PENETRATION TESTING
BUYER'S GUIDE

risk crew

Shelter from the Storm

GET THE MOST FROM YOUR PENETRATION TESTING INVESTMENT

CONTENTS

Introduction

Small steps lead to big changes

If you are just starting your testing programme or are looking to enhance the current one, this buyer's guide provides valuable insights — on everything from defining your scope, and choosing a provider, to receiving maximum benefits to protect your critical information security assets.

This buyer's guide was created by Risk Crew's accredited CREST penetration testers and expert information security professionals who possess 30 years of experience.

Suggested best practices within this guide, will help you gain a solid understanding of what not only should be considered in a penetration test but how to receive measurable results to increase your Return on Investment (ROI).

This guide focuses on six essential elements and three principles to follow — to ensure you receive the ultimate benefits from your penetration testing programme.

The Right Test

What is Penetration Testing?

Choosing the right test is the first step to a successful Penetration Testing engagement. Therefore, let's start with defining what a penetration test is and is not.

Security penetration testing is the process of identifying, assessing, and attempting to exploit security vulnerabilities associated with computer systems, applications, and network infrastructures to obtain unauthorised access.

The objective of penetration testing is to simulate an attack by a cyber threat actor and in doing so, "test" the security configuration and controls implemented to prevent a "penetration" of your defences. The process involves using an assortment of automated and manual tools to identify and exploit known, and unknown security vulnerabilities associated with a target to obtain a specific goal — such as unauthorised access.

It is an art

Penetration testing is an "art" and good testers are indeed, artists. They look at the canvas of vulnerabilities and don't just "connect the dots" — they visualise and execute the attack that could result in access. So, the outcome of a good penetration test is a real-world evaluation of the vulnerabilities in your application/ network.

What we all too often forget is that cyber security is an oxymoron. There is no such thing as a "secure" computer, system, application or network. All hardware and software are inherently vulnerable. A penetration tester knows this and approaches each test with the objective of finding the specific vulnerability (or combination of vulnerabilities) that should be addressed to reduce the real risk of a breach.

What it is not

A Vulnerability Scan (VA) is often confused with a penetration test. VA scanning is an inspection of the potential points of exploit on a computer or network to identify any security holes such as default passwords, missing patches or legacy builds. The scan detects and classifies weaknesses against the assumption that they are exposed to an attacker.

Vulnerability Scanning	Penetration Testing
Using automated tools to identify known security vulnerabilities associated with a target.	Using an assortment of automated and manual tools to identify and exploit security vulnerabilities associated with a target to obtain unauthorised access.

The Six Elements & Three Principles

There are six central elements to consider. Including all six in the planning of your penetration testing engagement will ensure you get the best return on your investment.

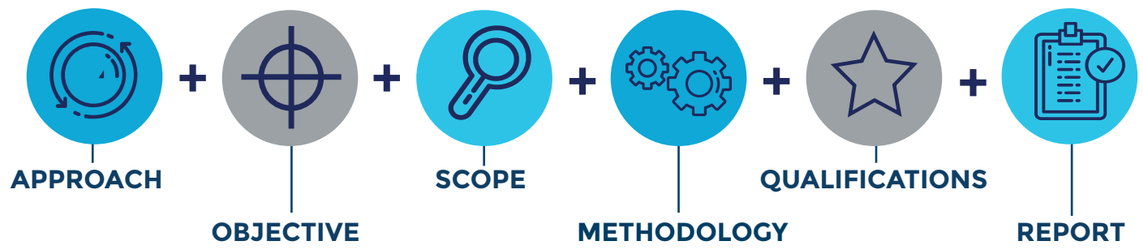
Before you start with any of these six central elements, there are three principles important to focus on. The quality of the test you receive is dependent on your focus on setting up the test, making sure that nothing is assumed between you and your testing provider, and that you are (in fact) part of that process.

Focus — Assume Nothing — Be Part of the Process which is the most crucial.

These three are crucial and will underline the approach, objectives, scope, methodology, qualifications and report standards.

Combining these six elements and three principles will help you optimise your penetration testing.

The Right Test = 6 Essential Elements



An optimised penetration test can give you knowledge and insight into a majority of your technical security weaknesses and provide you with the remediations and support required to fix those vulnerabilities. **With an optimised penetration test, you'll receive many benefits including:**

+ A reduction in your ICT costs over the long term
+ Improvements in the technical environment, reducing support calls
+ Greater levels of confidence in the security of your IT environments
+ Increased awareness of the need for appropriate technical controls
+ Opportunity for continuous improvement of your testing

1. The Right Approach

Know what you are asking for

Take the right approach by first asking yourself why are you testing? What's the goal? You need to answer these questions to set your expectations on what you expect the outcome to be.

Think it through, to understand how the test is going to benefit the business. Do not assume the penetration testers you engaged will know what you need — as they are assuming you know. They will assume if you are buying the test, then you must know what you want.

Buyer's Tips

You can optimise your penetration test from the very beginning by documenting your objectives and goals to then get the scope right. Additionally, this will help you determine the objectives and goals. Document the methodology, tools, tester qualifications needed and the vulnerability classification scheme that you want them to use for the findings document.

You may not have all the answers to what needs to be included in the testing engagement and that's understandable. However, before you put out a purchase order to secure the pen test, you need to document items both internally and externally with your testing supplier. This will ensure you get optimised testing. Otherwise, you will be depending on your service provider to do it for you and end up saying 'yes' to everything — which might not be what you need.

Identify to the specific service provider the test objectives, scope, methodology and any tools you may want to use, so you're not just relying on their assumptions. Sure, they know what they're doing, they're professionals but optimisations start at the very beginning with you. Sit down and document it yourself. Write them out so they are clear and then you can correct them if needed when in discussions with your testing provider.

2. The Right Objective

Ask yourself, why are we testing and what is the purpose of this test?

To obtain the right objective, you should ask yourself, why are we testing and what is the purpose of this test? You'll want to answer this yourself and not rely on the supplier to do so. You can start by answering what goals you want to receive out of the testing. **Is your goal to:**

- Identify vulnerabilities. If yes, what type of vulnerabilities?
- Test unauthorised access to your systems? (such as testing the ability of an outsider to gain access to the website, IP or network)
- Test unauthorised access to your information assets? If yes, what assets? (such as testing the ability of an outsider to access HR files or Credit Card data)
- What assets are you most concerned about? What are more or less sensitive assets?
- Test the ability to gain administrative privileges?
- Fulfil a compliance requirement?

If you cannot specifically determine the objective of your testing, then you might be spending a lot of money bringing in a third party to assess the security of your systems and not gain any return on investment.

Buyer's Tips

Look at all the security controls and include them in the testing engagement to optimise the objective. While your penetration tester is on your network, website and/or systems, consider having them investigate other security features such as:

- **Architectural design**
- **System security devices**
- **Anti-malware protection**
- **Change management programme**
- **Whitelisting programme**
- **User security policy compliance**
- **Incident reporting programme**
- **Incident response programme**

Consider widening the scope by adding additional objectives to get more return for your testing budget. For example, you might have the tester see if they can put traffic through a firewall port that you have put a lot of time and effort into securing.

3. The Right Scope

Identify what's in target

Determining the right scope involves verifying the target of **what's in scope,** but just as important is **what's out of scope**. It's crucial for the service provider, to understand the target IPs and URLs that host the targets. Additionally, a list should be provided for targets not to be tested. For example, you may want third-party partners, hosting providers and C-level executives to be excluded from the testing. Knowing what's out of scope is just as important as what's in, and both should be documented.

Align information assets and risk registers

The next step is to check the scope and connect the dots. Ensure everything lines up with your information assets and risks registers. Double-check if IPs and URLs are the correct ones, that host the information assets, you asked that provider to get unauthorised access to.

Where does your network start and stop?

The tester must understand what you want the scope to cover. Will it encompass Office 365, the Internet of Things (IoT) connections, mobile devices and any other technologies? What you asked for, is what you'll get. Never assume that testing will cover your whole network environment.

Buyer's Tips

Make a checklist and carefully tick off what's (in scope) and (out of scope) based on technologies that process, store and transmit your assets. **To optimise the scope, you should consider adding:**

+ Mobile device
+ Remote connections
+ Remote authentication connections
+ Home environment connections
+ Commercial partner connections
+ Third-party supplier connections
+ Vendor connections
+ Hosting providers
+ Staff!

A good pen test takes a holistic approach to include people, processes and technology. Risk Crew recommends that you include some baseline social engineering attacks, phishing, telephone vishing and pretexting attacks — to get initial metrics. Include a percentage of staff in the sample to allow you to capture metrics and key performance indicators (KPIs) to benchmark against your security awareness programme. Make sure that next time you test that it's with the exact same attacks, at the same time of day and uses the same testing methodologies, to see if the risk level has changed.

4. The Right Methodology

Determine the Methodology

Decide what methodology you want the testers to use, which could be CHECK, CREST or OWASP. If you do not know the right methodology, then ask your provider about what they recommend for what is to be achieved. If you require compliance-driven testing — ensure the methodology will meet the requirements. Also, it's important to determine the style of testing required, such as black, white, or grey box testing as outlined in the table below.

Get involved

We would like to assume that every testing provider knows the best methodology and tools to use. However, it's in your best interest to do your research before the discussion with them. Knowing the fundamentals will help you be a better buyer.

Buyer's Tips

Ensure your SLA mandates the methodologies to be used. Not only do the methodologies identify vulnerabilities but they exploit them.

Make sure the testers explain the methodology and the vulnerable register used. Also, ask the testers to tell you what classification schemes they will use. They should explain the toolset applicable to each testing phase.

If possible, try to get the tester on site. It will be worth the knowledge transfer alone. Having a tester in your offices will give them the ability to show you what they found in real-time. It gives you a tactile understanding of the vulnerability and its exploitability. Getting this knowledge transfer is an easy way to optimise the output from the test and it will leave you being much smarter about the whole process.

Testing type	Description	Pros	Cons
Black Box	No target details are provided. The objective is to bypass perimeter security. An example objective is to bypass security controls in order to gain unauthorised access.	It's fairly quick and inexpensive. Reproduces the scenario of an opportunistic external threat actor.	Only tests the external layer. Very limited identification of vulnerabilities. Testing is time-limited...threat actors are time unlimited!
White Box	The tester is provided with full attack surface intelligence. (i.e. Credentials, IPs & URLs, Network Access, Applications Source Code, Whitelisting etc.). Multiple testing objectives are included.	Supports a more targeted test on a system that requires testing of as many vulnerabilities and attack vectors as possible.	Significantly longer testing time with higher cost. Planning may be resource heavy on client IT teams. 'Be careful what you wish for!'
Grey Box	A hybrid of Black and White Box testing. Comprised of client-defined testing objectives.	Good value for money. Prioritised and targeted testing. Typically targeting high value assets.	Not as deep as a White Box test.

5. The Right Qualifications

Ensure your testing value

To obtain a quality penetration test, make sure your testers have the right qualifications. **You should ask your provider the following questions:**

- What are their qualifications?
- What professional certifications do they hold?
- How many years of experience do they have?
- Have they had background checks?
- Do they have experience testing similar systems?

Never assume

Don't assume that the service is going to be delivered by the same level of testers from one company to the next. You should trust your provider, but we recommend you verify the tester's qualifications. Also, you can require your provider to deliver CVs of the testing engineers who will be testing.

Buyer's Tips

The tester is going to have intimate knowledge of your systems and vulnerabilities. **Therefore, we recommend that you do the following:**

+ Require minimum certifications
+ Require minimum experience
+ Meet the tester and review the objectives with them
+ Have them explain the toolset and how it's conducive to the testing objectives

It's advisable to have an introductory call or meeting with the testers. You might ask them what they do and don't like about pen testing. This will give you an idea of what makes them tick. You'll get insight on if they manually exploit or rely more heavily on automated tools. Ask the testers to explain and review the tools they use.

If you were going to hire somebody to break into your house, you wouldn't just take anybody sight unseen. It's best to see them face-to-face to understand their mindset. You can also explain your expectations and more importantly understand the testers' expectations. This is the easiest way to optimise.

6. The Right Report

Get the report you expect

All this we covered, now comes down to the report. First, determine what you need. **Here is a list to ask yourself:**

- Do you want a non-technical or a technical report? Or both?
- What format would you prefer: Word, PowerPoint or Excel?
- Do you want visuals added?
- Do you need a compliance requirement addressed in the report?
- What evidence do you want to be documented?
- Do you need a certificate of compliance?
- How many copies?
- How would you like it transmitted?

Buyer's Tips

When you open up the first page of the report, you'll want to see if testing was targeted and if objectives were achieved. Did they get unauthorised access and access to privileges? Could privileges be escalated? These are yes or no questions that should be addressed — so make sure you ask for them.

Ask for visual evidence to show what vulnerabilities were found and how they were exploited. Ensure the findings show what real risk these mean to the business.

Continuous Improvement

Once you have the test in your hands, this should not be the last step. We recommend that you look it over thoroughly to identify continuous improvement. **Here's a short checklist to help you evaluate the testing and the report.**

+ Did staff identify testing?
+ Were incident response procedures implemented?
+ Confirm testing activity was identified in the firewall activity logs
+ Confirm testing activity was identified by IDS
+ Confirm testing activity was identified in the file integrity log monitoring reports
+ Were KRIs activated?
+ Were KPIs effective?
+ Should KPIs be changed or augmented?
+ How can you improve the next test?

Reviewing these will help you to see the impact of the testing and if improvement can be made on the next test.

The Service Level Agreement

Every question asked in these six elements was done for you to answer and put into the Service Level Agreement (SLA). Remember, if you don't ask for it, you're not going to get it. So, write everything down and include it in the SLA to ensure contractually that the service provider is required to provide it.

At the end of the day, if you have a dispute, it's all going to be settled by what contractually you asked the service provider to do. Remember, it's got to be in writing, it's got to be in the contract.

The Associated Costs

Simply said, testing costs will vary. Essentially, you are purchasing the time, experience and qualification of the penetration tester to provide the information you need.

A daily rate typically ranges from £600 to £3,000. Travel and accommodation expenses may need to be factored in. If paying for a premium 'branded' service provider, you may see a daily rate above £1,500 per day. If you have highly sensitive stakeholders, you may decide it's worth the cost of the brand name to reassure them.

We recommend you evaluate quotes that are obtained from three reputable providers. The content of the quotes and proposals will provide an idea of how much care they have taken to listen and to understand your needs and requirements.

Essential Resources

Open Source Security Testing Methodology Manual (OSSTMM) from ISECOM

OSSTMM is peer-reviewed and maintained by the Institute for Security and Open Methodologies (ISECOM). It was primarily developed as a security auditing methodology assessing against regulatory and industry requirements. OSSTMM is known for its Rules of Engagement, which is defined for both the tester and the client on how the test needs to properly run, starting from denying false advertising from testers to how the client can expect to receive the report. New tests for international best practices, laws, regulations and ethical concerns are regularly added and updated.

Open Web Application Security Project (OWASP)

(OWASP) is a not-for-profit foundation that aims to improve the security of software. Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

Penetration Testing Execution Standard (PTES)

PTES was developed by a team of information security practitioners with the aim of addressing the need for a complete and up-to-date standard in penetration testing. In addition to guiding security professionals, it attempts to inform businesses about what they should expect from a penetration test and guide them in scoping and negotiating successful projects.

National Institute of Standards and Technology (NIST)

NIST promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The NIST framework specifies the following three components of a penetration test: Pretest analysis based on complete knowledge of the target system(s) Pretest identification of potential vulnerabilities. Testing to determine the exploitability of identified vulnerabilities.

Provider Comparison

Notes:

P[1]

P[2]

P[3]

	Provider 1:	Provider 2:	Provider 3:
Company Name:			
☐	Provider holds pen testing credentials	Provider holds pen testing credentials	Provider holds pen testing credentials
☐	If testing for compliance, the provider's credentials align with the requirements	If testing for compliance, the provider's credentials align with the requirements	If testing for compliance, the provider's credentials align with the requirements
☐	Provider holds ISO 27001 certification	Provider holds ISO 27001 certification	Provider holds ISO 27001 certification
☐	Provider is highly recommended & can provide case studies & references	Provider is highly recommended & can provide case studies & references	Provider is highly recommended & can provide case studies & references
☐	Testers hold educational & professional qualifications	Testers hold educational & professional qualifications	Testers hold educational & professional qualifications
☐	Testers' CVs can be provided	Testers' CVs can be provided	Testers' CVs can be provided
☐	Testers are vetted, hold certificates & security clearances	Testers are vetted, hold certificates & security clearances	Testers are vetted, hold certificates & security clearances
☐	Testers are employees, not contractors	Testers are employees, not contractors	Testers are employees, not contractors
☐	Testing approach is both automated & manual (not just automated)	Testing approach is both automated & manual (not just automated)	Testing approach is both automated & manual (not just automated)
☐	Provider understands your risk profile and requirements & have included them in the scope	Provider understands your risk profile and requirements & have included them in the scope	Provider understands your risk profile and requirements & have included them in the scope
☐	Provider can provide sample reports & the quality is a high level	Provider can provide sample reports & the quality is a high level	Provider can provide sample reports & the quality is a high level
☐	Provider offers free retesting	Provider offers free retesting	Provider offers free retesting
☐	Provider provides follow-up service that includes on-call assistance	Provider provides follow-up service that includes on-call assistance	Provider provides follow-up service that includes on-call assistance
☐	Competitive pricing matches the criteria of the amount & quality of deliverables	Competitive pricing matches the criteria of the amount & quality of deliverables	Competitive pricing matches the criteria of the amount & quality of deliverables

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234
riskcrew.com
info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom