THE ULTIMATE HANDBOOK TO PENETRATION TESTING

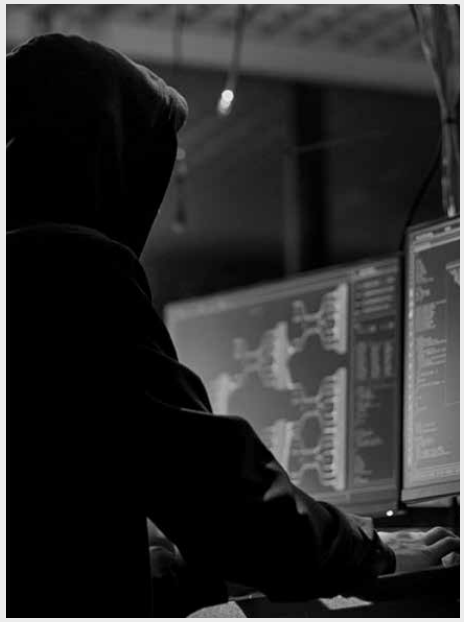
COMTACT
ALWAYS ON. ALWAYS SECURE.

CREST

THE ULTIMATE HANDBOOK TO **PENETRATION TESTING**

ABOUT THIS GUIDE

Penetration testing is a **critical part of an on-going cyber assessment programme** and is one of the common tools at your disposal, providing a real-world test of your cyber security defences.



Often referred to as ethical hacking, penetration testing uses all the tips and tricks available to real-world hackers, but performed in agreement with the company being tested, to a pre-defined scope.

The goal of a penetration test is to:

- **Identify security weaknesses**
- **Prove these weaknesses through exploitation**
- **Provide guidance on the remediation required**

This handbook is aimed at people who need to procure, plan and manage the life cycle of a penetration testing project.

WHAT YOU'LL LEARN

- **Gain a greater understanding of the various penetration testing aspects**
- **How to determine the right kind/s of penetration tests suited to your specific business context**
- **Guidance on the end-to-end process to achieve real value and full benefit from penetration testing results**
- **How and why penetration testing is a fundamental component to any risk management programme**

ABOUT COMTACT LTD.

Comtact Ltd. and its operations are ISO27001-accredited

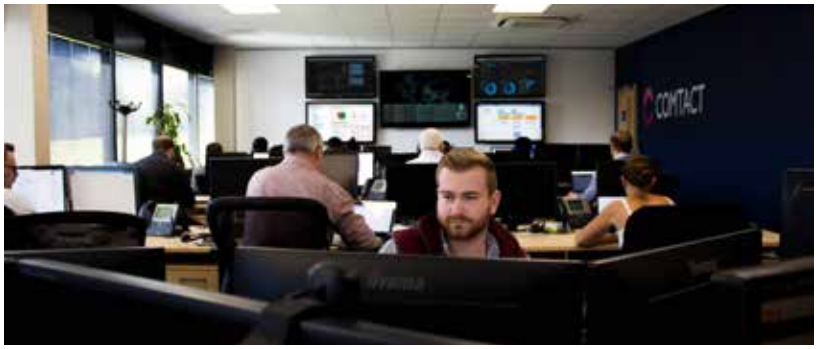
Established in 2005, Comtact Ltd. is a **specialist full-service cyber security provider** operating 24/7 from a state-of-the-art Security Operations Centre (SOC) in Northampton, UK – located at the heart of a secure Tier 3 data centre.

SECURITY TO THE CORE

Comtact's Security Operations Centre combines the very best practice on Cyber prevention and defence, with market-leading intelligence, to ensure we're always ahead of today's fast evolving cyber threats.

CYBER DEFENCE CENTRE

Located at the heart of a high security, controlled-access Tier 3 data centre in Northampton, Comtact's state-of-the-art UK Cyber Defence Centre (SOC) targets, hunts & disrupts hacker behaviour, as part of a multilayered security defence, helping secure some of the UK's leading organisations.



- **Highly experienced UK-based team**
- **24/7 'eyes on screen' security operations**
- **Best-in-class processes & services**
- **Redundant and secure state-of-the-art facilities**
- **UK focused, UK staffed, UK governance – on first name terms**

OUR EXPERTISE

We offer a full range of specialist cyber security services; always placing the client's needs at the heart of the solution.

ASSESSMENT

The first and most important step towards forming an effective defence.

- SECURITY ASSESSMENTS
- PENETRATION TESTING
- VULNERABILITY ASSESSMENT
- PHISHING-AS-A-SERVICE

PROTECTION

Protect, manage and secure your perimeter security – the first line of defence.

- ENDPOINT PROTECTION
- NETWORK SECURITY
- MALWARE PREVENTION
- SECURITY PATCHING & CONFIGURATION

MONITORING

24/7 'eyes on screen' monitoring to defend and protect your most critical assets.

- 24/7 THREAT MANAGEMENT -AS-A-SERVICE
- 24/7 SECURITY MONITORING
- 24/7 SOC-AS-A-SERVICE

CYBER AWARENESS

User awareness training & assessment, to assist and protect your workforce.

- USER AWARENESS TRAINING
- SOCIAL ENGINEERING

SECURITY CONSULTANCY

Call upon the expertise of some of the UK's leading security authorities.

- CYBER IMPROVEMENT PROGRAMMES
- BEST PRACTICE POLICIES
- DATA SECURITY & USER PRIVILEGES

WHAT'S THE DIFFERENCE?

PENETRATION TEST VS. VULNERABILITY SCAN

Vulnerability scans, or vulnerability assessments are often confused with a Penetration test – but they are very different and should be used in a very different way to assess and test your cyber security defences.

VULNERABILITY SCAN

A vulnerability scan uses software tools to automatically assessment your network infrastructure to identify unpatched software updates, open ports, or unsupported software – identifying "known" vulnerabilities – the most frequent exploit used by hackers.

Scans should be performed quarterly, as a minimum - both externally to the network, and from within the network.

Where a vulnerability scan fits into your overall security programme

Vulnerability management is a core pillar of every cyber security framework and is often used as part of a patch management programme.

VS

PENETRATION TEST

A penetration test uses both manual and automatic techniques to identify and validate each weakness, through successful exploitation – using the same knowledge and creativity a real-world hacker would use to achieve your pre-defined objectives.

WHY & WHEN IS A PENETRATION TEST NEEDED?

There are numerous reasons why you would require a penetration test:

1 PROVIDE A REAL-WORLD TEST OF YOUR SECURITY

No day passes without news of a cyber attack, or data breach. Testing your existing security controls provides a quick and clear answer to the question, “What is the current state of my cyber security?”

2 ON-GOING SECURITY ASSESSMENT

Any penetration test highlights your current risks and the impact on the Confidentiality, Integrity and Availability of your data, as part of an on-going cyber security assessment programme.

3 NEW OR UPDATED INFRASTRUCTURE

Whether and evolving, or expanding infrastructure, it is imperative that your security keeps pace with the changes. And particularly when launching a new product or service, you should rigorously test the validity of the security controls in place.

4 NEW BUSINESS ACQUISITION

As well as the significant network changes following an acquisition, there is also a significant transfer of legal risk. A penetration test will quickly identify critical security flaws which require remediation.

5 COMPLIANCE REQUIREMENTS

Penetration testing is often a requirement of legal, regulatory and compliance standards e.g. UK Government, PCI DSS, ISO 27001. While assessment would not guarantee security, it proves a framework and consistent standard.

6 HELP BUILD A ROADMAP OF IMPROVEMENTS

While no substitute for a comprehensive cyber security improvement programme, a penetration test will help identify the gaps in your security, from which you can build a roadmap of improvement.

7 JUSTIFY BUDGET INCREASE

All businesses need to control costs. A successful penetration test can help focus minds on the real threats faced, while providing a roadmap of short-term improvements required to reduce risk of attack.

TYPE OF PENETRATION TEST

There are several different types of penetration test, with different viewpoints and objectives. While there are numerous sub-categories and variations, generally, the different types of penetration test can be divided into four main groups:

External Network Penetration Test

An external network penetration test is typically what most people think of when talking about pen testing. Network devices, servers and software packages represent a constant challenge to secure, and a frequent opportunity for attack.

An 'external' penetration test involves trying to compromise an organisation's network across the Internet (remotely, as a hacker would be), to probe your perimeter defences and see where potential weaknesses and vulnerabilities lie.

Internal Network Penetration Test

An internal penetration test simulates either the actions a hacker might take once access has been gained to a network, or those of a malicious employee from within the network.

An internal network penetration test is typically performed from the perspective of both an authenticated and non-authenticated user, to ensure that the network is critically assessed for both the potential exploit of a rogue internal user, and an unauthorised attack.

Web Application Penetration Test

Website and web applications are in their nature globally accessible and easily probed, with many providing access to confidential user or credit card data. As these systems scale in complexity, the range of exploitable vulnerabilities rises, making web applications a highly prized target for cybercriminals.

A web application penetration test looks for any security issues that might have arisen as a result of insecure development or coding, to identify potential vulnerabilities in your web applications, including website, CRM, extranets and internally developed programmes.

Social Engineering

Social engineering is commonly seen as the modern frontier in IT security - and certainly one of your greatest risk.

A social engineering penetration test will help you assess and understand the susceptibility within your organisation to human manipulation via email, phone, media drops, physical access, social media mining etc.

In practice, hackers will often use social engineering as a first step to gain a foothold into the network, from which they can elevate user privileges - it is often easier to exploit users' weaknesses than it is to find a network or software vulnerability.

Which type of penetration test is right for me?

In practice, a pen tester might use a combination of techniques; it's very common for social engineering to feature in each type of test we've outlined. But importantly, the pen test should be tailored to meet your specific objectives.

CREATING A BRIEF FOR A PENETRATION TEST

When creating a brief for a penetration test, there are number of important factors to consider ensuring you achieve your desired objectives.

SET OBJECTIVES

Understand and set clear objectives for the test – in order to meet not just your requirements, but the requirements of other stakeholders.

ALLOCATE A BUDGET

Allocate an appropriate budget to complete the desired programme, taking into account the scale and complexity of your requirements.

DETERMINE THE TYPE

Ensure you understand and select the correct type of penetration test to achieve your objectives, including the prior level of knowledge provided to the pen tester.

DETERMINE CERTIFICATIONS

Place your trust in your testers. Ensuring you use CREST-certified testers is the best way to be confident is the capabilities.

ASK FOR REFERENCES

Ask for customer references, as well as the experience/profile of the assigned pen tester.

PREPARE

Ensure your organisation is prepared, with the necessary personnel and technical resources allocated to facilitate a trouble-free test. It is best practice to perform back-up prior to the test, as well as agreeing protocols if services are impacted during the test.

PENETRATION TESTING STRATEGIES

Black-Box Testing

The penetration tester is placed in the role of the average hacker, with has no internal knowledge of the target system, so the assignment depends on the tester's ability to locate and exploit vulnerabilities in the target's outward-facing services.

White-Box Testing

The penetration tester is given full visibility of the network architecture and design, source code etc., providing a comprehensive assessment of both internal and external vulnerabilities.

Grey-Box Testing

Grey-box penetration testers are provided some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network, providing a more focused and efficient assessment of a network's security than a black-box assessment.

LIFECYCLE OF A PENETRATION TEST

WHAT SHOULD YOUR PEN TEST REPORT CONTAIN?

Management Summary

A summary of key threats and business risks in a high-level risk-based format suitable for non-technical Directors, with 'at a glance' Critical and High risks.

Technical Details

Easy to follow summary of the identified vulnerabilities, and summary remedial action, plus details of each identified vulnerability and the steps taken by the pen tester to breach the network/defences.

Risk-scored Report

The report should include a vulnerability scoring system to rate discovered issues, based on severity and conform to a standardised scoring system, such as The Common Vulnerability Scoring System (CVSS).

Remediation & Next Actions

Details of the required remediations for each identified vulnerability, plus supplemental information and/or recommendations on any required security controls, process and policy improvements etc.

QUESTIONS TO ASK YOUR PEN TEST PROVIDER

1 What certifications do you hold?

Make sure your pen testing provider is CREST-approved, ensuring adherence to industry-standard best-practice, as well as an enforceable Code of Conduct.

CREST certification means that you can be confident your pen testing will conform to rigorous methodologies, up-to-the-minute techniques, and at the same time operational safety will be given the highest priority.

When discussing certifications, also don't forget to ask whether the provider has ISO 27001 certification - the essential information security standard, as you'll want to ensure that the company you engage will keep your sensitive data safe.

2 What's your pen testing methodology?

Broadly, this is guided by the requirements laid down by CREST, but the engagement process will vary from provider to provider. There is no 'one-size-fits-all' approach, specifically because every business is different - different infrastructures, different objectives. But a competent specialist should be able to talk you through different types of penetration test, various hacking strategies, what purpose they serve, as well as how they fit your overall objectives.

3 What do your pen test reports look like?

Be sure to ask for a sample penetration test report, and as you review them, consider what you want from a final report. Who will be reading it? What's their level of IT literacy? Look for clear and actionable advice for each identified vulnerability.

4 What is your own internal security like?

The penetration test is highly likely to uncover critical security vulnerabilities within your organisation's environment, and the accompanying report will document, step-by-step, how they are exploited. Ask for details on how this confidential data will remain secure, and any steps taken to ensure its safekeeping. Consider how you want the report to be delivered, and what the company recommends.

5 Do they offer remediation?

Suppliers will fall somewhere on a spectrum between offering broad advice, experts assistance with any corrective action required, or right up to full remediation services.

6 Can I talk to a previous customer?

Ask for references. A successful, reputable company will be able to provide you with numerous satisfied customers to vouch for their services - even if they are naturally unable to divulge the type of work they were carrying out.

You should also want to ask about the individual profile, experience and qualifications of the penetration tester that will be assigned to your project.

PENETRATION TESTING CHECKLIST

PRE-ENGAGEMENT

- Agree your objectives
- Attain approval from stakeholders (Board-level etc)
- Get a signed NDA to ensure confidentiality.

SUPPLIER EVALUATION

- Check certifications (CREST, ISO27001)
- Ask for references
- Get a copy of a sample penetration test report
- Confirm pen testing methodologies
- Review the experience & certifications of the pen tester
- Does the supplier provide remediation?
- Are costs competitive?

ENGAGEMENT DETAILS

- Discuss, agree and define scope of work and objective.
- Assign an internal Management-level contact (IT, or non-IT)
- Assign an internal Technical contact (IT)
- Agree testing strategy (Back box; Grey box; White box)
- Agree permitted pen testing techniques (e.g. social engineering)
- Agree scale and timescale of the penetration test (How many IP addresses; Day per location)
- Agree network appliances/IP address in/out of scope
- Agree critical alert protocol
- Agree time allocation

POST-ENGAGEMENT DETAILS

- Confirm final report delivery method
- Set report delivery and de-brief date

TAKE THE NEXT STEP

SPECIALIST CYBER SECURITY SERVICES

Your own 'full service' security operations team, fully resourced and expertly supported – 24/7, out of hours, or 'on-demand'.

24x7x365 SUPPORT

Comtact has a multi-skilled, three-tiered professional support, providing 1st line and 2nd line support operated from our 24x7x365 high security Tier 3 data centre.

Penetration testing forms such a vital part of an ongoing vulnerability management strategy, using real-world hacking techniquest to test the cyber security defences of your organisation.

We'll help you uncover the most critical vulnerabilities that could be lurking within your organisation's environment and prioritise future improvement plans.

CREST-certified

Performed by experienced CREST -certified security professionals.

Highly experienced

We've extensive experience across large, complex organisations, with a pool of skilled Penetration Testers, so we can always match the required skillset to the client.

Results-driven

Defined, rigorous testing methodology produces real results, all documented in an in-depth risk-scored report, with expert recommendations & next actions.

ADDITIONAL RESOURCES

ARTICLES

- A buyers guide to penetration testing services
- The best ethical hacking techniques
- Penetration Testing Certifications
- The difference between a vulnerability scan and a penetration test

SAMPLE REPORT

- Download a Penetration Test Sample Report

ON-DEMAND WEBINAR

- Developing successful security vulnerability management programmes

COMTACT
ALWAYS ON. ALWAYS SECURE.

Comtact Ltd.
Devonshire House, Bourne
Business Park, 5 Dashwood Lang Road,
Weybridge KT15 2NY

Tel: 03452 75 75 75
Email: enquiries@comtact.co.uk

www.comtact.co.uk

Comtact-Ltd

@comtact_ltd