Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Penetration Testing: The Third Party Hacker

Is my organization or infrastructure susceptible to compromise by a malicious attacker, unethical competitor or foreign government?" Both security consulting companies and Big Four audit companies have been trying to answer this question by offering penetration testing services to their clients in the last decades. This kind of specialized testing is a method for evaluating the security of an organization's information systems by simulating an attack. Its objective is to probe and identify security weaknesses in inform...

Copyright SANS Institute
Author Retains Full Rights

AD

Penetration Testing - "The Third Party Hacker"

"Is my organization or infrastructure susceptible to compromise by a malicious attacker, unethical competitor or foreign government?" Both security consulting companies and Big Four audit companies have been trying to answer this question by offering penetration testing services to their clients in the last decades. This kind of specialized testing is a method for evaluating the security of an organization's information systems by simulating an attack. Its objective is to probe and identify security weaknesses in information systems, such as an online banking application, the supporting network infrastructure, or even the physical premises of an organization. Companies expect third-party organizations that perform penetration testing to be truthful with them, but this has proven not to be the case in many instances. This paper is intended to help managers decide on a penetration testing firm by providing them with some essential points of attention and critical questions to ask the prospective service providers.

Because maintaining the security of information systems is important in any company, many are undertaking tests of the ability of outsiders to penetrate those systems utilizing third parties. Such tests, however, carry their own risks, and both the organization and the public should understand these risks. Any organization scheduling a third-party penetration test against a production system should understand the serious issues surrounding the decision and should 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.

Risk = Threat x Vulnerability

But first, for purposes of this analysis, it will be helpful to discuss why companies choose to outsource penetration testing to an external company:

- To determine the extent of vulnerabilities not detected through in-house audits
- To provide customers with third-party assurance of the security of online transactions, storage of company information, …
- To ensure these critical tests are performed by experienced and skilled auditors and because no such competencies are available within the company
- To test the adequacy of their incident management procedures and/or incident handling team
- Because it is not cost-effective to train or acquire skilled penetration testers

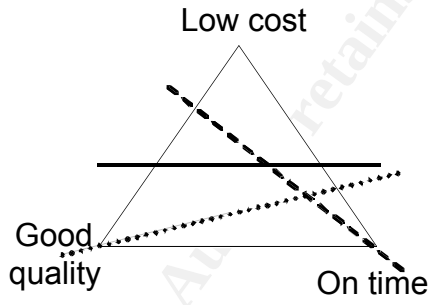
Below, a list of common threats of outsourcing penetration testing is provided. During the evaluation of service providers, a company should try to detect potential

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

vulnerabilities associated with these threats which could pose a risk for their organization:

- The service provider discloses, abuses or loses sensitive information obtained during the penetration test
- The service provider misses several vulnerabilities or weaknesses residing at the target
- The service provider impacts the availability of the target

As with any service, there are expensive, cheap, low-quality companies… but the hardest thing is to find a service provider which provides high-quality service within the planned time and for a reasonable price. The classic trade-off triad Cost, Quality and Timeliness applies.



A penetration testing service provider should not only be skilled, but should also be able to manage a project and to report in a non-technical way to a company's management. The attention points in the next sections are therefore organized in three distinct domains: project management, competence and reporting. It is recommended to verify each of these points when evaluating third-party vendors.

Project Management

- *Are the objectives and scope well-defined?*

  Before the service provider can make an adequate proposal, the scope and objectives should be clearly defined. If not, the service provider should request the company to provide the objective and the scope of the penetration test to create a proposal which can fulfil the requirements. To really emulate a hacker, a penetration test with full blown scope should be performed including social engineering. Limiting the scope to a single system or application can for example prevent the identification of vulnerabilities in trust relationships between the target and other (out of scope) systems or an end-user revealing his password by social engineering attacks.

  In addition, the objectives within this scope should include the level of testing required: does the provider just have to indicate that an information system is

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

vulnerable, or should he actively exploit it to demonstrate his observation? And if the second option is preferred, does that include vulnerabilities which can have an impact on the availability of the information system such as Denial-of-Service attacks? A well-defined scope and objective will ensure that there is no misunderstanding between the expectations and the service delivered by the third-party.

- *Does the third party provide a proposed planning and time table for the different phases in the test?*

  The execution of a penetration test should be performed based on a previously defined or communicated time table. This may include certain restrictions, such as only testing vulnerabilities with high impact outside the office hours. One could require that all testing be done during the normal business hours to test performance when under attack. Make sure the service provider proposes a schedule and check if it sticks to this schedule.

- *Is the provider prepared to sign a Non-Disclosure Agreement?*

  During a penetration test, sensitive information may be disclosed to the third party. This information can include infrastructure details, critical client information, trade secrets, and personal information of employees. Unintended disclosure of this information could have an impact on the company's image. Or worse: if the information comes in the hands of a malicious person, it can be abused for a more focused attack.

- *Does the third party use a documented methodology?*

  It is important to not hire "reckless" penetration testers who cannot provide a detailed testing approach. The third party should have its own, documented penetration testing methodology or make use of a commonly accepted methodology such as the Open Source Security Testing Methodology (OSSTMM).

- *Does the provider have a Single Point of Contact for emergencies?*

  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 and provides a single point of contact. Both persons 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. The SPOC at the client side must have the authority to intervene during the test, both to save engineers time if questions arise as well as to stop an event from occurring if it in itself poses an unacceptable risk to the company.

- *Does the service provider have liability insurance to cover themselves?*

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

All penetration testing service providers 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. If the service provider does not have a liability insurance, pay attention how they specify the liability in their 'Terms and Conditions'. Management must also assure that it 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.

Competence

- *Does the third party provide an overview of the proposed team and their details?*

  The service provider should provide an overview of the team which will perform the penetration test. Details about the team members should be requested. Of particular interest should be any relevant certifications such as GIAC Certified Incident Handler (GCIH), Certified Ethical Hacker (CEH), OSSTMM Professional Security Tester (OPST)… While these certifications do not guarantee quality, they do provide a certain level of assurance that the penetration tester has been trained for this type of engagements. Also beware that the service provider does not propose skilled team members in their offer, and subsequently have the project executed by unskilled trainees. It is very difficult to find this out before the project starts, but it can be verified after the engagement by thoroughly questioning the service provider about their findings and their steps taken to conclude on these observations.

- *Does the provider allow a company representative to be present?*

  To be able to witness the actual functioning of the team carrying out the penetration test, the company might want to have a representative attend on-site. A service provider that has nothing to hide, should have no problem allowing this presence.

- *Does the service provider provide relevant references?*

  When evaluating penetration testing organizations, it is good practice to ask for references from previous clients. It is possible that the service provider will not honour this request because of confidentiality agreements with its other clients. Management should then request that the testing company provide a list of clients who have given their explicit permission to be used as references. If possible, do contact these references to hear about their experiences with the service provider.

- *Can the service provider respond 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

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

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.

Reporting

- *Can the service provider provide anonymous example deliverables?*

  By requesting an example deliverable, it is possible to verify the reporting quality of the service provider. Good reports generally include a well-founded and non-technical executive summary, technical details of the identified vulnerabilities including reference screenshots, a basic risk assessment, and a full detail of the actions taken during the penetration test.

- *Does the service provider keep logs and traces of all actions taken during the penetration test?*

  To ensure accountability of the actions taken during a penetration test and to be able to prove these actions, the service provider should log and trace every packet sent to the target during the test. These log files can become as big as several gigabytes, but this is the only way to verify their actions. Copies of them should be handed over to the company that was tested.

- *How will the service provider archive information obtained during the project?*

  Ask the service provider how and where they archive information obtained during a penetration test. Do they encrypt all information on CD/DVD or lock it away in a secure facility? Or do they keep the client files on a shared network drive? To ensure confidentiality of this information, a service provider should be required to only securely save this type of sensitive information and to remove/protect all insecurely stored engagement information.

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 the company's network.

© SANS Institute 2006, As part of the Information Security Reading Room Author retains full rights.

Acknowledgement
This paper was originally written by Jessica Lowery in 2002 for SANS Institute. It was partially reworked and rewritten by Pieter Danhieux and Wouter Clarie in 2006 with permission from the author.

© SANS Institute 2006, Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**