

# What You Need to Know Before Buying Penetration Testing Services

Ron Trunk, CCIE, CISSP, Senior Consultant, Chesapeake NetCraftsmen, LLC

“On the surface, penetration testing sounds like a good idea – if ‘experts’ can’t break into your systems, then you’re pretty secure, right?”

Many organizations use penetration testing services as a way to determine their network’s resistance to Internet-based attacks. Outside companies are regularly contracted to launch attacks against the organization’s Web sites, e-commerce sites, and other accessible devices. These penetration testing services charge a fee for performing this evaluation, usually on a monthly basis.

Most firms offer two types of penetration testing: “black box” and “clear box” (also called “crystal box”).

In the black box version, the tester simulates an attacker with no knowledge of your network, *i.e.*, someone scanning the Internet, looking for vulnerable systems – just like a burglar walking down a street, trying everyone’s doors to see if any are unlocked. The tester “pretends” that they know nothing more about your network than your IP address or domain name – hence your network is a “black box.”

With clear (or crystal) box testing, the tester is provided information about your network. The information can be very detailed, including network diagrams, passwords, *etc.* Here the idea is that the attacker simulates an “insider,” with some knowledge of your system. Armed with this information, the penetration tester attempts to gain access to your network. This time the burglar knows which doors are most likely to be unlocked.

On the surface, penetration testing sounds like a good idea: if “experts” can’t break into your systems, then you’re pretty secure, right? The problem often is that penetration testing by itself only provides limited “bang for the buck,” especially when committing to a regularly scheduled service, as most providers sell. The money could be spent on other things that would improve your overall security.

Before you run out and hire a penetration testing service, consider carefully where the testing fits in your overall security plan (you do have one, right?). Here are just a few things to think about before you start testing:

## 1. Start by securing the perimeter.

Does your security policy define what traffic is allowed in and out of your network? Have you identified all the applications and/or services that can be reached from the Internet, or make use of the Internet? Does your organization even have a security policy?

Are all your servers (public-facing, especially) fully up-to-date with patches and/or service packs? If not, don’t waste your money with a penetration test – you *are* vulnerable and you need to fix those problems. Just as importantly, you need a way to insure that critical updates are always applied in a timely manner.

## 2. Don’t be hard and crunchy on the outside, soft and chewy on the inside.

Recent crime statistics indicate that the majority of losses due to computer attacks come from inside, rather than outside your network. So it makes sense to spend more of your effort and resources on prevention of an insider attack.

Have you implemented strategies to limit the damage of inside network attacks? Have you taken steps to minimize DHCP attacks, ARP attacks, Spanning Tree attacks and MAC flooding attacks – many of which are designed to gain unauthorized access from inside your network?

Is your network designed to limit the damage caused by a network attack? Is your network infrastructure (switches and routers) hardened to prevent unauthorized access? If a server is compromised, will your network design limit the harm that an attacker can do? Have you compartmentalized your network applications so a problem with one doesn't necessarily affect another? Even minor improvements to your infrastructure can make a big difference in your resistance to attacks.

### **3. Pay close attention to wireless networks – even if you think you don't have any.**

If you use wireless networking, are you still using WEP or MAC filtering, neither of which can be considered adequate security? If you think you don't have wireless, do you test for rogue wireless access points installed by well-meaning but unauthorized users? Could an unauthorized access point have become an open port to steal your data? More importantly, what steps have you taken to prevent or detect rogue access points? If the answer is "none," spend your money on that before you test.

### **4. You need more than hardware to make your network secure.**

How well-informed are your users? They are often the weakest link in the security chain. Could someone call up a user and, masquerading as help desk staff, persuade the user to reveal his or her password? Do your users leave their computers logged on when they're away from their desks? Are people in your company opening e-mail attachments from unknown senders? If these are open issues, then educating your users to be security-aware will be more valuable than performing a penetration test.

Finally, are your operational procedures and controls where they ought to be? Who is authorized to make changes to the network? Who checks that changes were done correctly? How often are the firewall policies reviewed for relevance? Do you have a meaningful and applicable security policy?

### **5. Don't count on penetration testing alone to make you more secure.**

Penetration testing can only show you a very narrow view of your network's vulnerabilities – much narrower than actually exist. Moreover, a penetration test is just a momentary snapshot of your vulnerabilities, since new ones are discovered all the time. By simply going through a list of open ports, un-needed services, etc., you are just patching holes instead of taking a systematic approach to your network security. Your time and money might be better spent designing security into your network.

The bottom line is that there's little value in penetration testing if you haven't taken the time to harden your network in the first place. You are just paying someone to tell you what you already know: your network is vulnerable to many types of attacks.

The best way to take advantage of penetration testing is to make it part of a comprehensive security plan. Implement security controls across the network in a systematic manner. That way, your test results will be not only be more meaningful, you'll likely hear more good news than bad.

**Chesapeake NetCraftsmen, LLC** delivers high-availability solutions for Network Design, Operating Systems, Applications, Security, Storage and IP Telephony with deeply experienced CCIEs who excel at Knowledge Transfer.

Chesapeake NetCraftsmen consultants include some of the most experienced Cisco CCIEs in the country. Most of our technical staff has a minimum of 10 years' of experience in the networking industry and many have taught Cisco Certified training.

**For more information on Chesapeake NetCraftsmen, [click here.](#)**