RHINO SECURITY LABS

BUYERS GUIDE:
6 QUESTIONS TO ASK EVERY PENTEST COMPANY

Finding and evaluating a penetration testing company doesn't need to be a headache.

With this buyers guide, you'll get the 6 questions to ask every vendor, what to look for in each question, and the key takeaways from the discussions.

TABLE OF CONTENTS

Introduction

Finding the right penetration testing vendor can be a hassle, particularly for those unfamiliar with the space. What do we ask? How do we know who's technically qualified or capable? How do we identify risky or unqualified providers? What should reporting look like? How is pentesting priced out?

With these vendor selection criteria – and associated questions in the following pages – you'll have all of these addressed. By the end of this document, you'll know what to look for in a potential vendor, potential fit falls, how to compare options, and eventually make the best choice for your security needs.

If you're unsure about how to compare pentest companies or what to look for in a provider, this is the eBook for you.

Vendor Selection Criteria

Personnel and Talent

The personnel on your project can make or break the success of the engagement. Even a top-tier, trusted security provider will provide poor results if the wrong resources are brought in. Understanding who's on your project and their qualifications will significantly improve your chances of a positive outcome.

Technical Expertise

How do you judge the technical expertise of the provider? Research and development can be a good indicator for both your assigned engineers and the firm as a whole. Between your own searching and asking them directly, you can get a better idea of their security capabilities and what they offer. Those without recent technical research may be outdated in their capabilities or unable to provide adequate depth of testing.

Penetration Testing Reputation / Trust

The vendor's reputation as a quality, trustworthy provider is another key aspect you should consider. Before even setting a meeting, do some research on their background and expertise. Googling them, what can you find? Do they have anything in the media? Any detailed expertise or blog posts related to your technical needs? This background will give you better insight into the firm and provide more discussion during the call.

Effective Documentation

Proper reporting is critical but quality of documentation can vary widely. Ask for example reports of each of the services you need (network, webapp, mobile, etc) and make sure you fully understand the vulnerabilities in the example. Nothing can be more frustrating than an engineer's poor writing style or ambiguous process details.

01

What Security Research / Vulnerability Disclosures do you have?

Focus: Technical Expertise

Why this matters

When choosing a pentest provider, one of the most important factors – and often the hardest to identify – is the quality of the penetration testing services. While a buyer can rely on 3rd party standards or quality ratings in many other markets, no such standards exist for penetration testing. Even without an external rating scale, security research can be a great indicator for judging technical capability.

Research and development by a security vendor demonstrates two important things. First, the assessment team has the technical capability to dive deep into security problems. The skillset of the individual personnel can make-or-break the success of a security assessment (and will be covered in more depth in later questions). The second aspect is whether the company is *willing to invest in the quality of its pentesting services*

What to look for

An effective penetration testing firm will have multiple recent research projects to review. Building new security and pentesting tools, identifying zeroday vulnerabilities, and diving into the security of new technologies are promising indicators. Private research is common, but be skeptical if they can't showcase any public capabilities.

A side benefit of this question is a better understanding of the vendor's technical focus, and reviewing the match to your own technical needs. Using Rhino Security Labs as an example, we have research specialists in AWS testing, web application security, and Linux/UNIX exploitation. We have strong capabilities in many other areas, but companies with these needs may be the best fit.

Key Takeaway

Think of selecting a pentest firm as if you were interviewing a prospective candidate for a job. Technical capability is an effective filter, but once that's established the fit with your needs is a consideration as well.

Does the security vendor have a particular security focus or expertise? How does that match to your own environment and technical needs? Remember, this is an assessment on your information security posture - quality is key!

02

Who would be on the Project?

Focus: Personnel Qualifications

Why this matters

In professional services industries, it's an unfortunately common tactic to sell clients on the firm's most senior, qualified experts, then quietly use junior personnel for the actual services. While this resource dilution technique has historically been an enterprise move, even boutique firms have been caught using this to mislead potential clients.

This practice not only results in a poor quality penetration test (missed vulnerabilities and higher risk - but also leads to higher chance of testing accidents and business impact.

Of course this isn't all penetration testing firms – and in some cases, the experts are the ones doing the engagement! Being able to identify - and sidestep - these techniques will help get you the best assessment for your money.

What to look for

When meeting with a prospective firm, ask for the names and qualifications of the pentesters that would be on the engagement. Confirm any promoted "rockstars" are actually the engineers in your engagement, and what their roles would be.

Vague language around who "may" be involved can often be a warning sign.

A slight variation of the same tactic is having a given experts be involved in a small way for multiple engagements simultaneously. That allows the vendor to list that person on your engagement, even if they're not contributing in a significant way.

Key Takeaway

A prospective firm should be able to provide you the names of all pentesters, as well as their qualifications and expertise, who will be on your engagement. Ensure you know who these people are, and can validate their capabilities and credentials.

Clarify any ambiguities around roles and the level of involvement for everyone listed on the project.

03

How much of the Penetration Test is Tools-Based?

Focus: Effective Process / Technical Expertise

Why this matters

Automated tools and scanners are the start to any pentest, but they have limitations and often miss the more subtle and high-impact risks. The amount of manual testing is another easy way to identify potential quality issues with the offered penetration test.

A quality pentest will be largely a manual, deep-dive review process - upwards of 90%, in the case of Rhino Security Labs. The other 10% is a range of specialty tools we've developed internally, and a range of industry-standard vulnerability scanners for the low hanging fruits.

The level of hands-on attention can often be the difference between "no significant findings" and gaining access to critical data and systems.

What to look for

When asking about how much of the testing is based on tools, remember that scanners only go so far. The experience (and time commitment) of the penetration tester will make a bigger impact than the specific tools.

The answer to these should have a high emphasis on the hands-on review of your application, network, or other assets in scope. Scanning and other automated tools are a small contributor to any thorough pentest.

This conversation around tool focus can lead into the next question as well, focusing more on the methodology and process of testing itself.

Key Takeaway

If the vendor indicates most of the test is automated or doesn't ask many questions about your environment, be wary. These vulnerability assessments (priced and marketed as full pentests) can bring a false sense of security – and bring about additional risks in the process.

Thorough and comprehensive pentests manual, structured, and provide the best results.

04

What is your Penetration Testing Methodology?

Focus: Effective Process

Why this matters

Any security assessment needs a well-defined methodology and to follow the structured process. This helps establish a proper workflow to minimize confusion while maximizing security benefit and tests results.

The industry-standard methodology is the Penetration Testing Execution Standard (PTES), and ensures a structured process – and eventually, the success of the assessment.

1. Pre-Engagement Actions (identify scope, obtain formal approval)
2. Reconnaissance (information gathering on the targets)
3. Threat Modeling (identify components that require the most review)
4. Vulnerability Scanning and Analysis
5. Attack and Exploitation (exploit identified vulnerabilities)
6. Post-Exploitation (evaluate the impact of the compromise)
7. Reporting (develop thorough documentation of the project)
8. (optional) Remediation Testing

What to look for

While penetration testing is as much art as science, professional engineers will always use a structured process and procedure. If they elaborate on their assessment structure, ensure it starts with the reconnaissance or information gathering phase. While this seems like a small detail, proper recon is often neglected and can lead to missed security opportunities.

Similarly, due to the inherent concerns of business impact in a pentest, ensure that you can contact them directly in the event that unusual activity or downtime is identified. Engagement communication is critical in mitigating potential problems, and the team should be available for direct contact when needed.

Key Takeaway

Ensure the firm has established a clear, well-defined methodology that aligns with industry standards. Methodologies help define standards and a workflow to keep pen tests in line with your scope and test objectives.

05

Do you have Example Assessment Reports Available?

Focus: Reporting and Documentation

Why this matters

Pentest reports are critical for you to understand where IT security risks and weaknesses reside within your environment; these vital documents will remain well after the assessment has completed, and will be sent to those who never interacted with the vendor. Clear and thorough documentation is critical.

But this is easier said than done, and reports need to meet the needs of a range of people - from the technical experts to management. This range of needs means a greater chance something is missed and someone is confused about the results.

This is where example reports come in. By reviewing the documents for each pentest scope you'll be incorporating (networks, web applications, etc), you'll know if these will fit your internal needs.

What to look for

There's a wide range of penetration testing reporting options, but there's a few things that should always be present.

- **Executive Summary** – High level overview of the engagement; provided for leadership and non-technical focals to review results.
- **Vulnerability Overview** – For both management and engineers alike. Should include a summary remediation for each associated issue as well.
- **Vulnerability Details** – The risk-prioritized technical breakdown of each risk identified. Should also include how the vulnerability was exploited.
- **Detailed Remediation Steps** – Part of each vulnerability in the detailed section; outlines possible fixes for a given flaw.

Key Takeaway

Request samples of pentest reports by each prospective firm. Good pentest firms will always have samples of each engagement type available for you to review.

You can find Rhino Security Labs reports for download here.

06

Are all pentesters US citizens? Do you use contractors for pentesting?

Focus: Legal Risk

Why this matters

Penetration testers can be from a range of backgrounds, and with access to basic internet, located anywhere in the world. While this allows security vendors to source employees from around the globe, it can add additional legal and security risks to a highly sensitive service.

Simply put, US law isn't enforceable in other countries.

Using at-will contractors can also provide a similar risk, as very often these personnel do not have the same background checks and familiarity of full time employees.

Examples abound where foreign contractors were brought in for a security assessment, only for data to be lost or stolen after the conclusion of the engagement. Since the other party was in another country, legal remedies were almost nonexistent.

What to look for

First, understand any previous contractual obligations that may limit who you could hire for a pentesting firm, or who would perform the engagement. Customer data agreements, privacy agreements, and regulatory standards may have clauses which outline who sensitive data may be accessed by.

Beyond that, confirm with the pentest vendor that all its penetration testers are US citizens and full time employees. This may not be the case, but is worth considering in the buying process.

Key Takeaway

Penetration testing and security assessments are a highly sensitive, invasive process. Ensure you're 100% comfortable with the vendor, as well as those personnel assigned to the project.

Citizenship or employment status does not guarantee the quality or thoroughness of a pentest, but it will have an impact on the legal risk being incurred. Consult legal counsel when appropriate for compliance or contractual requirements.

Conclusion

The process of finding and vetting the penetration testing vendor can be daunting, but there are questions to help guide you through the process. By providing the aforementioned questions to each vendor, you'll have the details to make a more educated, informed decision – no technical expertise needed!

Trust, technical expertise, quality of personnel, and depth of reporting are some of the most important aspects of choosing a security assessment firm. However these aren't the only details that should be considered. Pricing structure, potential conflicts of interest, previous references, and industry experience can all be important considerations as well. In addition to the questions provided here, ask your own questions and ensure you're comfortable with the provider you choose - your security is too important to gamble with!

For additional support on these questions – or to get our answers to these – contact us at:

rhinosecuritylabs.com/contact

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a boutique penetration testing and security assessment firm focused on networks, applications, IoT, and social engineering. With manual, hands-on engagements, we identify and mitigate security vulnerabilities which put client assets at risk. Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.

We bring together the security research, proprietary technologies, and industry-leading security engineers to create the best penetration testing firm in the industry. So whether your focus is the external network, complex web applications, in the AWS cloud, or social engineering testing, we have the specialists to fit your unique needs.

RHINO SECURITY LABS

info@rhinosecuritylabs.com
(888) 944-8679
www.RhinoSecurityLabs.com