How To Choose the Right Vendor

Information you need to select the IT Security Testing vendor that is right for you.

Netragard, Inc
Main: 617-934-0269
Email: sales@netragard.com
Website: http://www.netragard.com
Blog: http://pentest.netragard.com
How To Choose the Right Vendor

Feedback Request
This document was created to help prospective customers select an IT Security Testing vendor that is right for them. If you would like to see additional topics covered in this document that are not already included, please submit a request to sales@netragard.com.

Introduction
A definition is the exact meaning of a word. Therefore, there can be only one correct definition for specific terms. Despite this, most vendors define their services differently and often times incorrectly. This is problematic because it causes confusion among prospective buyers, which makes the process of purchasing services exceedingly difficult by affecting the buyer’s understanding of what they are purchasing.

High-quality IT Security Testing vendors do exist but are hard to identify. Most vendors appear to offer identical services when in fact their services are very different. This document is designed to arm prospective buyers with the information that they need to clearly understand and select the vendor that’s best for them. This is important because there is a significant difference between passing any test and passing a high-quality test.

This document contains three primary sections, each of which provides high-level coverage of important topics. The first section provides clear, accurate, dictionary based definitions for terms that have been tarnished by the IT Security Testing industry. These terms are Penetration Test, Vulnerability Assessment, Vulnerability Research and Vulnerability Scanning.

The next section of this document covers project scoping and pricing methodologies. Specifically, it is possible to evaluate a vendor based on their traits and scoping methodologies. For example, a high quality vendor will typically measure the attack surface in order to create an accurate proposal. Other vendors will build a proposal based on the count of targets to be tested. Engagements that are scoped by count alone are often dependent on automation and therefore lower quality.

The final section of this document contains vendor qualification questions. These questions are designed to help evaluate and understand the technical capabilities of any given vendor. This is important because many vendors will talk a good talk but don’t walk the walk.

Finally, there are cases where customers are more interested in passing a test than they are in receiving high-quality services. This document isn’t geared towards those customers. This document is geared towards customers who understand the need for quality security testing services.

Correct Definitions
The following section defines common service types that are offered by IT Security Testing Vendors. The definitions that we provide are based on the US English dictionary. It is important that service types are defined properly as definitions also create boundaries through meaning. Many vendors use incorrect terminology when selling and even delivering services. This is problematic, especially with services that carry as much potential risk as offensive security testing services.
Penetration Testing (High Quality)
The term “Penetration Test” as defined by the English dictionary, means to identify the presence of points where something can find or force its way into or through something else. Penetration Testing is not unique to IT Security and is used in a wide range of other industries that include but are not limited to soil penetration testing, armor penetration testing, chemical penetration testing, etc. When applied to IT Security Penetration Testing is most often used to positively identify points of vulnerability.

Since Penetration Tests are tests, they must determine the genuineness of the vulnerabilities that they identify, hence the word “test”. In most, if not all cases this determination is done through exploitation. If a potential issue is successfully exploited then it is determined to be a genuine vulnerability and is reported. Findings that cannot be exploited are either not reported or are reported as theoretical findings when justified. Because Penetration Tests prove the genuineness of vulnerabilities their deliverables should always be free of false positives.

Penetration Test Limitations
The term Penetration Test does not impose any limitations on the methods that can be used to determine the presence of points where something can make its way into or through something else. When limitations are imposed they are the product of customer requirements, project scope, team capabilities, and resources.

Penetration Test Threat Level and Quality
With regards to IT Security, a Penetration Test should produce levels of threat that are at least equal to those which are likely to be faced in the wild. This enables the testing team to identify the same types of vulnerabilities that might otherwise be identified by the real threat. Once those vulnerabilities are identified they can be remediated against thus preventing a compromise. Testing at less than realistic levels of threat is ineffective and akin to testing a bulletproof vest with a squirt gun instead of live rounds.

Note: The real threat commonly uses malware, social engineering and phishing (a form of social engineering) when attempting to penetrate targets.

Penetration Testing & Uses
In IT Security Penetration Tests are most commonly applied to Networks, Web Application, and Physical Security. In theory, anything can undergo a Penetration Test.
Vulnerability Assessments (Medium Quality)
The term “Vulnerability Assessment” as defined by the English dictionary is an estimate, or best guess, as to how susceptible something is to attack or damage. As with Penetration Testing, Vulnerability Assessments are not unique to IT Security. Unlike Penetration Tests, Vulnerability Assessments are restricted to “assessing” and so cannot exploit the vulnerabilities that they identify.

Vulnerability Assessment Limitations
The term Vulnerability Assessment imposes limitations with the word “assessment”. Because the service is an assessment it cannot exploit the vulnerabilities that it identifies. Some of the limitations include but are not limited to:

- Social Engineering cannot be performed in tandem with a Vulnerability Assessment. Social Engineering exploits human vulnerabilities and that exploitation crosses the boundaries of a Vulnerability Assessment.

- Vulnerability Assessments cannot be applied to running Web Applications. Testing a running Web Application requires the submission of malformed and/or augmented data. When the data is received by the application, if the application is vulnerable, then an error or unexpected result is returned. This error or unintended result constitutes a degree of exploitation and as such crosses the Vulnerability Assessment boundaries.

- Distributed Metastasis (also known as Pivoting) cannot be performed during a Vulnerability Assessment. This is because Pivoting depends on the attackers ability to exploit vulnerabilities as a method of propagating penetration.

Vulnerability Assessment Threat Level and Quality
With regards to IT Security, a Vulnerability Assessment produces a less than realistic level of threat and is generally a lower quality service. Vulnerability Assessment deliverables contain False Positives because Vulnerability Assessments cannot provide proof of vulnerability through exploitation. Instead, the findings presented in a Vulnerability Assessment report are the product of a best guess or estimate.

Vulnerability Assessment Uses
Vulnerability Assessments are ideal for performing quarterly checkups, source code reviews, configuration reviews, and other similar types of assessments. Vulnerability Assessments when applied properly are a good way to maintain strong security. In most cases Vulnerability Assessments do not provide the same degree of depth and coverage as Penetration Tests.
How To Choose the Right Vendor

Vulnerability Research (High Quality)
The term Vulnerability Research is best defined as the systematic investigation into and study of materials and sources in order to establish facts about how susceptible something is to attack or harm. In IT Security, Vulnerability Research often involves but is not limited to advanced source code reviews, reverse engineering, exploit development, etc. As vulnerabilities are identified methods for remediation can be created and implemented thus eliminating the vulnerabilities.

Vulnerability Research Limitations
Vulnerability Research is only limited by the project scope and the researchers overall capability. Finding a capable Vulnerability Researcher is difficult and rare. A good researcher will typically have a deep understanding of assembler for a wide variety of different architectures and will have extensive experience in reverse engineering technology. Most talented researchers will also be experts at exploit development and higher-level programming.

Vulnerability Research Threat Level and Quality
Vulnerability Research when applied to a threat bearing service produces the highest possible levels of threat. For example, when applied to Penetration Testing, Vulnerability Research almost always guarantees successful penetration. This is because a researcher is able to select a specific piece of technology, perform research against it and identify one or more vulnerabilities. Once a vulnerability is discovered the researcher can write a program called an exploit that is designed to take advantage of the vulnerability. In most cases, exploits allow attackers to take control of the affected system. Once a single system is compromised the researcher can then propagate his or her penetration through out the entire infrastructure.

Vulnerability Research Uses
Vulnerability Research can be used to augment services such as Penetration Testing and Web Application Penetration Testing, or it can be delivered as a stand-alone service. Often times Vulnerability Research is used to determine how secure or safe technology is for use. Other times it may be used to create programs that are designed to penetrate into systems by exploiting vulnerabilities. Vulnerability Research is at the core of system penetration, malware research, exploit development, etc. Netragard is often hired by software vendors to perform vulnerability research against their technology.
Automated Scanning

In most cases Automated Scanning refers to Vulnerability Scanning and is done by a computer program called a Vulnerability Scanner. Vulnerability Scanners rely on a set of rules (also known as signatures) that are made up of patterns that represent certain vulnerabilities. When a vulnerability scanner is running against a particular target its goal is to match patterns in the target with patterns in a rule. If there is a match then the vulnerability scanner assumes that a vulnerability has been identified and reports accordingly. Vulnerability scanners include but are not limited to Web Application Scanners, Network Scanners, Source Code Scanners, etc.

Automated Scanning Limitations

Automated Scanners are possibly the most limited in that they produce the lowest possible levels of threat. Automated Scanners produce a high degree of false positives and false negatives, which results in vulnerabilities either being falsely identified or not identified at all. Vulnerability scanners cannot detect vulnerabilities that they do not have pre-existing signatures for.

Automated Scanning Threat Level and Quality

The level of threat produced by Automated Scanners is minimal and far less than what is likely to be encountered in the wild. Automated Scanners are useful for augmenting specific security processes, but should never be relied on for security. The quality of the results produced by Automated Scanners is generally poor.

Automated Scanning Uses

Automated Scanners are useful in the hands of talented security professionals so long as the professionals do not rely on the scanner results alone. Automated Scanners cover a lot of ground very quickly and are often very useful for reconnaissance.
How To Choose the Right Vendor

Important Notes and Comments

- **The Terms Penetration and Vulnerability do not denote testing perspective.** Many vendors will inaccurately define a Penetration Test as an External test and a Vulnerability Assessment as an Internal Test when in fact the dictionary provides no definition of perspective for those words. Penetration Tests, Vulnerability Assessments, Web Application Penetration Tests and Vulnerability Scans can be delivered from either an Internal and/or External perspective.

- **A high quality Penetration Test must be delivered by a high quality testing team.** This team should be able to perform their own research, write their own code, understand how exploits work, and ideally be able write their own exploits if required. Most Penetration Testing teams do not have this level of expertise and rely heavily on third party tools and scanners. Yet the Penetration Testing companies that you are considering and ask them to provide you with proof of research. Proof of research includes but is not limited to 3 or more published advisories, 3 or more published research articles, 3 or more published exploits, etc. Also, check for exploits and materials on security websites such as http://www.packetstormsecurity.org. We recommend against using non-research capable testing vendors.

- **Penetration Tests should be the product of talent and experience, not the product of vetted Automated Scanner results.** Any service that is the product of vetted Automated Scanner results is likely to be a poor quality product.

- **Penetration Tests may include many or all of the methodologies that are used to deliver a Vulnerability Assessment, but they do not include Vulnerability Assessments.** The terms Vulnerability Assessment and Penetration Test define very specific boundaries, one cannot include the other.

- **The purpose of a Penetration Test is to identify vulnerabilities so that they can be remediated against before malicious hackers exploit them.** To do this successfully they must be able to identify the same types of vulnerabilities that malicious hackers might identify. As such, Penetration Tests must test at levels of threat that are at least equal to that which is produced by malicious hackers. Testing at less than realistic levels of threat is ineffective from a security perspective.

- **Not all tests are created equal and not all tests are effective.** If a bulletproof vest is tested with a squirt gun it will pass the test but likely be useless in a firefight. If a bulletproof vest passes a test with a Barrett .50 caliber sniper rifle then it will likely be very effective in a firefight. The same is true of Network and Web Application Penetration Testing. While passing a test might help you to be PCI compliant, if the test is low threat then you certainly won’t be secure.

- **Being compliant is a far cry from being secure but being secure usually results in compliance.** Regulatory requirements do not provide a method through which vendor quality can be measured (hence the goal of this paper). Most regulatory requirements, especially PCI can be satisfied with even the most basic, poor quality Network Penetration Test. This is problematic as regulatory requirements often inadvertently help to promote a false sense of security.
How To Choose the Right Vendor

How To Scope A Project
Different vendors scope engagements using different methodologies. Prospective customers can use a vendor’s scoping process as a tool to partially gauge the quality of the vendor’s services. All vendors will claim that their services are high quality but only a few vendors will actually live up to that claim. In this section we provide a high level overview of two pricing methodologies and provide insight into what they really mean.

Accurate Measured Attack Surface Pricing
If a vendor intends to deliver a service that is high quality, then the service must be the product of real expertise and must use a methodology that is driven by hands on testing. In order to price a service that is driven by hands on testing the vendor must have a solid understanding of the work time requirement. The only way to get that understanding is to perform a detailed assessment of the customers actual attack surface.

An attack surface is best defined as the sum of all potential attack vectors. An attack vector is any single parameter that can be attacked. A Web Application used to send email may have parameters that include “From”, “To”, “Subject” and “Message” but may also have hidden parameters that include “UserID”, “SessionCookie”, etc. Likewise network connected devices that offer services like FTP, IMAP, and SMTP also contain unique parameters. Each parameter requires a certain amount of time to test.

Parameter identification requires that the vendor perform a basic technical assessment as a part of the project scoping process. This technical assessment should identify all of the services being offered by all of the in-scope targets and should count the parameters for each particular service. The technical assessment should also consolidate groups of systems that are identical so that one system can represent many. This type of consolidation can result in significant cost savings.

Only after the attack surface has been properly measured is it possible to determine testing time requirements from which project cost can be derived. Any vendor that delivers services based on hands on manual testing must understand the customers attack surface in order to accurately price a project. A failure to assess the attack surface properly for a vendor that performs real manual testing can result in a project that runs financially negative.

Inaccurate Target-Count Pricing
A common and inaccurate pricing methodology is the target-count based methodology. This methodology usually sets a price per IP address for Network Penetration Tests or Network Vulnerability Assessment services. Alternatively, it sets a price per page or per click for Web Application Penetration Testing services. This methodology is faulty because it does not perform any assessment of the actual attack surface. This is problematic because it is impossible to accurately price a project without a solid understanding of work requirements.

Each network-connected device has an IP address that presents a measurable attack surface. Some devices might have an exceedingly complex attack surface while others an extraordinarily basic one. Pricing per IP address does not take these attack surfaces into account and instead sets a particular value to each IP address.

Suppose that a Network contains 3 devices and a vendor charges $500.00 per IP address. The cost of the engagement would be $1500.00. The industry average hourly rate for a moderately skilled Penetration Tester is $250.00 per hour. A price of $1500.00 would allow such a tester to deliver 6 hours of testing which equates to 2 hours per target.
How To Choose the Right Vendor

Now imagine that the targets that are in scope provide no services what so ever. This means that there would be no surface for the tester to work with and so no work would be done. The tester would simply generate a report that contained no findings and a note about the lacking attack surface. In such a scenario the customer will have paid $1500.00 for no work product.

Alternatively, suppose that each of the 3 targets requires 6 hours of testing due to somewhat complex attack surfaces. That equates to 18 hours of testing time plus 4 hours of reporting time which totals 22 hours of total work. If the project is priced at $1500.00 then the hourly rate for the tester is reduced to roughly $68, which is far below the industry standard and would likely run the project negative.

Despite the obvious problems with target-count pricing it is still the most widely used pricing methodology. Vendors avoid the negative financial burn that can result from an improperly scoped project with a heavy dependency on automation. Increased automation decreases work time requirements but also greatly decreases overall project quality.

Note: The same is true for Web Application Penetration Testing. It is possible to have a web application made up of a single page that presents an enormous attack surface. It is also possible to have a web application made up of hundreds of pages that contains a minimal attack surface. It is impossible to provide accurate project pricing for a Web Application Penetration Test without first measuring the Web Application’s attack surface.

As a general rule of thumb, if a vendor does not take the time to measure your attack surface then they don’t truly understand how much work needs to be done to complete the project. In such cases pricing is literally arbitrary.
How To Choose the Right Vendor

Proposal Evaluation and Selection
A business proposal is a written offer from a seller to a buyer. Its job is to clearly define the services that are being proposed, their respective boundaries and pricing. A well-written business proposal will contain clear details about the work to be done, the vendors understanding of the problem statement (the need), and the final deliverable. A well-written business proposal will not contradict its self nor will it contain conflicting terms. Below are some areas to pay close attention to:

Stick to the boundaries
Many IT Security Testing vendors create proposals that are both unclear and contradictory. For example, numerous vendors will deliver a Vulnerability Assessment proposal that contains language about how vulnerabilities will be exploited. This is an unmistakable contradiction as the definition of the term “Vulnerability Assessment” does not allow for exploitation.

Technically Impossible Projects
Some vendors offer a “Vulnerability Assessment and Penetration Test” as a service. This is both contradictory and confusing. Specifically, a Vulnerability Assessment does not allow for exploitation and yet a Penetration Test requires it. Some vendors might suggest that a Penetration Test includes a Vulnerability Assessment but that is inaccurate. A Penetration Test should cover the same ground as a Vulnerability Assessment (with more depth) but the boundaries of a Penetration Test are significantly different than those of a Vulnerability Assessment. One service class cannot contain the other.

There is no defined perspective
Some vendors define a Penetration Test as a service that is delivered from the perspective of an Internet based threat. They further define a Vulnerability Assessment as a service that is delivered from the perspective of an internal LAN based user. Where in the dictionary does it provide an internal or external perspective for the words Penetration, Vulnerability, Test or Assessment? It doesn’t.

Undefined terms aren’t helpful
Proposals that contain check boxes for undefined service additions like “External Validation” or “Enhanced Testing” should be avoided or rewritten. Many vendors will add optional modules to their proposals but fail to define what those modules do. It is critically important that buyers take the time to ensure that all terms are properly defined and understood.

Strip it naked
Strip the proposal of all content that is not related to the service that is being offered. For example, marketing content like discussions about corporate ethos is irrelevant with regards to the service being offered. Other content that is irrelevant includes but is not limited to undefined terms, information about past engagements etc. The goal is to strip the proposal down to its bare minimum required components so that the real offering can be clearly understood. If the offering can’t be understood after the proposal is stripped then you should likely consider a different vendor.
How To Choose the Right Vendor

Vendor Evaluation Questions & Answers

This section provides questions that you should ask vendors prior to making a purchase decision. Their responses combined with the information provided by this document should help you to determine which vendor best suits your requirements.

1. **What percentage of your testing is done with Automated Scanners?**

   As a general rule of thumb, the greater the dependence on automation the less the dependence on hands-on manual testing. This is also proportional to service quality. The more Automated Scanners are relied on for testing the lower the test quality and overall results will be.

2. **How do you define Penetration Test?**

   The term Penetration Test was clearly defined earlier in this document. It is important that the vendor not define the term Penetration Test with an example of methodology but actually define the term in such a way that demonstrates their understanding of boundaries. It is dangerous to receive services from any vendor when boundaries are not clearly defined and/or understood. It is also important to understand that quality penetration testing should be the product of human expertise and not the product of or dependent on Automated Scanners.

3. **How do you define Vulnerability Assessment?**

   The term Vulnerability Assessment was clearly defined earlier in this document. It is important that the vendor not define the term Vulnerability Assessment with an example of methodology but actually define the term in such a way that demonstrates their understanding of boundaries. It is dangerous to receive services from any vendor when boundaries are not clearly defined and/or understood. It is also important to understand that a Vulnerability Assessment should be a manually driven process and should not depend on the output of Automated Scanners.

4. **What are the differences between a Penetration Test and a Vulnerability Assessment?**

   A Penetration Test is a test that provides proof of vulnerability through exploitation and produces a deliverable that is free of false positives. A Vulnerability Assessment is an estimate as to how susceptible something is to harm or attack and provides no proof of vulnerability through exploitation. The deliverable produced by a Vulnerability Assessment will usually contain false some positives.

5. **How many False Positives do your Penetration Testing reports contain on average?**

   As previously states, Penetration Tests provide proof of vulnerability through exploitation. Exploitation is either successful or it is not. As a result, Penetration Tests deliverables should never contain even a single false positive. They may however contain theoretical findings. A theoretical finding is supported by science and is not a false positive. For example, it may be possible to crack an encrypted token but it may require 6 months time. It is possible to prove through science that the token can be cracked without actually performing the attack. Such a finding would be theoretical.
6. **Does your company perform vulnerability research?**

If yes, then ask the vendor for at least three advisories that they have published, or documents that they have published related to said research. If they cannot produce proof of research then chances are they don't really do research. Alternatively you can search various websites for research that they may have done. Most vendors that do research publish some, but not all of the research for marketing purposes. Some sites are listed below that collect such research products and advisories:

http://packetstormsecurity.org
http://www.exploitdb.com
http://www.securityfocus.com
http://secunia.com/
http://xforce.iss.net

7. **Does your company offer testing with real, homemade malware?**

Homemade malware enables a Penetration Testing vendor to test at realistic levels of threat. Specifically, malicious hackers are constantly using malware to penetrate into and take control of networks. Homemade malware does not include the Metasploit meterpreter.exe program but instead is something that is custom built for the engagement.

8. **Define Web Application Penetration Testing?**

A Web Application Penetration Test is a Penetration Test that is applied to Web Applications.

9. **Do you perform Web Application Vulnerability Assessments?**

This is a trick question. Based on the definition of the term Vulnerability Assessment, it is impossible to perform a Web Application Vulnerability Assessment. This is because Web Application Testing (when in a live and running state) can only be done by sending malformed data to the application. If the data hits a vulnerable point in the application then the application responds with an error condition or unexpected data. That response represents a degree of exploitation and crosses the boundaries defined by the term Vulnerability Assessment.

10. **What percentage of your service is based on Automated Vulnerability Scanning?**

It is our opinion that Automated Vulnerability Scanning should only be used for reconnaissance (information gathering) and should not be relied on for issue identification. As a result, we suggest that a vendor's services be made up of no more than 10% Automated Vulnerability Scanning.

11. **Can you send me a realistic sample report that contains some sanitized real-world findings?**

All vendors should provide sample reports to their customers when asked. The sample report should not be the product of an automated scanner, but instead should be hand-written. Often times automated scanners produce reports that contain sections with the exact same formatting but different content. When reports are created by a human there are slight to major differences in the way that each finding is presented.