What to Expect During a Penetration Test

Client Handbook

Contents

1, Introduction

A penetration test is a controlled, authorised simulation of real-world cyberattacks designed to identify weaknesses before a malicious actor can exploit them. This handbook explains exactly what to expect when BlackBox Pentesters conducts your assessment, from preparation all the way through to final reporting.

Our goal is simple: give you a clear, structured experience with no surprises, meaningful insights, and practical outcomes that strengthen your organisation.

2. Before Testing Begins

2.1 Scoping

We start by confirming:

- Systems, applications, and infrastructure in scope
- Testing type (internal, external, web app, cloud, physical, social engineering)
- Testing hours
- Exclusions
- Points of contact
- Risks and constraints
- Reporting expectations

A clear scope means clean, efficient testing.

2.2 Pre-Engagement Requirements

Clients provide:

- Required credentials (if authenticated testing)
- Test accounts
- Access details (VPN, URLs, allowlists)
- Any documentation useful for navigating the environment

BlackBox Pentesters validates everything before testing begins.

2.3 Change Control Awareness

We strongly recommend informing:

- IT operations
- Security teams
- Service owners

This prevents false alarms and avoids blocking legitimate test traffic.

3. During the Test

3.1 Realistic but Controlled

Our consultants simulate genuine attacker techniques using safe, agreed-upon methods. No destructive tools are used, and no actions exceed the approved scope.

3.2 Noise and Log Visibility

You may see:

- Login attempts
- Scanner activity
- Unexpected 404/500 logs
- Authentication alerts

This is normal during a penetration test.

3.3 Communication

You'll receive:

- A daily or agreed checkpoint update
- Immediate notification if a critical vulnerability is discovered
- Fast communication for any access issues that arise

3.4 Business Impact

We design tests to minimise disruption. However, certain tests (authentication brute force, WAF rule testing, API fuzzing) may generate load. Where needed, we'll coordinate timing to avoid operational impact.

4. Types of Activity You Can Expect

Depending on the engagement type, BlackBox Pentesters may perform:

4.1 External Network Testing

- Service enumeration
- Vulnerability assessment
- Firewall analysis
- Misconfiguration discovery
- Attack path mapping

4.2 Internal Network Testing

- Lateral movement
- Privilege escalation attacks
- Password and credential analysis
- Network segmentation testing
- Active Directory security checks

4.3 Web Application Testing

- Authentication testing
- Session and token security
- Input validation
- Business logic review
- API security validation

4.4 Cloud Environment Testing

- Identity and access review
- Conditional access testing
- Misconfiguration checks
- Role and permission analysis

4.5 Physical / Social Engineering

(If in scope)

- Tailgating attempts
- Badge cloning trials
- Reception interaction
- Device insertion attempts
- Vishing / pretexting

This is always carried out safely and discreetly.

5. Safety, Confidentiality & Ethics

BlackBox Pentesters:

- Does not access live customer data unless unavoidable
- Does not run destructive payloads
- Does not exceed scope
- Logs and tracks all test activity
- Uses encrypted channels and secured infrastructure
- Maintains full confidentiality

Your data and systems remain protected at all times.

6. After the Test

6.1 Initial Debrief

You receive:

- A clear summary of key findings
- Critical risks highlighted immediately
- Remediation priorities

This usually happens the same day testing concludes.

6.2 Full Report

The written report includes:

- Executive summary
- Technical findings
- Risk ratings
- Evidence
- Attack paths
- Practical remediation guidance

Reports are structured for both technical and non-technical readers.

6.3 Retesting (If Included)

Once fixes are applied, BlackBox Pentesters can retest relevant findings to confirm closure.
Many clients use this as a final check before audits or accreditations.

7. What Success Looks Like

A successful penetration test gives you:

- A clear picture of your security posture
- Identified risks with real-world context
- Practical steps to improve resilience
- Evidence for compliance, audit, and insurance
- Greater confidence in your systems and processes

The objective isn't to "pass" or "fail" — it's to discover issues before attackers do and give your organisation the clarity it needs to strengthen its defences.

8. About BlackBox Pentesters

BlackBox Pentesters delivers high-quality penetration testing, red teaming, and physical intrusion services backed by real adversarial experience. Our approach is built on clarity, professionalism, and raising standards in cybersecurity testing.