GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Penetration Testing
"The Third Party Hacker"

By:
Jessica Lowery
Information Security Specialist
Version: 1.3
February 2002

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Penetration testing is the process of probing and identifying security vulnerabilities in a network and the extent to which they might be exploited by outside parties. It is a necessary tool for determining the current security posture of an organization. A new CIO, for example, might order a penetration test to get a quick understanding, or "sketch," of potential problem areas in a local area network. Such a test should determine both the existence and extent of any risk. Target Companies expect third party vendors who perform penetration testing to be very honest with them, but this has proven not to be the case in every instance. Moreover, the risks associated with use of third-party testing organizations are somewhat different from those associated with the usual issues of penetration of the system from outside. This presentation is intended to help management make the right choice when outsourcing penetration testing.

Because maintaining the security of information systems is important in any financial institution, many such organizations are undertaking tests of the ability of outsiders to penetrate those systems utilizing third parties from outside the system. Such tests, however, carry their own risks, and both the institution and the public should understand these risks. Any organization contemplating a penetration test against a production network should understand the serious issues surrounding the decision and thoroughly analyze the risks associated with such a test. Because risk is a function of both threat and vulnerability, an effective risk analysis will reveal the extent of both. Just remember that without both threat and vulnerability, there is no risk. (3,7)

Risk = Threat x Vulnerability

Example scenario of penetration testing related to risk analysis

Corporate Trade Secrets Revealed to a Third Party Vendor = (% Loss in Corporate Revenue + % Exposure Rate)

After completing a risk analysis for penetration testing, senior management should focus on planning the test and deciding what limits they will place on access to their network by any third-party providers of penetration-testing services. But first, for purposes of this analysis, it will be helpful to discuss why companies choose to outsource penetration testing. (7)

© SANS Institute 2000 - 2005 Author retains full rights.

Why Outsource?

Companies choose to outsource penetration testing for a number of reasons:

- ✓ To determine the extent of system vulnerability not detected through in-house audits.
- ✓ To show customers how safely they can perform e-commerce transactions over the World Wide Web. Marketing departments frequently drive such demonstrations.
- ✓ As a prelude to restructuring the security system and enhancing the perceived value of institutional integrity for customers.
- ✓ Time constraints in performing such a restructuring are frequently involved in the decision to outsource penetration testing. (3,4,9)

What to Look For When Evaluating Third-Party Vendors

Does the testing organization ask to see the company's security policy?

Those evaluating third-party vendors should note whether those organizations being considered have explored and analyzed in depth the company's security policy to determine company standards or best practices in making their proposal. This should occur before any negotiation between the two organizations takes place. (3)

Does the penetration-testing group have liability insurance to cover themselves?

All penetration-testing organizations should have liability insurance sufficient to cover the costs associated with the risk of losing a client's proprietary information and any potential loss in revenue that might result from unexpected downtime caused by their activities. Management must also assure the company can recover from a loss of data during testing by having in place adequate incident-response and disaster-recovery plans that have been developed and verified before testing begins. (11)

During the initial meetings with management of the prospective penetration-testing team, management should pay close attention to the team leader to see if he or she asks for a designated "cutout" in the target organization. A cutout is essentially the company's in-house monitor over the course of the test. This person should be completely aware of how the test will be conducted, the time frame for the test, and how deeply the tests will probe the target system. This person must have the authority to

© SANS Institute 2000 - 2005, Author retains full rights.

intervene during the test, both to save engineers time if questions arise and to stop an event from occurring if it in itself poses an unacceptable risk to the company. (8,11)

Why Does the Organization Feel They are the Right Company for the Job?

At the end of the first meeting with representatives of a prospective vendor, it is a good idea to ask them why is why their company is the best choice for the job. Their answer should say several things:

- ✓ The prospective vendor should be able to demonstrate that their organization has well-qualified and trained engineers with at least five to ten years of experience in network security.
- ✓ The prospective vendor should be able to show that their performance ratings are quite high when compared to those of competitors.
- ✓ They should be able to point to a number of satisfied customers.
- ✓ Ideally, the prospective vendor will have worked on similar projects for companies with similar security issues.

Does the organization perform a bait and switch once the contract is drawn up?

"Bait and switch," in this context means, "Does the company sell their services using highly skilled and trained personnel, only to employ unskilled engineers when the work is actually performed?" Management should also determine whether the testing organization employs hackers as part of its testing team. A hacker is a person who breaks into, attempts to break into, or use, a computer network or system without authorization, for personal amusement or gratification. Hackers often do not probe networks with malicious intent. However, hiring hackers is an insult to legitimate security professionals everywhere, and it degrades public confidence in the profession's integrity. Hackers know nothing that a well-trained security engineer will not also know, and you will not gain anything from hiring them provided the rest of the team is competent. (2)

What questions does the penetration-testing team ask about the targeted host?

Most penetration tests on an internal network should require only the IP addresses of the hosts being targeted. They might also inquire how those hosts are deployed over the LAN or WAN and what countermeasures are presently in place to guard against attacks (i.e. network diagrams, firewall configurations, IDS.) In general, a precise audit does not require knowledge of network configuration resources, and that information

© SANS Institute 2000 - 2005, Author retains full rights.

should not be given out unless the vendor makes a strong case that the testing team actually needs them. Hackers usually do not have the advantage of obtaining proprietary information before they launch an attack, so withholding that information usually simulates the actual conditions faced by real hackers more accurately than if the testers were in possession of detailed system information. Balanced against this, however, is the consideration that withholding proprietary information means the test may take more time and be more costly to the company. It may actually be the case that if proprietary information is given to the testing team at the beginning of the study, the testing team can focus on giving a more complete assessment of overall system security. Once again the target company must balance risks and validity issues. (3,8,10)

What should be off limits during the test?

In order to get a complete view of what could really happen if the company was attacked, all systems ideally should be included in the test. But even though this gives management the most information, it also exposes the company to additional risk, hence raising a "risk verses validity" issue. For example, would Company ABC really want to risk having a production OFX server go down during a penetration test and possibly lose a significant percentage of daily revenue? The person in charge of the penetration test should sit down with key personnel before testing begins and decide exactly the nature of the risks and whether adequate recovery systems are in place. Balancing such risks should be the responsibility of top management and not that of a third party. (3,8,9)

How many clients does the company have?

When evaluating penetration-testing organizations, it is always good practice to ask for references from previous clients. Tell them that management will be calling on those references. Management should require that the testing company provide a list of clients who have given them explicit permission to be used as references, to be sure, but if it is possible, should also ask for a more complete list of customers who can be checked at random.

Can the testing organization find a known vulnerability early in the test?

A potential customer could also set up a fake honey-pot, or known security vulnerability, in their DMZ before the actual testing is scheduled and see whether the testing organization finds it fairly early in the test. The testing company's performance on this test will provide an important gauge of the testing organization's level of security is and how well they can interpret their findings.(7)

Does the prospective vendor tend to use intimidating tactics?

© SANS Institute 2000 - 2005 Author retains full rights.

Management should not let a third party use intimidation. The testing organization is essentially the target company's employee during the project. Both company security and the project manager's job are on the line. If a testing company insists that employees of the target company "stay out of the way" during the project, find another prospect. The testing company should actively seek the involvement of the target company's staff both to ensure the integrity of the test and to reduce the vulnerability of both companies.(11,3)

Can the prospective vendor respond adequately to technical questions?

Management should be prepared to ask technical questions of any vendor presenting a proposal. For example, managers should ask the testing company specifically about the tools they use on the platform at the target company and how many tests will actually be used against it. If the target shop runs mainly UNIX, and the vendor says, "Well I thought this company was mainly a Windows shop," then managers should be prepared to probe more deeply to be sure they have the technical competence to work on the target company's platform. After being satisfied that the vender is sufficiently familiar with the target platform, interviewers might try probing them with other related technical questions such as, "Are there any tools that you are using that contain proprietary code that could harm our production environment?" It is a good idea to be aware of the many enumeration tools that testing companies currently use. Here are a few of the more commonly used tools:

Nmap – A very fast and user-friendly port scanner for multiple or single hosts on a network.

Nmap FYI:

- ✓ Freeware – Nmap is available free on the internet at http://www.insecure.org/nmap/nmap_download.html
- ✓ Compatible with many OSs – Nmap supports Windows, Linux, Open/Free/Net/BSD, Macintosh, Solaris, HP-UX
- ✓ Scalable – Nmap can apply ping sweeps, perform port scans, and sketch out networks who are behind firewalls all in one tool. (6)

Nessus – An intense security-auditing tool that looks for numerous security holes in a network.

Nessus FYI:

- ✓ Freeware – Available on the Internet at http://www.nessus.org/

© SANS Institute 2000 - 2005 Author retains full rights.

- ✓ Uses client-server architecture in which the daemon (Nessusd) runs on a UNIX-based machine and the client portion that provides the user interface could run on a Unix or Windows-based operating system.

- ✓ Very Scalable – Nessus gives you the right to their source code and you can create external plug-ins to suit your scanning needs. Nessus has the ability to search against many exploitable families that have been grouped together such as the category of "gain root remotely."(5)

Network Supervisor by 3Com – A very powerful SNMP based network-management tool used to map out IP-connected devices in a graphical, easy-to-use format.

Advantages of Network Supervisor:

- ✓ Shareware: Available at 3com.com. To extend use beyond 60 days, you may register online for a permanent license key.
  http://www.3com.com/

- ✓ Scalability: Network Supervisor can support over 2000 IP-connected network devices.

- ✓ User Friendly: NS comes with a nice graphical interface that allows testers to easily view what is going on of the network in question.

- ✓ Presents a network map either grouped by IP subnet or as a flat Layer 2 view of the entire network.

- ✓ Users may specify what subnet to look for and the ability to discover boundaries in a network on various ports. (1)

On What Level Will the Penetration Test Try to Expose Vulnerabilities?

This concept addresses the level of sophistication of the attacker modeled by the testing team. Hackers are usually grouped into three levels of sophistication:

- ✓ Sport intruder: Usually broken down into subcategories of "novice" (a single-machine attacker), "crackers" (multiple machine attackers who write their own cracking tools), and "apprentices" (usually taught by a hacker and use freeware off the Internet until they are up to writing their own tools).

- ✓ Competitive Intelligence: These hackers are usually just trying to gain insight into the capabilities of a competitor. They might also employ a "packet sniffer" to monitor traffic from a destination IP address in top management or

© SANS Institute 2000 - 2005, Author retains full rights.

corporate marketing.

- ✓ Foreign Intelligence: Such attackers attempt to gain information that will be used by a foreign country or international terrorist organization. For instance, Osama bin Laden's top security officer might attempt to create a back door into a company that is a vendor of security or weapons systems to the United States government.

Most tiger teams or penetration testers do not go beyond a low- or mid-level technique to exploit vulnerabilities. It is very uncommon that a penetration testing team can emulate hacker skills of all levels during a predefined period. (11,3,9)

Categories of Vulnerability

- ✓ OS specific bugs, exploits, vulnerabilities and security holes
- ✓ Weaknesses in firewall and routers among different brands
- ✓ Exploitations of web-server scripts
- ✓ Exploitable shares and trusts between systems and files

What Type of Reports Should You Get and What Should They Tell You?

The obvious answer to this question should be something of this nature. "We, XYZ Testing Company, have conclusive evidence that Company ABC is vulnerable to an attack of this specific nature," or, "We, XYZ Testing Company, conclude that Company ABC is not subject to an attack of a known exploitation or vulnerability." On the other hand, management should realize that if the testing company does not find that the target network is free of known vulnerabilities it is not free from risk. New advisories are posted everyday by the manufacturers of operating systems and also security organizations like CERT and SANS. (3)

Where Will Their Findings Be Stored?

Management should determine that the testing organization is itself secure, and that both findings and proprietary information will be safely stored. It should not be stored on active hard drives, but should be on separate media (floppy disks or CDs, for example) in a tamper-proof safe. (10)

How Much Should It Cost?

© SANS Institute 2000 - 2005, Author retains full rights.

Cost is a big factor when determining which penetration testing team to use. However, remember the old saying, "You get what you pay for." In most cases it's like choosing a Checkpoint firewall over a Cisco brand when Cisco is leading the industry in data communication technology and is rich in research and development. The cost of testing should be based on the number of devices being audited and how much auditing is going to be performed on those devices. The best advice would be to meet with several vendors, review their backgrounds, and choose the one that best suits the target company's needs within realistic budgetary constraints. (3,9)

After the Test

After the audit is over, inspect the target company's logs for IP addresses originating from the testing company's address range. They could be having fun with proprietary information gained from the target company. Check firewall reports, failed dialup attempts, and IDS logs for clues that the testing company is still connecting to the target network. If they accessed any host or computer in the target domain, be sure to look for backdoors and Trojan horses using freeware such as Nessus. If you trust them after the test is over, bring them back in after all corrections are made and let them re-evaluate the network. (3)

In-house Vs Third Party

Now there's the question of, "Why should I outsource it when there are so many risks?" A highly regarded in-house security department should always have an intrusion-detection specialist who can perform all or most of the functions that could be performed by a third-party vendor. Training personnel in auditing methods is the best way to stay ahead of the game. Such trained in-house staff will already know how the network operates and what services are running. Why not just send them to school for auditing training two to three times a year? The risks associated with third party exposures would decrease and so would the cost of outsourcing to a third party. Not all will agree with me on this but in most ways it is true. However if there is any doubt as to the knowledge and skill of your security personnel then outsourcing will be your best option. (3)

Conclusion

The intention of this paper was to prepare those who have to make a decision regarding outsourcing penetration testing. Managers can prepare for this decision in many ways, but the final decision usually boils down to managing risks. Please take the time and make a wise decision before allowing a complete stranger to take over your company's network.

© SANS Institute 2000 - 2005, Author retains full rights.

The Third Party Checklist

© SANS Institute 2000 - 2005, Author retains full rig

- ✓ Assess the risk = Threat x Vulnerability
- ✓ Find vendors that ask to see the company's security policy before they make any recommendations.
- ✓ Use an established and well-known firm.
- ✓ Deploy a fake honey pot and see if they can detect it.
- ✓ Ask about types of tools used and what operating systems they are used on and how many.
- ✓ Do they ask for a cutout?
- ✓ Get references, no matter what.
- ✓ Get the proposal in writing.
- ✓ What other services do they promise? (follow-ups etc.)
- ✓ Ask to see their certification.
- ✓ Do they use the bait and switch technique?
- ✓ Do they employ hackers?
- ✓ Meet with the forensic engineers one on one.
- ✓ Ask for a security clearance.
- ✓ Ask them where will the data be stored after the test is over and for how long.
- ✓ Be there on site all the time!
- ✓ Run a background check on them yourself if there is any doubt.
- ✓ Get what you pay for.
- ✓ Perform follow up checks on their IP address range destined to your network.

© SANS Institute 2000 - 2005

Author retains full rights.

References:

1. 3Com Professional Services "3Com Network Supervisor Integration" URL: http://www.3com.com/products/en_US/prof_services/infra_solutions/integration/network_supervisor.html

2. Esec Consulting Services "Penetration Testing Services," May 2001. URL: http://www.esec.com.au/ecs/images/pentest_may01.pdf

3. Kevin Glass. Information Security Manager, Colonial BancGroup. Personal Interview. 3 Jan 2001.

4. Mathew Schwartz. "Trust but Verify", February 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57532,00.html

5. "Nessus". January 2001. URL: http://www.nessus.org/intro.html

6. "Nmap" January 2001. URL: http://www.insecure.org/nmap/

7. Perri Wilbert. "Getting Serious About Security", October 2001. URL: http://security.kingsley.co.za/articles/article3.htm

8. Philip Moyer "Penetration Testing: Issues for Management," March 1998. URL: http://www.hyperon.com/papers/pen-tst.pdf

9. Shane Robinson. MCSE, Georgia Core of Engineers. Personal Interview. 21 Jan 2001.

10. Thomas Rude "Knock'n At Your Door", October 2000. URL: http://www.crazytrain.com/penetration.html

11. "What to Demand from Penetration Testers," March 1998. URL: http://www.gocsi.com/penet.htm

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.