Best Practices for Hiring Penetration Testing Services

Nathan W. Dickens

East Carolina University

July 21, 2014

Abstract

The following paper will be exploring the best practices for a company looking into hiring a service provider that offers penetration testing. A brief overview will be explored for individuals who are unfamiliar with what exactly penetration testing is. The importance of penetration testing will be presented in order to give the reader a basis for justifying the reasoning behind pursuing a service provider's offerings. The majority of the paper will be dealing with the best practices for evaluating an appropriate service provider to meet the needs of the hiring company. Certain areas will be explored such as the reputation, credibility and follow-through of the provider after the test results in order to give the customer a complete job. Procedures for the company will also be explained, as to provide them with enough information prior to going into the evaluation process. By the end the reader should be knowledgeable enough to handle working with a service provider and getting all the details necessary to successfully hire a penetration testing service provider.

Best Practices for Hiring Penetration Testing Services

In this day and age, most people would feel pretty confident in purchasing a vehicle and believing they can get a security system on it to prevent car theft. Naturally you would hope the security company designed it from a thief's point-of-view in order to prevent or deter the assailant from completing their job (such as the fuel injector shutting off without proper key codes or an alarm going off to alert the presence of the thief). However, when looking at something at face value, you can't really tell if everything is 100% guaranteed to do its job without testing it first.

This goes the same way in the Information Security world; where companies believe they can just put a few firewalls in place and become 100% secure, when in reality they may be rattled with vulnerabilities that they are unaware of. This is how the art of penetration testing is born. Throughout this paper, we are going to explain some of the best practices that a company can utilize to hire in-house or outsourced companies to penetrate their Internet infrastructure to eliminate these vulnerabilities. We will briefly go over an explanation of what penetration testing is and how it's useful to a company's information security needs. We will then cover the many variables that are available for companies to rate businesses who offer these services. This way companies can get their needs met without wasting time or money in the process.

What is Penetration Testing?

To be able to analyze the situation a company is in, we need to first be familiar with what penetration testing actually is. A penetration test is using attacking methods by trusted

individuals that would be similar to attackers or hackers. These types of tests range anywhere from small port scan or IP scans of machines that are unwillingly offering backdoors into your environment; to full-blown intrusion detection of your business infrastructure. However, some companies can be fooled into believing that this type of testing is a security audit of their system when it's not. ("Everything you need," 2014) Understanding the scope of the test is all a part of the process, which will be discussed later on as a focal point in selecting your service provider. Keep in mind that most of these tests that are conducted are not meant to be a onetime event as you are only testing for what is currently vulnerable in your system. Once these misconfigurations are resolved, there an entirely different situation or vulnerability may occur if you are frequently making environmental changes. To summarize, Northcutt et al. (2006) described penetration testing as the following:

> "Penetration testing is the process of attempting to gain access to resources without knowledge of user-names, passwords and other normal means of access. The main thing that separates a penetration tester from an attacker is permission. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report."

Now that one has an understanding of what a penetration test is, we next need to discover the reasoning behind why one should perform a penetration test in the first place. This can be a compelling question for both large and small companies. Take into consideration some of the situations below as to why performing penetration testing on a company's infrastructure is needed. (Bing et al., 2008)

Important Factors When Considering Penetration Testing

Data Breaches

Depending on the type of industry, a data breach can be incredibly unfortunate. Not only could this hurt you in the backend on revenue but this could also deteriorate one's reputation. Using a bank as an example, one would want to make sure that no customer records are being stolen or that there is no tampering with funds within accounts themselves. For a manufacturing business, one would not want company secrets to be stolen with which one could easily lose the competitive edge in the market place. By testing the infrastructure, you can not only prevent these types of breaches, but it would also be a good learning lesson for your team to be able to react accordingly in the event of a real attack. By simulating the situation, valuable time will be saved later when it's needed the most. ("Pen Testing," 2014)

Baseline for Security Programs and Checking Security Controls

For new companies and especially for CISO's, they will need to have a firm handling on what their team is capable of and also how effective their security program is to the company. By performing a penetration test, they will be able to create a foundation for the company to work upon when refining their IT security program. For some legacy companies who are trying to retrofit their current set of protocols and rules, they will find this type of test valuable to being able to adjust into the information security market with a strong team behind them. (Wai, 2002)

Many companies believe that their networks are secured as they have implemented all the common preventive measures in place. These can be appliances such as firewalls or intrusion detection prevention systems. Some companies have in house teams that set up this equipment or maybe they were provided by a service from an external partner. From the outside looking in, it can be a different story though. The configurations may seem sound, but as infrastructure grows, so does the possibility of misconfigurations which can lead to vulnerabilities. A penetration test will put those defenses to the test and really fleshes out any loose gaps that may surface without a team's knowledge. (Northcutt et al., 2006)

New Application Security

For a small company, rolling out a new application may not seem to be a big deal, but in a large organization, this may happen without the knowledge of all IT departments. This type of situation can cause a huge problem down the road when gone unchecked. For example, if a piece of software is meant to collect customer data and pool it into a SQL database, what if that port is accidently left open to the outside world? This type of opening is a honeypot for attacks and can cause a potential data breach which can affect the company in the long run. Even over-the-counter commercial software can have potential vulnerabilities when not properly patched, which can happen as sometimes causing downtime to do patch management is costly to most companies. Some companies would rather leave the older versions of the software running than taking the time to update it, as it would decrease productivity. A penetration test would surface these vulnerabilities and be able to show in a report of how much more it would cost to leave it wide open as it is.

Verifying Compliance and Security Staff Training

Depending on the type of business a company deals with, one may or may not have to deal with being compliance to a particular standard. The financial industry has to maintain a bevy of different standards in order to stay in business. One in particular is the PCI DSS (Payment Card Industry Data Security Standard), which actually requires penetration testing to be performed. This standard is in place in order to reassure the customer that their data is well protected from attackers who are looking to steal their identities or information. One would need to understand how and what scope of a penetration test to be performed in order to meet the audit and obtain your certification.

Training a staff to be able to react to only mock scenarios and "what-ifs" can lead to a team that's not ready and unprepared when the real situation happens. Being able to perform a penetration test on your infrastructure can help inform staff members on how to properly monitor for future vulnerabilities in the environment and also how to apply those skills to respond to incidents as they occur. As we have discussed several reasons as to why to perform a penetration test, we will need to now look at what to look for in a penetration testing service provider in order for a company to get their needs fulfilled without wasting money or time in the process. (Northcutt et al, 2006)

Getting the Right Service Provider

Hire the Right Company

Hiring the right company is probably the most obvious goal one would have in mind

when wanting to get a company for penetration testing, but it also is the most important. If you were attempting to have your transmission rebuilt in your car, you would not take your car to just any old car shop. You would want to make sure that they have an experienced technician on site that has plethora of experience under their belt. This goes the same for the Information Security world. When first selecting out a company, it is important to do research first about the company. This way you is not going in blind when speaking with them. ("Choosing, Managing," 2014) Make sure you asking the correct questions and look at their portfolio of jobs they have completed. A reputable service provider will be able to provide a detailed structure of how they will come up with a test plan, rules of engagement and also how they will report their findings back to you in an understandable format. A few good questions you may want to bring to the table when you go would be:

- A timeline structure that would be required to complete the job
- Are they able to perform physical penetration testing as well?
- What types of testing time frame is preferred and would they be able to commit?
- Do they have issues with handling systems are they are out of date and delicate?
- What type of methods and procedures are performed? (manual or automated)
- Will this affect production while the tests are performed? (degradation of operations) (Stanislav, 2014)

One good method is also checking with the companies' compliance team to see how they are accredited to be able to perform these tests. There are various certifications out there that prove their knowledge and ability to perform the work. One particular certification is the GPEN by GIAC (Global Information Assurance Certification). They describe their certification as follows;

> "The GPEN certification is for security personnel whose job duties involve assessing target networks and systems to find security vulnerabilities. Certification objectives include penetration-testing methodologies, the legal issues surrounding penetration testing and how to properly conduct a penetration test as well as best practice technical and non-technical techniques specific to conduct a penetration test." ("GIAC Penetration," 2014)

There are also other certifications that will help with any concerns and they are the ISO 270001 and OSEE (Offensive Security Exploitation Expert).

Scope of the Test

This is where attention to detail is a must as this can cause a waste of not only time but also company money. While working with the service provider, a company will need to define what the actual scope of the test will be. Look at what your company is trying to accomplish from the test and this will help the consulting company come up with an approach that is effective and also beneficial for future tests. With external testing of the company infrastructure, especially networking, you are going to want to define IP addresses ranges, external URLS and also any applications that may be used for internal and externally by the company. The service provider will then able to focus on the core of your system or the particular part you are concerned about. If you are looking to do a physical penetration of the buildings infrastructure, you will want to provide all the possible entrances and exit of the buildings, as well as any parts of the facility that could be used for removing or placing equipment such as dumpsters / loading docks / roof hatch access). (Basu, 2013)

By defining these particular outlets, you will keep the service provider from accidental tampering with another company's property or with unwanted access to internet infrastructure

that could lead to a unwanted breach. The scope will also help define how much the overall test is going to cost, as capital is being spent, you want to make sure you are getting your money's worth. When looking at cost, don't always go with the cheapest, as you may get what you're paying for in the long run. Penetration tests can run anywhere from hundreds of dollars to tens of thousands. This is mostly based on scope, so this is why it's very important to narrow down your testing perimeters. (Basu, 2013)

Testing Methods

When looking at a company, you will want to inquire on how they perform their tests and what methods they utilize. There are tons of over-the-counter software that can be used but what you need to know is will they be doing a black-box test or a white-box test of your environment or a combination of both (gray-box test). All of them have their advantages and disadvantages.

Black-Box Testing. This particular technique is a test that will be performed without having any knowledge of a company's infrastructure. The tester will be clueless of the actual architecture at which they are attempting to breach and thus a larger number of decently skilled testers could perform this method with no knowledge of programming language or Operating Systems. However there are some disadvantages to utilizing this particular method and the primary one being that it can be inefficient for the scope of the test. Without having any plan to work with, time could be spent incorrectly in areas that are not as vulnerable thereby wasting company money. For the most part, these can be hard for a consultant to design since the knowledge is not there. On the positive side, this method can also lead to

certain aspects of the company environment that an attack would have to come up with from scratch. Thus giving the company a more real world approach to how hackers have to work with almost nothing to get the job done. (Basu, 2013)

White-Box Testing. This method is almost the polar opposite of black-box as the tester is given all the information they need about the network and infrastructure to perform the penetration. Generally the company will provide login information and source code of the software they are attempting to uncover vulnerabilities in. This has some distinct advantages that are inherited and one of which is time and money spent appropriately. The tester will be able to spend more time on breaking the applications and network infrastructure rather than trying to collect and discover resources like a black-box test would have to. This will also show how the threat of an attack is indeed great from the outside but also how dangerous people inside the company can be as well; especially ones who have access that goes unchecked for long periods of time. Though there are a few disadvantages, most are related to cost. Because the perimeters of the project might be defined, it could demand particular expertise could increase the cost of the test. Although you could say that is somewhat of an advantage to a black-box, where a tester is wasting time and money, but it's somewhat of a double-edged sword at times. One other disadvantage of this type of method is maintaining the tools needed to perform these tests. As generally these can be specialized at times, it requires updated software to perform at its best to give the best possible results. (Basu, 2013)

Grey-Box Testing. This method is somewhat of a mixture of the black and white box testing methods. A tester will be given limited knowledge of the company's infrastructure in

order to complete the job. For example, the company may say their internal websites are operations.abccompany.com but not hand over the actual login credentials to that website for them to get in. So basically you can absorb some of the advantages of both black and white box testing. Tests are generally done from the point of view of a user and not the designer of the application or network. There are still disadvantages and one could be the fact that the tests could already be redundant to ones that the designed already performed. Thus wasting the time and money you spent upon the test. (Omar, Ibrahim, 2010)

Schedule Properly and Reduce Impact

Once you have selected a penetration testing company and figured out what method of testing you require, now you need to figure out when the best time to perform the test on your system will be. This can be a critical step as using the wrong time could cause degradation in your networks performance or potentially leave your company vulnerable for other attackers to get in. Let's look at network performance for an example. If you were a manufacturing company and ran several production lines, you would not want to run a test during peak production, as the time of investigation could cause network performance to drop; thus creating delays in computing systems supplying vital information to your lines to bottleneck. This essentially results in you attacking and hurting your own company without the intending to. This could also be true for online e-commerce sites that are doing penetration testing for vulnerabilities in their payment collection system or customer SQL database archiving. You will want to plan out the most appropriate time to perform these tests without impacting your own business. (Basu, 2013)

Some companies may want to test certain parts of their network during high volume to test for capacity overloading from such attacks like DDoS (Distributed Denial of Service). However, you would want to isolate that type of attack away from any other parts of your company that you would not want to be affected. This is critical to the design process and generally the service provider will offer suggestions as it will depend on the scale of the test. (Turpe, Eichler, 2009)

Reporting Structure

Reporting structure is what comes after your tests are done and how you will be able to determine what to do next. A company should be able to show you a template of sorts for you to be able to clearly define your goals and objectives of the test being performed. When having to report this information back to executives or upper management, you are going to want an understandable format. Also, make sure that when you are stating your goals to the service provider that you realize that not all goals may be met during the test. This doesn't necessarily mean it's a bad thing it just means that the scope of the test was too large for the particular time frame. The main focus of the report should be to reflect to show that the highest vulnerabilities are brought to the foremost attention and that other low impacting ones can be also be addressed but prioritized. They may also offer recommendations for future tests and scope that will help set up a baseline. (Northcutt et al, 2006)

Recommendations

The last good measure to take is to check with your colleagues and peers at other companies who have had similar experiences with service providers. Reputation carries a lot of weight at any company. If you have networked with tons of companies, use those assets at your disposal. They may be able to share valuable advice that at first you may have never thought of. While hindsight is sometimes a good thing, going into the situation better prepared is a life saver. Some service providers may have testimonies and those individuals may be willing to speak with your company within certain situations to describe their ordeal with them. (Basu, 2013)

Conclusion

A penetration test may not be for every company, but it certainly is incredibly important to the industry as a whole. Companies who are looking to avoid data breaches, network instability due to attacks and potential revenue loss, have to fully understand the areas at which a service provider can help. By looking at the several factors we discussed, a company should be able to confidently hire the right talent for the right job. We just have to keep in mind that just because you performed a penetration test today and found 10 holes in your network, it doesn't mean a hacker tomorrow will not find a 11^{th} one.

References

Basu, E. (2013, October 13). What Is A Penetration Test And Why Would I Need One For My Company?. *Forbes*. Retrieved July 6, 2014, from http://www.forbes.com/sites/ericbasu/2013/10/13/what-is-a-penetration-test-and-why-would-i-need-one-for-my-company/

* Bing Duan; Yinqian Zhang; Dawu Gu, "An Easy-to-Deploy Penetration Testing Platform," *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for* , vol., no., pp.2314,2318, 18-21 Nov. 2008 doi: 10.1109/ICYCS.2008.335 or URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4709333&isnumber=4708921

Choosing, Managing, And Evaluating A Penetration Testing Service. (n.d.). *Dark Reading*. Retrieved July 10, 2014, from http://www.darkreading.com/choosing-managing-and-evaluating-a-penetration-testing-service/d/d-id/1140511?

Everything you need to know about Penetration Testing. (n.d.). *Everything you need to know about Penetration Testing*. Retrieved July 12, 2014, from http://www.penetration-testing.com/penetration-testing-guide.html

GIAC Penetration. (n.d.). *Penetration Testing*. Retrieved July 16, 2014, from http://www.giac.org/certification/penetration-tester-gpen

* Geer, D.; Harthorne, J., "Penetration testing: a duet," *Computer Security Applications Conference, 2002. Proceedings. 18th Annual* , vol., no., pp.185,195, 2002 doi: 10.1109/CSAC.2002.1176290 or URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1176290&isnumber=26404

Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R., & Mancini, S. (2006, June 1). Penetration Testing: Assessing Your Overall Security Before Attackers Do. . Retrieved July 16, 2014, from

https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Pen Testing: Making Passion A Priority. (n.d.). *Dark Reading*. Retrieved July 15, 2014, from http://www.darkreading.com/pen-testing-making-passion-a-priority/d/d-id/1140580

* Omar, F.; Ibrahim, S., "Designing Test Coverage for Grey Box Analysis," Quality Software (QSIC), 2010 10th International Conference on , vol., no., pp.353,356, 14-15 July 2010 doi: 10.1109/QSIC.2010.44 or URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5562984&isnumber=5562921

Stanislav, M. (Director) (2013, April 20). So You Want to Hire a Penetration Tester?. Lecture conducted from Uncompiled.com, .

* Turpe, S.; Eichler, J., "Testing Production Systems Safely: Common Precautions in Penetration Testing," *Testing: Academic and Industrial Conference - Practice and Research Techniques, 2009. TAIC PART '09.* , vol., no., pp.205,209, 4-6 Sept. 2009 doi: 10.1109/TAICPART.2009.17 or URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5381625&isnumber=5381544

Whitepaper. (n.d.). *What Is Penetration Testing? An Intro for IT Managers*. Retrieved July 23, 2014, from https://information.rapid7.com/what-is-penetration-testing-whitepaper.html?LS=1138726

Wai, C. (2002, January 1). Conducting a Penetration Test on an Organization. . Retrieved July 14, 2014, from http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67