

How to Buy Security Testing Services

Jason Thacker, CISSP, CEH

Introduction

In recent years, the security services industry has boomed, and many companies promising security for those who buy their products and/or services have sprang up. For the most part, these companies' offerings will enhance your organization's security, but there are many potential traps and a good deal of wasted expense to be had if you choose poorly. The following paper will provide guidance in purchasing security testing services, and help you avoid problems you may encounter.

Definitions

Vulnerability Assessment – A vulnerability assessment is usually performed by a security professional using an automated set of tools, which is run against a certain set of IP addresses. A full vulnerability assessment will usually include vulnerability scans of all parts of the network, along with a review of policy, physical security, and interviews with the IT staff. The results of all parts of the assessment will be combined to create a report which identifies vulnerabilities within the organization and suggests a course of action to remediate those issues.

Vulnerability Scan – A vulnerability scan is usually part of a vulnerability assessment, and refers to just the automated scanning of a network for potential vulnerabilities using software tools.

Penetration Test – A penetration test is generally defined as a simulated, realistic attack of a target using a specified set of methods. The goal should always be the testing of existing security controls under real-world, worst-case scenarios. The reaction to an attack made by both staff and network should be measured and an assessment should be made of what vulnerabilities were found, which were successfully exploited, and a course of action should be proposed.

Steps for buying testing services

- 1) **Decide why you want testing to occur.** This will depend upon requirements placed on your organization by various legislation (GLBA, SOX, HIPAA, PCI, etc.), as well as those placed by your organization's governing body (FDIC, NCUA, etc.). Aside from requirements outside your control, you may want to perform testing because of internal policy, or just because you want to be secure. Whatever the case may be, it is important to keep in mind the reason this process is starting, and to make sure that the original goal is met in the end.

- 2) **Determine which parts of your organization need to be tested.** For both physical and network testing, it is important to set the scope of the project early on. It is important to keep in mind that the more complete the scope of the project is, the more accurate your assessment will be. Also keep in mind that the most damaging attacks usually come from the inside, so an internal test should be just as important as an external perimeter test.
- 3) **Determine what kind of assessment needs to be done.** For those just starting in the world of security assessments, a vulnerability assessment will give you a good starting point. Vulnerability assessments are generally more affordable than a full-blown penetration test, and should uncover the biggest security problems first. Be sure to hire a testing company that will come on-site for a walk of the facilities and an interview with the IT staff. You will likely need help with interpretation and remediation of the issues in the report, so be sure that your testing company will provide that. If you have already had several vulnerability assessments done, and you have passed at least one with no major issues, then the next step is to look in to a penetration test. A penetration test should cover a broad range of attacks on all major internal and external services. Once your network gets a passing grade on a penetration test, you should be pretty well secure. From this point on, penetration tests should be performed on a regular basis (about once a year), and whenever major network changes are made.
- 4) **Shop for a security testing company.** This may be the trickiest part, as every testing company has a different definition of what a penetration test or vulnerability assessment will consist of (what methods are used, and how deep the attack will go). One company may sell a penetration test that isn't nearly as thorough as another company's vulnerability assessment. Be careful to do your research and choose a company that really meets your needs. If you need help deciding, get the opinion of a trusted source. Also be wary of companies meeting any of the following criteria:
 - a. Headquarters or other main office outside the US
 - b. Sells hardware, software, or other related services as a cross-sell
 - c. Pushes contractual relationships longer than 1 year
 - d. Outsources testing (especially overseas)
 - e. Testing performed by non-certified personnel
 - f. Not willing to come on-site
 - g. Employs kids or convicted felons to do security work
 - h. One-person operations (unless your organization is also very small)
- 5) **Keep up the good work.** Unfortunately, there is no single solution for security. Security is a never-ending process, and needs constant maintenance to stay current. If the company you chose isn't meeting your needs, start shopping immediately. Even if your current company is doing well, it is still a very good idea to have another testing company perform an assessment on a regular basis. In

practice, a secondary testing company should be used about once every fourth or fifth test.

- 6) **Consider additional services to enhance security.** Once your organization's security is in good standing, consider employing an outside security monitoring service and/or patch management solution to further enhance security. Be mindful to use different providers for each service, and that no one service will cover all of your security needs.

13 Important Points

- **Check the location of the testing company.** Make sure the company you select is headquartered in the US. In the event of legal troubles, you will have the ability to seek compensation in court.

- **Make sure the company you choose doesn't outsource your work.** Security testing is very sensitive business, and should only be between your organization, and the one you select. Be VERY careful that the company you choose is not using overseas testers in Pakistan, Hong Kong, China, Russia, India, or any other country where our legal system cannot reach.

- **Unless your organization is very small, avoid doing business with "one-man-band" testing companies.** They often lack the resources needed to do all but the smallest of jobs without outsourcing their work.

- **There is no required standard for what a "Penetration Test" or "Vulnerability Assessment" consists of.** Be sure to dig deeper into what each company is actually offering, and how it fits your needs. Price is seldom an indication of what work is really being done.

- **Unless a fully certified professional comes on-site, the job isn't getting done.** The most important part of assessing security is being thorough, and no test should be complete without an on-site walk-through and interview with IT personnel.

- **Understand the results.** The company you choose should spend as much time as is required to help you understand the results of the assessment. Avoid any companies that simply mail you a report and send you on your way.

- **Ethics need to be paramount.** You would have good reason to be wary of a doctor who gives checkups, fills prescriptions, and provides therapy all at the same time. The same goes for security companies. Companies that provide security assessments, sell hardware and software, and provide managed services are likely not going to give you an honest review of your security.

- **Avoid long-term contracts.** The security industry changes on an hourly basis, so don't commit to any one security company for more than a year.

- **Change security companies on a regular basis.** While having a trusting relationship with a security company is important, your organization's security is more important. Just as financial auditors are required to change every 5 years, so should you have different companies check your security.

- **Use only security companies who employ certified professionals.** One of the very few ways to immediately check the validity of a company's staff is to ask for certification info. Look for one or more of the following: CISSP, GIAC, CEH, Security+, CISA. Also be sure that a certified professional is the one actually performing the tests on your network.

- **Bigger is not always better.** Security assessment is something that demands customized service due to its sheer complexity. Just as with many other industries, bigger companies will usually not be able to provide the exact service required to fulfill your needs.

- **Don't pay for what you can get for free.** Some companies will sell you resources that are freely available on the Internet. Libraries of pre-written policies, software, hardening guides, and other resources are sometimes rebranded and sold as a separate service. The security company you choose should be helping you find the resources you need as part of their service.

And, the VERY most important thing to keep in mind:

- **Ask the right questions, and get the answers in writing.** Use the above points to ask the right questions and get your security company to guarantee their answers in writing. If the prospective company can't do that, they don't need to be anywhere near your sensitive systems.