11 Questions to Ask Your Pentesting Service Provider

Trustwave®

Introduction

Penetration testing is an essential part of a security program. There are many organisations ready to help you, but how do you know which one is the best fit for your business? This guide aims to rapidly arm you with essential questions to ask your penetration testing provider. The objective is to help you choose the right provider, and ensure you maximise the ROI from your testing investments.

1

What is your mission in performing penetration testing for my business?

Ask the organisation for their mission statement, a vision and values. Pentesting is at the heart of understanding your cyber risk profile and is probably one of the easiest tools to highlight the most obvious gaps in your defences. They should be able to give advice on what to test in context with your business needs. Look for a provider who values their pentesting team and freely communicates their approach to pentesting. They should have fixing has the client's security risk profile as the driving goal, and have staff that can efficiently and effectively communicate how the risks have shown up in your IT environment with remediation advice on how to fix them.

A specialist pentesting provider has advantages – they're usually experienced enough to have done an extensive variety of pentesting types, but are pragmatic enough to not over-recommend expensive and lengthy testing that is unnecessary. The investment in training and developing their pentesting staff should also be reflected in their organisational values. The quality of pentesting work you receive will often be a reflection of how up to date staff are on the latest attack methods and vectors.

It will also be opportunistic to choose a service provider that has also helped organisations remediate the issues found through penetration testing. They'll be familiar with what recommendations can be applied quickly in your existing environment, with massive impact to your posture, and perhaps little impact to your budget. Pragmatism should be a key attribute in their guidance (and reflected in their mission).

Read more about Trustwave SpiderLabs Testing services

2

What certifications and credentials do your staff and organisation have?

Use providers that have recognised credentials, such as Offensive Security Certified Professional (OSCP), Offensive Security Certified Expert (OSCE), CREST Registered Penetration Tester (CRT-Pen), CREST Certified Tester (CCT) and CCSAS/CCSAM.

For a larger piece of work, ask for references and resumes. A reputable vendor will be willing to provide you with the names of other testing customers who are satisfied with the services. Consult your peer network and ask the people whom you trust if they have any recommendations.

Trustwave is a global CREST member with an extensive team holding a large number of individual certifications.

3

What type of security research do you do?

What reputation does this provider have in the industry for finding vulnerabilities? The commitment of your penetration testing provider shows up in the type of research they do. Is this available on their website? Do they regularly investigate for new as well as know vulnerabilities? Are they looking across both physical and digital platforms that may be penetrated?

All work and no play makes for pentesters who rarely get time to explore out-of-the-box vulnerabilities. And this impacts the quality of the testing you will receive. Look for a provider that is willing to show where their staff have explored beyond the day-to-day and are sharing their experience in the industry including their experience with both known and unknown CVEs. An excellent pentesting firm will also have teams of people doing forensic investigations for clients and are able to apply their knowledge of the latest TTPs to their testing methodology.

The SpiderLabs blog is an excellent resource that demonstrates the type of research that we do.

4

What capacity do you have to do my testing? And who will be performing the tests?

Look for a tester with a large and diverse team; the larger the team is, the more likely the vendor can field a tester with experience in the specific technology stack, in the industry, and in the time frame you need testing. Smaller players may not have the right person available when you need them.

If you procure a lot of testing, it is both healthy and desirable to have a panel of testing companies to call, rather than being locked into a single provider. This practice gives you a larger pool of testers and

thus more ability to test as and when you need to. Importantly, different vendors testing the same target may uncover differing issues, so cycling your testers is also to your advantage.

Remember not to fall into the trap of choosing the cheapest quote. If you do this, compare both the quoted effort and daily rate. (A low day rate is only less expensive if the number of days is less.)

Ask your pentesting provider for their Net Promoter Score (NPS). Class any score above 70 as EXCEPTIONAL.

5

Is this a vulnerability scan, or a penetration test?

Don't pay a vendor to find blank MS-SQL passwords or tell you that your servers are unpatched; use a vulnerability scanner for these more common issues. Scanners are great at finding blatant network vulnerabilities and other low hanging fruit. Your penetration test vendor should be identifying the paths to data compromise that a vulnerability scanner never will.

While a penetration tester might use various tools, it is the human element that makes the difference. The ability to understand nuances, think creatively, and both make and test hypotheses are the difference between automated tools and a human-led penetration test. It is unlikely that many people possess Michelangelo's ability to create stunning sculptures out of marble, regardless of how many cool power tools they may own. Without human ingenuity directing them, the power tools are nearly useless.

Learn the differences between vulnerability scanning and penetration testing in this blog.

6

What reporting of results do you provide?

The penetration testers your business uses need the ability and discipline to document and explain what they conducted and found concisely. This will help you address gaps and accurately perform retesting to ensure issues with your systems or applications are resolved. Ask for samples of the reports that they deliver to clients. These should be detailed enough to make you feel comfortable that every significant aspect was investigated.

The final report should contain details of issues, including a clear description of the potential to exploit each and, when applicable, either a proof of concept or instructions to recreate the issues. This information will give your teams a better understanding of the problems and how to remediate them. If you are paying for advanced testing, ensure that the report includes enough detail to allow a technical reader to reproduce the results. This may include written descriptions, screen shots, and in some cases video evidence. Additionally, ensure the report helps you prioritise the remediation activities, addressing the issues with the greatest impact and likelihood first.

Your testers should also be willing and able to jump on a call with your technical teams and explain their methodology and findings where necessary. A good tester will relish the opportunity to explain to a developer how they can find and prevent similar issues in their future work.

Our Trustwave Security Colony portal hosts a complimentary 'Penetration Testing Request for Proposal Template'. Sign up for free access at SecurityColony.com and check the resource library for the latest edition, or if you are already a member click here.

7

What recommendations do you have for the scope of this test?

Understanding the scope of a test is the key to understanding how much effort will be required.

A testing scope can be as narrow as a single URL, or IP Address, or even a specific functionality within an application following an update. Conversely, the test's scope can be as broad as your entire internet-facing attack surface and supporting infrastructure. Work with your vendor to determine the best type of test for your requirements; they can help you decide between a vulnerability assessment versus something more detailed.

Blackbox, greybox and whitebox testing classifications identify how much information the tester receives about the target system before the test itself. Although it may seem counterintuitive to provide a tester with intel that a real-world attacker might not have, time is of the essence. Performing research to understand something that ultimately does not lead to any vulnerabilities is precious time lost.

Additionally, the recommendations resulting from a penetration test can often be far more specific and detailed when testers have a firm working knowledge of the environment they are testing. This knowledge can be the difference between a testing report stating 'investigate why login field accepts special characters' and 'upgrade the following dependency to version 2.3.7'.

8

Does the scope of my tests include re-tests?

In our experience, every system and application we have tested has some vulnerability or security flaw. It's advisable to set up your testing program so that you have additional retests built into the scope of the contract. This will allow you to resubmit your system for testing and ensure that the security flaw is resolved, before your company puts the system into production. A review of your final system through objective eyes is essential for solid security practices.

Learn how the Trustwave Fusion portal can simplify the management of your ongoing testing needs in this blog.

9

Are you experienced with testing cloud systems?

The commonplace adoption of cloud platforms dictates that your pentesting service provider should definitely have experience in delivering effective tests for this type of environment. Testing in the cloud requires a slightly different approach. Not understanding the nuances between cloud and internal testing can lead to poor outcomes such as:

- Testing efforts scoped incorrectly or overpriced
- Testing unmanaged or unowned components
- Overlooked/missed issues
- A potentially toxic relationship with your cloud service provider

You should not need to and will be very unlikely to get permission to test the underlying cloud infrastructure.

Ask if your testing provider already has experience with common cloud service providers such as AWS, Google Cloud, and Microsoft Azure platforms, as well as PaaS and SaaS vendors. Their prior experience will be to your advantage as their testers will have experience knowing where the boundaries are for aspects under your control.

Read more about the top 6 cloud security problems Trustwave commonly identifies here.

10

At the end of the engagement, ask the person leading the testing engagement if they had enough time for the test?

Asking a tester if they had enough time is a great question to ask at the conclusion of every test to be better prepared for the next round of testing.

The most effective way to determine if the estimated effort is sufficient would be to carry out the testing and ask the tester if they would have preferred more time. Because of tight deadlines, sparse budgets, or the system simply not being ready during the testing window, a tester may feel that the time they had was insufficient, which may imply a need for additional testing.

Most testing organisations use a concept called Timeboxing when scoping a test. Timeboxing means the testers will attempt to cover all common issues and then use their experience to maximise any remaining time by applying a risk-based approach to identify crucial vulnerabilities first. Prioritising the time remaining after identifying any common issues acknowledges that the testing time is finite, and poorly scoped tests will not come close to identifying any remaining issues that may exist.

11

How do you plan to grow with my organisation over time?

Building a relationship with your pentest provider over time has its benefits. If your industry is suddenly exposed to a known attacker or vulnerability within common software or systems, it's excellent to be able to call on them for emergency pentesting services to see if your business has been exposed, but woks only if that company can scale with your business and perhaps meet the need to do that testing in real-time (and possibly overnight!).

Ensure the provider you choose has mature processes and experience that allow the identification of complex and 'difficult to find' vulnerabilities as your pentesting needs grow.

Look for flexible contracting options that cater to large programs of work and multiple tests requiring scalability. For large programs, expect a named technical account manager that you can work with to plan your testing program and maximise your return on investment.

About Trustwave SpiderLabs Testing Services

With the very best people in the industry, Trustwave strives to give actionable technical consultancy so that our clients are able to secure their people, processes and technologies against all threats.

Our vision for Trustwave SpiderLabs Penetration Testing Services is to be the assurance service of choice and a leader in the field, by investing in our people, demonstrating our core values to clients, and striving to be the best.

Our key values for penetration testing:

- **Client First** putting the client first is at the heart of what we do.
- **Quality** the highest quality in everything we do, from Pen Testing, communication, to reporting.
- **Honesty** honesty is imperative with pentesting, we are always honest with clients and ourselves.
- **Integrity** Clients expect the highest integrity from an impartial testing provider, we put integrity at the centre of our values in SpiderLabs
- **Passion** the Spiderlabs Pen Testers love their job, that'll be evident when you speak to anyone of them.
- **Flexibility** being flexible around client needs is important to clients and to us.

About Trustwave

As a recognized global cyber defender that stops cyber threats all day, every day – we enable our clients to conduct their business, securely.

Trustwave detects threats that others can't see, enabling us to respond quickly and protect our clients from the devastating impact of cyberattacks. We leverage our world-class team of security consultants, threat hunters and researchers, and our market-leading security operations platform, to relentlessly identify and isolate threats with the right telemetry at the right time for the right response.

Trustwave is a leader in managed detection and response (MDR), managed security services (MSS), consulting and professional services, database security, and email security. Our elite Trustwave SpiderLabs team provides award-winning threat research and intelligence, which is infused into Trustwave services and products to fortify cyber resilience in the age of advanced threats. For more information about Trustwave, visit www.trustwave.com .