L|PT, CPTS, C|EH, ECSA is a Senior Technology Services Consultant at S.R. Snodgrass, A.C. Jeremy's areas of expertise include Network Attack and Penetration and other IT audits for financial institutions and private companies. Snodgrass is best known for our expertise in the financial services industry. We have extensive industry business experience and sound working relationships with all of the regulatory agencies. Examples of that experience are displayed on our Web site's *Knowledge Bank* at *www.srsnodgrass.com*, where you can view several articles and video presentations on banking-related topics.